Derecho y Realidad
Núm. 20 • II semestre de 2012
Facultad de Derecho y Ciencias Sociales, UPTC
ISSN: 1692-3936

Los delitos contra los datos personales y el habeas data en la Ley 1273 de 2009

Offences against personal data and habeas data in 1273 of 2012 Law

Libardo Orlando Riascos Gómez*

Resumen

En el presente artículo se hace un análisis conceptual del derecho fundamental del habeas data, que en principio se acuñó en el constitucionalismo del Brasil producto de los trabajos doctrinales y legislativos, y luego se extendió al derecho latinoamericano. Colombia lo recogió en el artículo 15, inciso 2º de la Constitución de 1991 y recientemente lo reglamentó en forma parcial desde el punto de vista de la información o datos financieros en la Ley 1266 de 2008, la cual fue declarada exequible por la Corte Constitucional colombiana en Sentencia C-1101 de 2008. Por su parte, la Ley 1273 de 2009 adicionó en forma parcial el actual Código Penal colombiano de 2000, al establecer un nuevo bien jurídico que protege las informaciones y los datos personales, creando nuevos delitos que afectan el llamado habeas data y los datos personales, tales como: la interceptación de datos personales, el uso de software malicioso, la violación de los datos personales, la suplantación de sitios de web para capturar datos personales, entre otros.

* Docente Titular de Derecho Público, Facultad de Derecho de la Universidad de Nariño desde 1986. Magíster en Criminología de la USTA-UDENAR, 1994. Doctor en Derecho Público de las Universidades españolas de Navarra 1986 y Lleida 1999. Escritor de obras jurídicas y artículos en revistas jurídicas especializadas nacionales y extranjeras.

Palabras clave

Habeas data, delitos contra los datos personales, derecho a la información, derecho a la intimidad y al buen nombre.

Abstract

In this article we make a conceptual analysis of the fundamental right of Habeas Data, which was originally coined in the constitutionalism of Brazil as a product of doctrinal and legislative works and then spread to Latin American law. Colombia picked it up in article 15, paragraph 2 of the Constitution of 1991 and recently regulated it partially, from the point of view of information or financial data in 1266 of 2008 Law, which was declared enforceable by the Colombian Constitutional Court in Sentence C-1101-2008. In turn, 1273 of 2009 Law, that added partially the current Colombian Criminal Code of 2000, establishing a new legal interest that protects information and personal data creating new offences that affect the so-called habeas data and personal data, such as the interception of personal data, the use of malicious software, the violation of personal data, phishing web sites to capture personal data, among others.

Key words

Habeas data, offences against personal data, right to information, right to privacy and a good reputation.

1. Cómo surge el término habeas data[1]

El término *habeas data* que hoy universalmente conoce el ámbito del derecho como una eficaz y expedita institución jurídica constitucional y legislativa para la defensa y protección de los datos o informaciones personales y el pleno ejercicio de los derechos y las libertades constitucionales, ha tenido una explicación etimológica generalizada y homologada en los Estados latinoamericanos y principalmente en Brasil donde nace la institución con dicho nombre.

El constitucionalismo brasileño creó, en 1988, el *remedio* o acción procedimental del habeas data como un mecanismo jurídico-constitucional preventivo para el acceso y el conocimiento de los datos o informaciones personales y como un instrumento sancionatorio, de corrección, actualización y supresión de datos cuanto estos son incorrectos. En el desarrollo legislativo nueve años después, el habeas data se convirtió en una acción exhibitoria de los datos personales de carácter civil y administrativo, según la naturaleza jurídica de las personas naturales o jurídicas que manejen los datos. El legislador volvió sus ojos al origen de la institución jurídica románica: un interdicto exhibitorio de acta o de documento.

El término *habeas data* proviene del término inglés *data* o datos, o del singular *Datum* dato, que se le aplica por agregación a la definición del *Habeas* latino, pues, como lo demuestra *Puccenilli* (s.f.), el término data no significa datos ni su singular dato en latín, como casi todos los lectores deducen fonológicamente por vez primera de los términos *habeas data*. Este desfase léxico va más allá del simple uso de términos latinos e ingleses unidos, para explicar una institución jurídica que se convierte en un mecanismo constitucional y legal de protección y defensa de otros derechos de igual rango.

2. La conceptualización del habeas data

2.1 El habeas data en la Constitución de Colombia es una acción de tutela específica de tipo jurisdiccional o una vía administrativa

El habeas data en la Constitución de Colombia es una acción de tutela específica de tipo jurisdiccional o vía administrativa que protege todas las fases del tratamiento de los datos personales y los derechos constitucionales, entre ellos el de la intimidad y el buen nombre.

La institución jurídica colombiana del habeas data se estructura a partir del inciso 1º y 2º del artículo 15, el artículo 20 y 74 de la Constitución de 1991. A saber:

---

[1] (Riascos, s.f.).

Todas las personas tiene derecho a su intimidad personal y familiar y a su buen nombre... De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Agrega el inciso segundo, *En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*.

El artículo 20, a su turno, reza: *Se garantiza a toda persona la libertad... (de) informar y recibir información veraz e imparcial...*

Por su parte el artículo 74, sostiene: *Todas las personas tienen derecho a acceder a los documentos públicos...*

En la primera norma se encuentra el núcleo esencial del habeas data, pues mientras en el inciso 1º se confiere el ejercicio de la acción de tutela específica a toda persona natural o jurídica para que pueda aprehender el conocimiento de las informaciones o datos personales que le conciernen, y una vez conocido el contenido de estas, si lo encuentra incompleto, no veraz, erróneo, *antiguo* o contrario al derecho, podrá solicitar su actualización y rectificación, siempre que la información haya sido recabada en bancos de datos y *en archivos de entidades públicas y privadas* en forma manual, mecánica, escrita o electrónica (informática)[2]. Conocimiento, acceso, actualización y rectificación de los datos personales del concernido que afecten el manejo, uso y control de la información de la persona, como sus derechos fundamentales, principalmente el derecho a la intimidad personal y familiar y su buen nombre.

La primera parte del inciso 1º del artículo 15 constitucional establece, en nuestro criterio, una especie de *habeas data administrativo*, si el concernido con los datos ejercita el derecho de petición (artículo 23, constitucional) o los recursos administrativos ordinarios o extraordinario previstos en el Código Contencioso Administrativo (C.C.A), (artículos 49 y ss., y 69 y ss.,) para solicitar la aprehensión o acceso de los datos personales y lo hace ante una persona de derecho público de cualquier nivel administrativo (nacional, distrital, departamental, municipal y corregimental), ante una persona de derecho privado con función o servicio público (artículo 1º C.C.A.). Esto sin perjuicio de ejercer la acción de tutela ante los jueces individuales y autoridades, tribunales y altas cortes judiciales que forman parte de la jurisdicción constitucional colombiana y según los factores de

[2] En la Obra hacemos una amplia explicación de los medios mecánicos y electrónicos, telemáticos o informáticos, utilizados en el tratamiento de datos personales, en la elaboración del documento electrónico –*E-document*– y en la tipificación de las nuevas conductas delictivas sobrevenidas por la abusiva o ilegal utilización de las nuevas tecnologías de la información y la comunicación (medios TIC) y la informática. (Riascos, 1997, p. 10 y ss).

competencia, ejercicio de la acción utilizado como mecanismo transitorio para defender o garantizar el derecho fundamental de petición, o bien ejercida directamente cuando se han agotado previamente los mecanismos administrativos o jurisdiccionales pertinentes y no existe otro remedio jurisdiccional o administrativo para tutelar un derecho fundamental (artículo 86 constitucional y Decreto 2591 de 1991). Si se ejercita la acción de tutela en una de las dos formas para aprehender el conocimiento o acceso a la información o datos personales del concernido, decimos que emplea el *habeas data jurisdiccional* en esta fase del tratamiento de datos.

Iguales reglas previas o concomitantes al ejercicio de la acción de tutela específica o de habeas data, se podrán impetrar por parte de la persona concernida o afectada con los datos o informaciones inexactos, incompletos, erróneos, *antiguos*, falsos o contrarios al ordenamiento jurídico vigente, cuando se persigue la actualización y rectificación de los mismos. En efecto, el interesado o afectado con los datos personales, podrá hacer uso del habeas data administrativo si estima que más viable y expedito que el habeas data jurisdiccional. Sin embargo, como profundizaremos más adelante al comentar los tipos de habeas data en la doctrina, se ha impuesto en la praxis colombiana que la acción de tutela es la seleccionada por los colombianos para proteger y defender los derechos fundamentales incluidas las facultades del habeas data de conocimiento, acceso, actualización y rectificación de la información o datos personales y se justifica como lo exige el reglamento de la acción de tutela, que esta se emplea como *mecanismo transitorio para evitar un daño irreparable* pese a existir otros mecanismos jurisdiccionales con igual finalidad[3].

El inciso 2º del artículo 15 constitucional, se refiere a las etapas o fases del tratamiento o procesamiento de datos, sean estas efectuadas con medios mecánicos o escritos, o bien con medios informáticos (electrónicos o telemáticos). Estas fases son: *la recolección, tratamiento y circulación de datos,* en las cuales, como lo enfatiza la Constitución, *se respetarán la libertad y demás garantías consagradas en la Constitución*.

En el transcurso del tratamiento o procesamiento de datos personales, como profundizaremos *ut infra,* son viables tanto el habeas data administrativo como el habeas data jurisdiccional, y aquí con mayor razón, ya que es en estas fases del tratamiento de datos donde se presenta la alta tensión, vulnerabilidad o defensabilidad y protección de los derechos y libertades fundamentales de la persona.

---

[3] *LA TUTELA COMO MECANISMO TRANSITORIO.* Aún cuando el afectado disponga de otro medio de defensa judicial, la acción de tutela procederá cuando se utilice como mecanismo transitorio para evitar un perjuicio irremediable. En el caso del inciso anterior, el juez señalará expresamente en la sentencia que su orden permanecerá vigente sólo durante el término quela autoridad judicial competente utilice para decidir de fondo sobre la acción instaurada por el afectado… (art. 8º del Decreto 2591 de 1991).

Cuando el artículo 20 constitucional *garantiza a toda persona la libertad* (...) *de informar y recibir información veraz e imparcial* (...) está garantizando un derecho universal[4] y un derecho incorporado al derecho nativo mediante la Ley 74 de 1968, por la cual se aprueba el Pacto internacional de derechos civiles y políticos y la Ley 16 de 1972, por la cual se aprueba el Convenio Americano sobre derechos humanos o Pacto de San José de Costa Rica. En los artículos 19 y 13, respectivamente, se recogen el derecho, los deberes y las responsabilidades del Estado y los particulares respecto al derecho a la información, entendido este en el más amplio sentido y no solamente en la especie aplicable al derecho periodístico, de prensa o de imprenta. Se garantizan las dos visiones del derecho a la información: la activa, de informar veraz, oportuna, completa y libre de errores o limitante o restricción alguna, salvo las estipulada en la Constitución y la ley y en cabeza del Estado o sus entidades, organismos o dependencias o de los particulares con función o servicio público; así como la visión pasiva de recibir información veraz, completa, imparcial, oportuna, eficaz y libre de limitantes y restricciones que no sean las autorizadas por el ordenamiento jurídico vigente.

Finalmente, el artículo 74 garantiza a *todas las personas* el derecho que ostentan *para acceder a los documentos públicos* que interesen o afecten un derecho o libertad fundamental de una persona natural o jurídica y se hayan recabado en un banco de datos o archivo de una entidad pública o privada con función pública, o bien cuando dichos documentos estén involucrados en una cualquiera de las fases del tratamiento de datos personales. El derecho de acceso a la información pública cualquiera sea la forma del almacenamiento o del tratamiento (mecánico, escrito o electrónico), garantizado a toda persona natural o jurídica, se encuentra reglamentado con carácter pre y post constitucional a 1991, en la Ley 4 de 1913, artículo 32; en la Ley 57 de 1985 o Estatuto de la Información, en el Código Contencioso Administrativo, la Ley 527 de 1999 (acceso electrónico a documentos o páginas de web públicos y privados) y la Ley 962 de 2005 o *Estatuto Antitrámites* en Colombia.

La acción de tutela específica de habeas data en Colombia, desde su instauración en la Constitución de 1991, como segundo Estado de Latinoamérica en instituirla y elevarla a rango constitucional, ha provocado, en buena hora, un amplio y fructífero trabajo jurisprudencial de la Corte Constitucional como una mesurada labor de la doctrina especializada en pro de la estructuración, desarrollo, alcances, efectos jurídicos materiales y sustanciales y la evolución de la institución jurídico constitucional del habeas data, tal como lo demostramos a lo largo de este ensayo

[4] El artículo 19 de la *Declaración Universal de los derechos Humanos* de 10 de Diciembre de 1948, por el cual Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. informan el proceso de administración de bases de datos personales. Sentencia T-279 de 2002 de la Corte Constitucional.

jurídico. Esto, por cuanto en nuestro país todavía no nace a la luz pública una ley que regule integralmente el derecho y garantía constitucional del habeas data.

El Congreso de la República desde antes de la Constitución de 1991 y con mayor razón después de esta, ha avocado el conocimiento de diversos proyectos de ley ordinaria y de ley estatutaria que persiguen regular sectorial o parcialmente el derecho de habeas data, sobre todo en algunas fases del tratamiento informatizado o no de datos personales, con énfasis en el dato financiero de carácter comercial, bancario, tributario y tarifario o de servicios públicos domiciliarios.

La institución jurídico constitucional del habeas data en Colombia, hoy en día, a pesar de haberse expedido la Ley 1266 de 2008, por la cual se dictan *las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y proveniente de terceros países…*, en todos aquellos otros datos personales no económicos o financieros, sigue siendo una acción de tutela específica que *a priori* tiene las siguientes connotaciones: (i) la acción de tutela puede ejercerla toda persona que vea amenazado o vulnerado algún derecho o libertad fundamental; (ii) el habeas data, por la ubicación orgánica, denominación y clasificación en la Constitución *ab initio,* es un derecho fundamental[5], a tenor del artículo 86, constitucional; (iii) es un derecho de aplicación inmediata, según el artículo 86, es decir, *que no requiere previo desarrollo legislativo o de algún tipo de reglamentación legal o administrativa para su eficacia directa y que no contemplan condiciones para su ejercicio en el tiempo, de modo que son exigibles en forma directa e inmediata*[6]; (iv) como derecho fundamental que es el habeas data, si el legislador decide reglamentarlo, solamente deberá hacerlo mediante una ley estatutaria (art. 152-1, constitucional), cuya aprobación, modificación o derogación exigirá de la mayoría absoluta de los miembros del Congreso y deberá efectuarse dentro de una sola legislatura, según el artículo 153 ibíd. Además, requerirá del control de constitucional previo y automático de la Corte Constitucional sobre la exequibilidad del proyecto. Se aclara *in fine* del artículo citado que *cualquier ciudadano podrá intervenir para defenderla o impugnarla*[7]*;* (v) es ejercita para garantizar y proteger los derechos fundamentales, incluidos la intimidad, el buen nombre, el honor, la

---

5 El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición y actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales. Sentencia T-279 de 2002 de la Corte Constitucional.

6 Corte Constitucional. Sentencia T-002-1992.

7 El trámite de varios proyectos de ley ordinaria del Habeas Data posterior a la expedición de la Constitución de 1991 y hasta antes de la Sentencia C-008-1995 que declaró inconstitucional el proyecto No. 127/93 de la Cámara y No. 12 /93 del Senado, relativo a las fases del tratamiento de datos financiero, por no seguir el trámite especial de ley estatutaria, permitió vislumbrar el carácter de derecho fundamental regulado por ley estatutaria que tiene el Habeas Data.

información, el libre desarrollo de la personalidad, contra toda amenaza o vulneración por acción u omisión de las *autoridades públicas*; (vi) la protección efectiva de la tutela consistirá en la orden judicial que imparta el juez constitucional mediante sentencia para que el funcionario o autoridad pública actúe o se abstenga de hacerlo; (vii) la acción procederá cuando el interesado o perjudicado no disponga de otro medio judicial, salvo que se utilice como un mecanismo transitorio para evitar un perjuicio irremediable; y, (viii) el habeas data origina un procedimiento sumario y preferente y sin mayores formalidades o ritualidades, adelantado a voluntad por la persona concernida o por quien lo represente.

2.2 Conceptualización de habeas data, titulares de los datos y los datos personales en la Ley 1266 de 2008 y en el derecho comparado

El objeto de la ley citada es *desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en banco de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países*.

El habeas data, en consecuencia, es un derecho de rango constitucional circunscrito no solo a los elementos de estructuración dados en forma explícita en el artículo 15 constitucional, sino en complementariedad con los artículos 20 y 74 de la Constitución, en definitiva tal como habíamos conceptualizado aun antes de la expedición de la ley.

La diferencia evidente del concepto dado al habeas data en la citada ley, es la referencia excluyente de los datos financieros o económicos sobre todos los demás, que, a propósito, son muchos, que fue el objetivo primigenio y último de los proponentes de los proyectos de ley estatutaria (Congreso y Gobierno) que finalmente se convirtió en ley.

La presente concepción de habeas data está estructurada por una serie de elementos (i) el jurídico, que incorpora la connotación de ser un derecho fundamental, autónomo y diferente a la intimidad, el buen nombre, el libre desarrollo de la personalidad y el de autonomía personal y el de información, aunque tengan identidades y tronco común como el valor de la dignidad de la persona humana; (ii) el estructural, constituido por unas acciones o verbos consecutivos: conocer, actualizar y rectificar informaciones o datos de la persona que le conciernen y hallan recolectados y almacenados en bancos de datos o ficheros; (iii) el procedimental, constituido por

las diferentes etapas del procedimiento por el que atraviesan los datos personales para llegar a ser cedidos, transferidos o puestos en circulación. Esas etapas son: la recolección, el tratamiento propiamente dicho y el almacenamiento en bases de datos; (iv) el ideológico, compuesto por el contenido mismo de los datos personales, su reserva, confidencialidad y disponibilidad según su connotación jurídica y entronque con otros derechos y libertades constitucionales.

Por tal razón, a continuación haremos una reseña de los datos personales y las diversas clasificaciones previstas en la Ley 1266 de 2008.

De la conceptualización generalizada del habeas data como derecho y como garantía constitucional, se puede deducir que los sujetos que intervienen en su estructuración son, de una parte, (i) los titulares de los datos, los causahabientes o sucesores, y de otra, (ii) el Estado como persona jurídica de derecho público y los responsables de los bancos de datos públicos o privados, o de las centrales de información financiera (crediticia, bancaria, bursátil, tributaria, tarifaria, etc.) o especializada.

2.2.1 El titular de los datos. El habeas data en el ámbito latinoamericano es un derecho constitucional aforado a *toda persona* que tiene como facultades prioritarias, en principio, el acceso y conocimiento de la información o datos personales que a ella le conciernen, y luego, según la aprehensión de este conocimiento, si observa que los datos son inexactos, incompletos, erróneos, antiguos, falsos, discriminatorios o no conformes a derecho, podrá solicitar ante las personas, autoridades públicas o privadas, en vía administrativa o vía jurisdiccional, según el Estado latinoamericano y las reglas de competencia por estos establecidas: la actualización, la rectificación, la eliminación o la anulación de los datos personales.

2.2.2 Las personas físicas, naturales o humanas. En el contexto de las Constituciones latinoamericanas y las correspondientes leyes reglamentarias del derecho de habeas data (Riascos, 2009, p. 67 y ss), en forma inequívoca se confiere la titularidad de los datos personales a toda persona, *ab initio*, natural, física o humana determinada o determinable, pues no cabe la titularidad de los datos para una persona anónima. La titularidad evoca un claro derecho de propiedad inmaterial sobre el dato, además de las facultades o derechos inherentes al habeas data: acceso, conocimiento, actualización, rectificación y eliminación de datos personales recabados en bancos, registros, bases o ficheros de datos o informaciones personales, sean de naturaleza pública o privada.

2.2.3 Las personas jurídicas, morales o de *existencia ideal*. Aunque en principio se discutió la titularidad de datos personales por parte de las personas jurídicas, morales o de *existencia ideal* (como se le denomina en el derecho argentino, uruguayo y del Paraguay), muy pronto se desistió de la tesis negativa, por las siguientes

razones: (i) la persona jurídica, al igual que la persona física, es titular de derechos y obligaciones en el derecho universal; (ii) los textos constitucionales y leyes latinoamericanas, al reglamentar la institución jurídica del habeas data (como acción, recurso, garantía o proceso) lo hace recaer en toda persona, como del titular de los datos personales, sin hacer distinción alguna sobre su naturaleza jurídica (humana o moral), el sexo, la nacionalidad, el domicilio e incluso la edad cronológica (desde el *nasciturus* por vía excepcional tendría titularidad en este derecho); y, (iii) aunque algunos derechos inherentes a la persona humana, como el de la intimidad por ejemplo, no serían los tutelados cuando se solicita la protección de datos de la persona jurídica, sí podría eventualmente solicitarse la tutela del derecho a la *identidad o a la buena imagen,* porque en este caso *el habeas data protege un derecho a la verdad sobre los datos sociales que se posean en un determinado registro y que hagan a la reputación fama y buen nombre del afectado* (Palazzi, 1998, 4 de noviembre).

2.2.4 Personas humanas y jurídicas. Excepciones. La Ley Nacional de Protección de Datos de la Argentina de 2000 en el artículo 2º, inciso 7º, y en similar sentido varias leyes latinoamericanas sobre el particular, reconoce expresamente que es titular de los datos personales, *toda persona física o persona de existencia ideal (o jurídicas) con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento de datos*. En cambio, la Ley No. 19.628 de 1999, relativa a la *protección de la vida privada o protección de datos de carácter personal*, al prever como bien jurídico tutelado solo a la privacidad o la intimidad de las personas, arroga la titularidad del derecho de habeas data a la persona física en el artículo 2º-ñ, así: *Titular de los datos, la persona natural a la que se refieren los datos de carácter personal* (AA.VV., s.f.).

Este proceder de la legislación chilena es coherente, porque la ley solo protege el derecho a la intimidad individual y familiar de las personas, al igual que lo siguen haciendo las leyes de protección de datos personales de Europa, tanto las nacionales (caso de España[8], Portugal, Francia, Alemania) como las comunitarias (Recomendaciones de OCDE y Convenio de Estrasburgo de 1980 y 1981, respectivamente y las Directivas 95/46/CE y 97/66/CE). En todas ellas el titular de los datos es el *afectado o interesado* con los datos personales, que solo puede serlo la persona natural o física.

La Ley Federal Alemana de protección de datos de 1976-1994 o LFAPD, consecuentemente con lo anterior y al hacer mención a la persona humana como titular de los datos, en el *proceso* o tratamiento de datos, hace expresa referencia a los derechos derivados del acceso y consulta de la información. Estos derechos

[8] Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento de datos.

son: (i) la información acerca de los datos almacenados en relación con la persona; (ii) la rectificación de los datos almacenados en relación con su persona, cuando los mismos fueren inexactos; (iii) el bloqueo de los datos almacenados en relación con su persona cuando no pudiere determinarse su exactitud o inexactitud, o cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento; y (iv) la cancelación de los datos almacenados en relación con su persona, si su almacenamiento no había sido admisible o bien -a elección, además del derecho de cancelación- cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento.

Tanto las personas humanas como jurídicas están legitimadas para incoar una acción, recurso o garantía de habeas data en un proceso jurisdiccional o administrativo, bien sea en forma directa, mediante apoderado judicial o mediante el representante legal de la entidad, organismo o dependencia pública o privada, según fuere el caso y clase de persona.

En los proyectos de ley estatutaria del habeas data en Colombia, encontramos la corriente latinoamericana y no europea respecto de los titulares de los datos. En efecto, en el proyecto de Ley No. 64 de 2003, *por el cual se dictan disposiciones para la protección de datos personales y se regula la actividad de recolección, almacenamiento y circulación de datos*, se determina que es *Titular del dato personal* (...) *toda persona natural o jurídica, pública o privada a quien se refiere la información que reposa en un banco de datos o central de la información*.

En sentido similar, el proyecto de Ley Estatutaria nº 071 de 2005 *por el cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera y crediticia, y se dictan otras disposiciones*, cambia el término de *datos* por *información*, para concluir diciendo que el *Titular de la Información... es la persona natural o jurídica, a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de habeas data y demás derechos y garantías a que se refiere la... ley*. En idéntico sentido, el último proyecto de habeas data presentado al Congreso de la República: el proyecto de Ley Estatutaria nº 211/2007 Cámara, nº 027/2006 Senado, acumulado con el nº 05/2006 Senado, *por el cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios...*

Finalmente, el artículo 2º literal a, de la Ley 1266 de 2008, reconoce que el titular de los datos o la información, *es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de habeas data y demás derechos y garantías a que se refiere la ley*.

2.2.5 El afectado, cualquier persona, las organizaciones con fines e intereses colectivos y el Defensor del Pueblo están legitimados para incoar el habeas data colectivo. En el derecho argentino se planteó la posibilidad de *ejercer una suerte de Habeas Data colectivo en los casos de discriminación* (Palazzi, 1998, 4 de noviembre) previsto en el inciso 2º del artículo 43 de la Constitución por parte del *afectado, el defensor del pueblo y las organizaciones que propendan por esos fines* (protección al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general).

Estos estarían legitimados por activa para proponer la acción de habeas data en interés colectivo cuando en un banco o tratamiento de datos personales se amenace o vulnere un derecho fundamental con cualquier forma de discriminación.

En el derecho colombiano, el proyecto de Ley Estatutaria de Habeas Data de 2005, a instancias de la Defensoría del Pueblo, mencionó por vez primera *el habeas data colectivo* o *de interés público* ejercitable, según los artículos 3-4 y 24, por *cualquier persona, organización o al defensor del pueblo,* para *solicitar la suspensión, rectificación o cesación de un tratamiento de datos que se está realizando de manera irregular, con pretermisión de los requisitos establecidos para ello, o respecto de datos que no pueden ser objeto de tratamiento o cuyo tratamiento está sujeto a condiciones o requisitos que no se han cumplido y que afecta a una generalidad o grupo de personas determinadas o no*. Habeas data colectivo que no puede interpretar o confundirse con las acciones de grupo o popular constitucional previstas en nuestra Constitución en el artículo 88 y reglamentada en la Ley 472 de 1998, pues aunque el fundamento de unas y otras son los derechos de la colectividad, la *generalidad* o la comunidad, el objetivo específico del habeas data colectivo se dirige exclusivamente a restringir, limitar o prohibir un tratamiento o procesamiento de datos personales informatizado o no, que amenace o vulnere derechos constitucionales o legales de esa colectividad.

2.2.6 Curadores o tutores del afectado y los causahabientes. La LPD argentina de 2000, en el artículo 34, al mencionar la legitimación por activa de la acción de protección de datos personales o de habeas data, sostiene que podrá ser ejercitada además del *afectado* o titular de los datos, por *sus curadores o tutores*, es decir, por las personas elegidas o nombradas para cuidar los bienes o negocios de un menor de edad, o de quien no estaba en estado de administrarlos por sí.

El proyecto de Ley Estatutaria colombiana de Habeas Data de 2005, a instancia de la Defensoría del Pueblo, preveía un trato jurídico especial para los menores de edad que estuviesen involucrados en un tratamiento o procesamiento de datos o más aún cuando ya estuvieren recabados en una base o banco de datos, pues en el artículo 7º manifestaba que *el tratamiento, uso, transmisión o divulgación de datos*

se asegurará el respeto a los derechos prevalentes de los niños; agregaba en el inciso 2º, *El tratamiento de datos de carácter personal de menores sólo podrá hacerse con fines institucionales autorizados por la ley*; y finalizaba en el inciso 3º proscribiendo *el tratamiento, uso, divulgación, publicación o circulación de datos de carácter personal de menores cuyo fin sea su comercialización, tráfico, venta o cesión a terceros, excepto cuando se trate de información sobre solvencia patrimonial o financiera de menores adultos requerida en desarrollo de contratos de la misma índole para los cuales se encuentre habilitado por ley*.

De lo anterior se deduce que en el evento que pudiese estar involucrado un menor de edad en un tratamiento o procesamiento de datos personales y con este se afecte, amenace o vulnere derechos constitucionales o legales, este como titular de los datos podrá por intermedio de sus padres, o de su tutor o curador nombrado o designado al efecto, o mediante apoderado judicial, ejercitar la acción de habeas data.

Respecto al término *causahabiente*, utilizado por varias leyes latinoamericanas de protección de los datos personales, o también reglamentaria del habeas data; así como en el proyecto (colombiano) de Ley Estatutaria de 2003 y 2007, de iniciativa de la defensoría pública y de origen gubernamental y parlamentario, respectivamente, lo hacen en el sentido lato o amplio, es decir, que *causahabiente* genéricamente se denomina *a cualquier persona* que deriva el todo o parte de sus derechos de otra que se llama su *autor* o *causante*. Si la derivación se verifica por un acto entre vivos se denomina transferencia y si se verifica por causa de muerte, transmisión, la que puede ser a título universal o a título singular.

De suerte, entonces, que son terceros relativos los herederos y legatarios de alguna de las partes y los cesionarios de ellas, todos los cuales son causahabientes.

Los sucesores o causahabientes reciben el derecho de su causante o autor en las mismas condiciones en que este lo tenía, es decir, el derecho pasa de causante a sucesor con las mismas ventajas y cargas.

Los sucesores o causahabientes a título singular sufren los efectos de los actos realizados por su causante, solo en relación con la cosa o derecho que se les ha transferido o transmitido.

Los sucesores o causahabientes a título universal, en cambio, les afectan todos los actos de su causante, todos los actos les aprovecha o perjudica; todos los derechos adquiridos por su autor, salvo los personalísimos; y deben cumplir todas sus obligaciones.

El proyecto de ley nº 064 de 2003, al definir al *titular de la información,* manifestaba que ostentaba esta calidad la persona a la quien le conciernen los datos y sus causahabientes quienes *gozan también de legitimidad para el ejercicio de los derechos y acciones correspondientes* al habeas data.

El Proyecto de Ley Estatutaria de 2007, sin mencionar expresamente en la definición de *titular de la información* a los causahabientes, en el contexto del proyecto hace referencia a los derechos que estos tienen en todas las etapas del tratamiento o procesamiento de la información o datos personales, en las mismas condiciones y formalidades que los titulares de la información o datos. Verbigracia en la *circulación de información*, artículo 5º; así como también en el trámite del habeas data administrativo colombiano, originado por peticiones, consultas o reclamos ante las autoridades de control o los responsables de los bancos de datos o *centrales de información* financiera o especializada (artículo 16 del proyecto). De lo anterior se infiere entonces que los causahabientes son titulares de los datos por transferencia o transmisión de su autor o causante y por lo tanto, está legitimado por activa para ejercer los derechos o facultades del habeas data.

2.2.7 El Estado. En el término más universalmente conocido, el Estado es la persona jurídica de derecho público que puede adquirir derechos y contraer obligaciones. En tal virtud, los organismos, dependencias o entidades que hacen parte del Estado y estén representadas legal, estatutaria o legítimamente, podrán ser eventualmente titulares de datos que a estas les conciernan y estarán legitimadas para ejercitar algunas de las facultades o derechos componentes del habeas data, pero obviamente no en defensa y protección del derecho a la intimidad como derecho personalísimo exclusivo de las personas naturales o físicas, como anteriormente hemos sostenido.

Estos organismos, entidades o dependencias del Estado están legitimados en esta clase de asuntos del habeas data, tanto por activa como por pasiva, según si son titulares de los datos personales o por el contrario son responsables, administradores o manejadores de los bancos de datos públicos, o centrales de información financiera o especializada de carácter público.

Según *Palazzi* (1998, 4 de noviembre), al plantear la posibilidad de que el Estado sea *el actor en un proceso de Habeas Data*, será posible,

> *cuando este actúe en el campo del derecho privado. Pensamos que para que ello suceda, el Estado, o quien lo represente, debería estar registrado en un banco o base de datos, o al menos existir un determinado dato, o una información a la que se pretenda acceder*. Y agrega, *Recordemos que el artículo 43 establece un derecho de acceso y control de la información que puede ser ejercido en forma independiente del derecho de rectificar o actualizar esa información*.

De esta forma, el autor citado parece plantear que el Estado solamente podría ejercitar las facultades del habeas data de acceso y conocimiento de la información o datos y excluye las facultades de actualización, rectificación y cancelación de datos. En teoría es posible ejercitar todas las facultades del habeas data así sea el titular una persona jurídica.

3. Los responsables del tratamiento, banco o registro de datos, centrales de información financiera o especializada, los operadores de los datos, fuente-operador de información y las agencias de información comercial

Las definiciones son sinónimas en el concepto de ser personas naturales o jurídicas, públicas o privadas que administran, manejan, dirigen o son responsables de los bancos de datos personales públicos o privados y se constituyen como *sujetos pasivos* del tratamiento informatizado o no de datos, en otros términos, son los sujetos legitimados por pasiva. Se diferencian, en atención al Estado donde se aplican dichas denominaciones, así como en algunas funciones especiales y en las leyes que les dan origen: unas, por las leyes de protección de datos; y otras, por leyes reguladoras del habeas data integral, general o sectorial.

La Ley Orgánica de Protección de datos de España o LOPDP de 1999, en el artículo 3-d, define al *Responsable del fichero o tratamiento*, como la *persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*.

En la definición se destaca la naturaleza y titularidad jurídica de las personas que realizan el tratamiento de datos personales y sobre todo la finalidad, contenido y uso del mismo.

En la legislación argentina, LPDA de 2000, se define al *Responsable del archivo, registro, base o banco de datos, como la persona física o de existencia ideal pública o privada, que es el titular de un archivo, registro, base o banco de datos*.

En esta definición se parte del sinónimo de archivo, registro, base o banco de datos entendido solamente en el tratamiento informatizado o no de datos personales, para luego hacer énfasis en la titularidad pública o privada de dicho tratamiento y la persona que administra, dirige o es responsable de aquel.

Por su parte, el proyecto de Ley Estatutaria colombiana de Habeas Data nº 064 de 2003, definía al *responsable* del tratamiento, como *la persona natural o jurídica, pública o privada, o el servicio u organismo que trata datos personales por cuenta del operador del banco de datos o de la central de la información*. Se partía del ejemplo extranjero europeo y latinoamericano sobre el responsable del tratamiento

de los datos o del fichero o banco de datos, para luego incorporar en dicha definición también a los denominados operadores de los bancos o de la central de información. Esto, por cuanto en Colombia son las organizaciones privadas con servicios financieros, como la Central de Información de la Asociación Bancaria y de Entidades Financieras de Colombia –CIFIN-, Data Crédito, Covinoc, Computec, Inconcrédito, Credicheque, Fenalcheque, etc., *sociedades o agremiaciones de carácter privado en las cuales se registra el comportamiento crediticio, financiero y comercial de las personas que celebran operaciones con entidades financieras, cooperativas y empresas de sector real* (pág. web superfinanciera), y son las que han dominado el mercado de la información crediticia y bancaria en Colombia, por varios años y las que han generado gran parte de la jurisprudencia de la Corte Constitucional en materia del dato financiero en nuestro país. En el derecho comparado coexisten entidades u organismos de información financiera de carácter privado con las de naturaleza pública (por ejemplo, en el derecho argentino, la Central de Deudores del Sistema Financiero como sistema de información crediticia del Banco Central de la República Argentina (B.C.R.A)[9]

El proyecto de ley estatutaria colombiana de Habeas Data sectorial de 2006 y 2007, la nominación de responsables del tratamiento, responsables de los bancos de datos, responsables del tratamiento o bancos de datos por cuenta de un tercero: el operador o los responsables de las centrales de información para unificarlos en uno solo omnicomprensivo de todos los anteriores: el operador de la información.

En efecto, el artículo 3, literal c, del proyecto de ley, define al operador de información, como

> *la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por tanto el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente.*

---

[9] La central es un servicio de información del B.C.R.A, a través de la superintendencia de entidades financieras y cambiarias. Se ha estructurado con base en los datos que proveen las entidades financieras, las entidades no financieras emisoras de tarjetas de crédito y el propio B.C.R.A. Tiene por objeto brindar información sobre los deudores del sistema financiero a los bancos y demás instituciones que intermedian en el crédito, para facilitar la toma de decisiones en materia crediticia. Livellara (www.eldial.com)[

Este concepto se plasmó finalmente en la Ley de habeas Data de 2008. En una revisión de constitucionalidad de artículo 3, literal c), la Corte Constitucional declaró constitucionalmente exequible, mediante Sentencia C-1011-08, «en el entendido que el operador es responsable a partir de la recepción del dato suministrado por la fuente, por el incumplimiento de los deberes de diligencia y cuidado en relación con la calidad de la información personal, consagrados en esta Ley Estatutaria».

Los titulares de los datos o la información, entre otros derechos reconocidos por el proyecto de ley de 2006-2007, tendrán los siguientes derechos frente a los operadores de los bancos de datos: (i) ejercer el derecho fundamental al habeas data en los términos de la presente ley, mediante la utilización de los procedimientos de consultas o reclamos, sin perjuicio de los demás mecanismos constitucionales y legales; (ii) solicitar el respeto y la protección de los demás derechos constitucionales o legales, así como de las demás disposiciones de la presente ley, mediante la utilización del procedimiento de reclamos y peticiones; (iii) solicitar prueba de la certificación de la existencia de la autorización expedida por la fuente o por el usuario; (iv) solicitar información acerca de los usuarios autorizados para obtener información. En idéntica forma se plasmó en la Ley 1266 de 2008 en el artículo 6º, sobre los derechos de los titulares de la información.

Se aclara sobre estos derechos que (i) la administración de información pública no requiere autorización del titular de los datos, pero se sujeta al cumplimiento de los principios de la administración de datos personales y proyecto de ley; y (ii) la administración de datos semiprivados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero y crediticio, el cual no requiere autorización del titular. En todo caso, la administración de datos semiprivados y privados se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de ley. Estas aclaraciones quedaron plasmadas en el parágrafo único del artículo 6º de la Ley de Habeas Data.

3.1 Fuentes de Información y fuente-operadores de información financiera. El artículo 3, literal j, de la Ley de Protección de datos personales de España, como norma integral del habeas data, se ocupa, igual que la LPDA argentina de 2000, principalmente por determinar las fuentes accesibles al público, las cuales las denomina como

> *aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas*

> *pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación*.

En cambio, el proyecto de Ley Estatutaria colombiana del Habeas Data de 2006-2007, enfatiza en el concepto de fuente de información de carácter financiero, bien si actúa como tal o lo hace en forma sui géneris, como fuente-operador. En efecto, según el literal b, del artículo 3º del proyecto, se entiende como Fuente de información,

> *… la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos*.

Idéntico concepto quedó plasmado en la Ley 1266 de 2008, artículo 3, literal b.

Según el proyecto de Ley Estatutaria colombiana de Habeas Data 2006-2007, el titular de los datos personales tiene los siguientes derechos frente a las fuentes de información: (i) ejercer los derechos fundamentales al habeas data y de petición, cuyo cumplimiento se podrá realizar a través de los operadores, conforme lo previsto en los procedimientos de consultas y reclamos de esta ley, sin perjuicio de los demás mecanismos constitucionales o legales; (ii) solicitar información o pedir la actualización o rectificación de los datos contenidos en la base de datos, lo cual realizará el operador, con base en la información aportada por la fuente, conforme se establece en el procedimiento para consultas, reclamos y peticiones; y (iii) solicitar prueba de la autorización, cuando dicha autorización sea requerida conforme lo previsto en la presente ley. Estas derechos de idéntico tenor quedaron plasmados en el artículo 6º, numeral 2, de la Ley de Habeas Data colombiana.

3.2 Las agencias de información comercial. Excepciones normativas. En el literal i) del artículo 3º del proyecto de ley Estatutaria colombiana de 2006-2007, define a la Agencia de Información Comercial como

> *toda empresa legalmente constituida que tenga como actividad principal la recolección, validación y procesamiento de información comercial sobre las empresas y comerciantes específicamente solicitadas por sus clientes, entendiéndose por información comercial aquella información histórica y actual relativa a la situación financiera, patrimonial, de mercado, administrativa, operativa, sobre el cumplimiento de obligaciones y demás información relevante para analizar la situación integral de una empresa. Para los efectos de la presente ley, las agencias de información comercial son operadores de información y fuentes de información*.

En el parágrafo de la norma citada, el proyecto de ley aclara que a las agencias de información comercial, así como a sus fuentes o usuarios no se les aplicará lo siguiente: 1. Los deberes que tienen las fuentes de la información, siguientes: ((i) reportar, de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada; y (ii) informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma, con el fin de que el operador incluya en el banco de datos una mención en ese sentido hasta que se haya finalizado dicho trámite. 2. Lo relativo a la permanencia de la información, previsto en el artículo 13 del proyecto de ley; y 3. Lo referente al acceso a la información por parte de los usuarios, establecido en el artículo 15 del proyecto de ley.

Tanto la definición de *agencia de información comercial*, como las aclaraciones previstas en el parágrafo quedaron plasmadas en el artículo 3º, literal j, de la Ley colombiana de Habeas Data, no sin la breve explicación.

En efecto, como se dijo antes, la Corte Constitucional en Sentencia C-1011-2008, declaró condicionalmente exequible el literal c, del artículo 3º referido a los operadores de la información, pero declaró inexequible el aparte del literal j, que sostiene: *así como la información relativa a las demás actividades propias del sector financiero o sobre el manejo financiero o los estados financieros del titular*, contenida en el literal j) del artículo 3º del Proyecto de Ley Estatutaria

3.3 Los usuarios de la información. En particular, usuario-fuente. La LPDA de 2000, define al usuario de la información, como la *persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos*.

La Directiva Comunitaria No. 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación

de estos datos, entre las definiciones que incluye no regula al usuario de la información, sino a los destinatarios de la misma, porque entiende que este puede ser una persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. Aclara la directiva, que las autoridades que reciban una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios.

En el proyecto de Ley Estatutaria colombiana nº 064 de 2003, en el extenso catálogo de definiciones, sostiene que el usuario o destinatario de la información, es *toda persona a quien se suministra la información contenida en un banco de datos o central de información, debidamente autorizada por el titular*.

Por su parte, el proyecto de Ley Estatutaria colombiana de 2006-2007, sostiene que *usuario*, sin más, es

> *la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos*.

En el fondo, esta definición de usuario se apega al texto concreto y explicativo que traía la Directiva Comunitaria europea sobre los destinatarios de la información, el cual tenía derecho a la fase de comunicación de los datos, es decir, al acceso de la información. Sin embargo, el proyecto establece una connotación especial y por su puesto un régimen igualmente especial para los que denomina usuario-fuente.

El proyecto de ley regula los derechos que tiene el titular de los datos frente a los usuarios de la información, en general, así: (i) solicitar información sobre la utilización que el usuario le está dando a la información, cuando dicha información no hubiere sido suministrada por el operador; y (ii) solicitar prueba de la autorización, cuando ella sea requerida conforme lo previsto en proyecto de ley.

Además, los titulares de información financiera y crediticia tendrán los siguientes derechos frente a los usuarios de la información: (i) podrán acudir ante la autoridad de vigilancia para presentar quejas contra las fuentes, operadores o usuarios por violación de las normas sobre administración de la información financiera y crediticia; y, (ii) pueden acudir ante la autoridad de vigilancia para pretender que

se ordene a un operador o fuente la corrección o actualización de sus datos personales, cuando ello sea procedente conforme lo establecido en la ley.

Tanto la definición de usuarios, como los derechos de los usuarios en general, como aquellos que lo son de la información financiera y crediticia, quedaron plasmados con idéntico tenor en el artículo 3º, literal d, y 6º, numeral 3 y parágrafo, respectivamente.

4. En el ámbito latinoamericano: datos o Informaciones personales. Diversa protección según la clasificación de los datos

En el derecho latinoamericano, la definición de datos personales no solo se predica de las personas naturales sino también de las personas jurídicas. En la LPDA de 2000, los datos personales constituyen: *la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables*, es decir, que incluye la información generada por las personas jurídicas, morales o de existencia ideal.

En casi todas las leyes de protección de datos (Argentina), de protección a la vida privada (Chile), de acceso a la información pública y de transparencia de la gestión pública (Honduras), de protección al dato financiero (Uruguay); entre otras, contiene definiciones: sobre los datos o informaciones personales, similares a las que trae la LPDA de 2000, la cual a su vez, retoma la definición y los parámetros conceptuales del derecho europeo. Por eso la definición de la LOPD es prototípica.

Así mismo, la LPDA clasifica a los datos personales generales o simplemente datos personales y a los datos sensibles o pertenecientes al núcleo duro de la intimidad. Estos últimos se definen como aquellos *datos personales que revelan origen racial o étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual*.

En idéntico sentido regula la definición de datos sensibles la Ley chilena nº 19.628 de 28 de agosto de 1998, sobre protección a la vida privada o protección de los datos de carácter personal, y la Ley nº 17938 de 1 de octubre de 2004 o *Ley de protección de datos personales para ser utilizados en informes comerciales y el habeas data* del Uruguay.

5. En algunos proyectos de ley estatutaria y en la Ley 1266 de 2008 sobre habeas data en el derecho colombiano

En los primeros proyectos de leyes estatutarias del habeas data integral, general o en la mayoría de las veces de carácter sectorial (hacia el dato financiero), posterior

a 1995, se ha incluido en el capítulo definiciones atinentes a los datos personales y los datos sensibles, siguiendo los cuadros normativos latinoamericanos, ya que en el derecho continental europeo, los datos sensibles son una categoría de datos surgida en los tratados o estudios doctrinarios de los juristas, más que en la plasmación de textos normativos, como hemos visto. A partir de 2002 y hasta junio de 2007, en los proyectos de ley estatutaria, además de las definiciones de datos personales y datos sensibles, se aumentaron otras tales como: dato negativo, dato público, dato privado y dato semiprivado que más adelante precisaremos.

Así, por ejemplo, en el Proyecto de Ley estatutaria acumulado 201 de Cámara, 071 de 2002 de Senado, *Por la cual se regula integralmente el derecho fundamental al habeas data y demás libertades y derechos fundamentales de las personas en lo que respecta al tratamiento de sus datos personales a través de bases de datos públicas y privadas, y se dictan otras disposiciones*[10], los ponentes introducen una definición de dato personal, ampliada a la del derecho europeo y el latinoamericano, al afirmar que este es *toda información relativa a personas físicas, jurídicas o de hecho que de cualquier manera sea idóneo para permitir, directa o indirectamente, su identificación tales como, entre otros, los nombres y apellidos, los números de identificación personal, los datos financieros, tributarios o de solvencia patrimonial o crediticia*. Se amplía en la cobertura de aplicación de la definición, pues se entiende a las personas de hecho y se incluye aspectos de identificación de las personas humanas y jurídicas, de derecho público o de derecho privado.

También por inclusión de los ponentes, se define al *dato sensible*, como *aquel dato personal cuyo contenido involucra riesgos de prácticas discriminatorias por razones raciales y étnicas, opiniones políticas, convicciones religiosas, filosóficas o morales, la afiliación sindical, informaciones relacionadas con la salud, la vida sexual o cualquier otra circunstancia similar de carácter personal o social*. Y agrega en el inciso 2º: *La recolección, almacenamiento, procesamiento, tratamiento, uso y suministro del dato sensible requerirá del consentimiento expreso, previo y escrito de su titular*.

El dato o información sensible, como prefiere denominarla el proyecto, le asigna un plus de protección frente a los demás datos o informaciones personales. Este plus de protección está previsto en los artículos 4º y 27º así: (i) se requiere el consentimiento, previo y escrito del titular del dato, si por excepción es sometido a tratamiento o procesamiento de datos; (ii) nadie está obligado a proporcionar datos

[10] El título del proyecto original era: por la cual se regula el derecho de acceso a la información de interés público, en particular la de carácter comercial, financiero, la que tiene que ver con el cumplimiento de obligaciones fiscales y parafiscales y con el pago de servicios públicos domiciliarios, y se dictan otras disposiciones. (Pliego de modificaciones al proyecto de ley Estatutaria 201 de 2003 y 071 de 2002 Senado. Ponentes del proyecto acumulado: Vid. Hernández, J. & Vargas, J.).

sensibles; (iii) sin consentimiento pueden ser sometidos a tratamiento de datos, cuando medien razones de interés general autorizados por ley o cuando se persiga finalidades estadísticas o científicas y no puedan ser identificados sus titulares; y, (iii) queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revelen la identidad del titular de los datos sensibles. Sin perjuicio de ello, las iglesias, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

Por su parte, el proyecto de Ley Estatutaria del Habeas Data nº 064 de 2003, a instancia de la Defensoría del Pueblo, en el artículo 5º, amplía aún más la definición del anterior proyecto, al sostener que dato personal es *toda información relativa a personas físicas, jurídicas o de hecho que de cualquier manera sea idónea para permitir, directa o indirectamente, su identificación, tal como el nombre y apellidos, número de identificación personal, voz e imagen, o datos financieros, tributarios o de solvencia patrimonial y crediticia*. La amplía en los identificadores de las personas físicas o naturales: voz e imagen; y la mantiene en los de las personas jurídicas y de hecho.

En cuanto al dato sensible, en el numeral 7 del artículo citado, lo define como *aquel dato referido al origen racial o étnico, las opiniones políticas o filosóficas, las convicciones religiosas, la pertenencia a sindicatos o relativos a la salud o la sexualidad de una persona, cuyo tratamiento está proscrito por involucrar riesgo de prácticas discriminatorias*. En esencia, esta mantiene la definición del proyecto anterior, pero se mejora en la redacción de la norma. El inciso 2º conserva la esencia del consentimiento del titular con el nombre de autorización del titular de los datos, al decir: *La recolección, registro, almacenamiento, procesamiento, tratamiento, uso y suministro del dato sensible sólo se hará en los casos y para los fines previstos en esta ley*.

El dato sensible sigue siendo ultra protegido en todas las fases del tratamiento o procesamiento de datos personales, al punto que esta práctica se prohíbe por regla general (art. 34) y solo por excepción se permite, cuando el titular de los mismos otorga *autorización* (previa y escrita) solamente *para el tratamiento con fines históricos, científicos, estadísticos u otros de interés general previstos de forma expresa en la ley*. Se refuerza, cuando dice: ninguna persona está obligada a proporcionar datos sensibles (art. 67), salvo que *medien razones de interés general autorizadas por la ley* o para los fines anteriormente relacionados.

En el proyecto de Ley Estatutaria del Habeas Data 071 de la Cámara de 2005, que quizá sea uno de los más prolíficos en definiciones que se haya presentado al Congreso, no solo suministra definiciones técnico-jurídicas aplicables al habeas data, sino que las clasifica. Así, dentro de las definiciones en relación con la

clasificación de los datos según su naturaleza incluye: el dato personal, el dato público, el dato privado, el dato semiprivado y el dato íntimo, y en otras clasificaciones: dato y registro individual.

Define como *dato personal,*

> *cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uno personal. Los datos personales pueden ser públicos, semiprivados o privados*.

De esta definición se infieren las suministradas por separado como dato y registro individual, por lo cual se consideran innecesarias tales definiciones[11]. Ahora bien, se maneja una definición amplísima de dato personal cuando se hace referencia a cualquier pieza de información, aun cuando luego se refiera a la presunción que puede ser desvirtuada de dato solo referido a lo personal, pues si lo que se quería expresar es que la información, como se sostuvo anteriormente, se concreta desde una manifestación informática binaria hasta un dato escrito o electrónico, auditivo, visual, audiovisual o telemático, estos no son piezas sino medios de crear, conseguir o recuperar información. Hoy conocemos medios escritos o tradicionales y *medios electrónicos, telemáticos o informáticos*[12]. En tal virtud, es universalmente entendible la definición que inicie sosteniendo *cualquier información...* referida a la persona física o jurídica.

El proyecto de ley distingue entre dato sensible y dato íntimo, por vez primera para esta clase de normas, no solo en el ámbito europeo, sino en el Latinoamericano. En efecto, al dato sensible lo define como *aquel dato personal que puede potencialmente ser utilizado para discriminar a las personas, como es el relativo a la raza, la*

---

[11] En el numeral 17 se manifiesta: Dato: Es toda pieza individual de información contenida en los bancos de datos y en el numeral 19, Registro individual: Se refiere al conjunto de datos contenido en una base de datos relativo a un único titular de la información.

[12] Los medios escritos, documentales o tradicionales, son todos aquellos mediante los cuales se elabora, crea, modifica, archiva, procesa o destruye todo tipo de información no solo concerniente a las personas humanas o jurídicas, sino la referente a hechos, circunstancias, eventos no personales. En cambio, los medios electrónicos, telemáticos o informáticos, son aquellos mediante los cuales se trata o procesa información electrónica, con apoyo de las nuevas tecnologías de la información y la comunicación (TIC) y a través de software (programas de computador), hardware (equipos computacionales) y diversos elementos electro-magnéticos (Discos fijos y movibles, Discos compactos: CD, DVD, DI, etc., Disquetes; entre muchos otros.). El procesamiento electrónico de datos produce documentos electrónicos (EDI); bancos, bases, ficheros o registros electrónicos de datos de todo tipo, incluidos los bancos de datos personales, objeto y finalidad de leyes y proyectos de ley del Habeas Data. (Riascos, 1999, p. 286 y 505)

ideología o la orientación sexual. Reduce, con relación a los anteriores proyectos de ley e incluso en lo pertinente a las legislaciones europeas y latinoamericanas, de forma significativa, el contenido del concepto de dato sensible a tres aspectos que pueden discriminar a la persona: la raza, la ideología o la vida sexual.

El dato íntimo, se considera *el dato que, por su contenido o su naturaleza, las personas habitualmente prefieren mantenerlo en reserva y su conocimiento por parte de terceros no representa un interés general legítimo, como es el referido a los hábitos personales o a la vida familiar*. Podría decirse que estos son los datos del círculo profundo de la vida privada a los que solo llega la misma persona y no representan alguna importancia o interés sino para su titular. Pese a que puede ser asimilable teóricamente al dato íntimo, es difícil distinguirlo de un dato anodino o superfluo para las demás personas, pero para su titular de gran importancia y susceptible de tutela jurídica por el Estado. Por eso decíamos *ut supra* que en un dato anodino se puede esconder un dato personal o familiar, o viceversa y en ese hilo delgado de distinción se pueden cometer serias injusticias o desprotección estatal del derecho a la intimidad, al honor, al buen nombre, a la imagen.

Por esto se considera innecesaria e inconveniente la definición suministrada. Sin embargo, el proyecto de ley para definir el dato privado toma como base las definiciones de dato sensible y dato íntimo. Sobre este aspecto más adelante profundizaremos.

Finalmente, el proyecto de Ley Estatutaria nº 221/2007 de Cámara y nº 027/2006 de Senado, acumulado con el nº 05/2006 Senado, por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios y se dictan otras disposiciones, en el artículo 3º relaciona unas definiciones técnico-jurídicas aplicables al tratamiento o procesamiento de datos personales informatizados o no y en particular a las facultades o componentes del habeas data, con énfasis financiero.

Este proyecto, al igual que los anteriores, prosigue con la distinción entre dato personal, dato público, dato semiprivado y privado, elimina la definición de dato íntimo y agrega la que llama *Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países*. Concordantemente con esto último, el catálogo de definiciones comienza con explicar qué debe entenderse por titular de la información, y al efecto, dice: «Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de habeas data y demás derechos y garantías a que se refiere la presente ley».

El dato personal, según el literal e, del artículo 3º del proyecto, es *cualquier pieza de información vinculada a una o varias personas determinadas o determinables o*

que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semi-privados [sic] *o privados*.

La presente definición mantiene los elementos suministrados en el proyecto 071 de 2005, y, por tanto, son válidas para esta las observaciones hechas anteriormente para este proyecto.

Sobra haberse reiterado en la definición que no tienen sujeción al régimen jurídico del presente proyecto de ley estatutaria, los datos impersonales o no atribuibles a una persona determinada, o según el diccionario que *no se aplica a nadie en particular*, pues según el intitulado y en el contexto del proyecto se dice que la ley que rige para los datos personales o de la persona física o jurídica determinada o determinable. Estos datos impersonales tal como están excluidos de regulación podrían confundirse con los datos personales que han sido sometidos a procedimiento de disociación, de manera que la información que se obtiene no puede asociarse a una persona determinada o determinable. Estos datos disociados son objeto de regulación por parte de la LOPDP española de 1999, los datos disociados a efectos de la comunicación (circulación, transferencia o cesión) de los datos son perfectamente posibles sin necesidad de consentimiento y sin la previsión de derechos de cedente y cesionario (artículo 11º).

Por otra parte, parecería que no es dato personal la *Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países*, que el proyecto de ley define en el literal j), del artículo 3º. Parecería, decimos, porque *a renglón seguido de definir el dato personal dice que pueden ser públicos, semi-privados* [*sic*] *o privados* y excluye a propósito la información o datos financieros. Sin embargo, al emplear el término *pueden*, se entiende que además de las mencionadas en dicha definición caben otras posibilidades como la que señalamos. Esto es de capital importancia para el proyecto de ley de habeas data sectorial, pues este hace énfasis en el dato financiero.

Esta subespecie de dato personal se define así:

> *información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, aquella referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen, así como la información relativa a las demás actividades propias del sector financiero o sobre el manejo financiero o los estados financieros del titular*.

5.1 El dato semiprivado. El Proyecto de Ley Estatutaria nº 221/2007 de Cámara y nº 027/2006 de Senado, acumulado con el nº 05/2006 Senado, define al dato semiprivado, en el artículo 5º, literal g, como aquel dato que *no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios*.…

Se define esta clase de datos por deducción lógica de lo que no es y con el ejemplo aparentemente único del dato financiero que incluye al dato comercial, bancario, bursátil, tributario, fiscal o tarifario, como hemos sostenido anteriormente. Esta clasificación parecería estar mal, informando al operador jurídico de la norma que es una especie de dato personal sui generis del cual es propietario su titular, pero no solo le interesa a él sino a cierto sector o grupo de personas o a la sociedad en general, es decir, a todo el mundo, pero tan solo un poquito a él que paradójicamente es su titular concernido. Lo que no parece bien es que la norma, al igual que lo hacía el centenario Código Civil colombiano, explica las normas con ejemplos o casos ejemplarizantes (casuística). Esa técnica legislativa casi cerrada conlleva una pobre aplicabilidad general a diversos sucesos o eventos a los cuales podría estar dirigida.

En el proyecto de Ley Estatutaria nº 071 de 2005, se denominaba al dato semiprivado en la forma que lo hizo en el anterior proyecto, con la pequeña gran diferencia, que al final de la definición incorporaba aquello que en buena hora se eliminó en 2006-2007, es decir, que no se requería de autorización del titular para tratar o procesar esta especie de datos personales.

5.2 Dato privado. El proyecto de Ley Estatutaria nº 071 de 2005, define *dato* en el artículo 5º, numeral 14, como aquel *dato que por su contenido o su naturaleza sólo es relevante para el titular y no puede ser suministrado a terceros o usuarios, sino con su previa autorización. Son datos privados los datos sensibles y los datos íntimos. No podrá divulgarse o suministrarse un dato privado sin el consentimiento previo del titular, salvo las excepciones previstas en la ley*.

Esta calificación de dato privado encierra dos categorías especiales de datos, que en el derecho continental europeo, como se dijo antes, tiene una protección reforzada porque implica, ni más ni menos, los datos del famoso núcleo duro de la *privacy* anglosajona y por tanto, susceptible de máxima protección por parte del Estado. Así lo entendió el proyecto de ley de 2005, al imponer como requisito fundamental para tratar estos datos, el consentimiento o autorización previa, expresa y escrita del concernido, sobre todo cuando se somete el dato a la fase de comunicación a terceros o usuarios.

Por su parte, el Proyecto de Ley Estatutaria nº 221/2007 de Cámara y nº 027/2006 de Senado, acumulado con el nº 05/2006 Senado, en forma aparentemente simple define en el artículo 5º, literal h, el dato privado como aquel *que por su naturaleza íntima o reservada solo es relevante para el titular*. Es aparente, porque aunque elimina la calidad de dato sensible al privado le otorga otro candado de mayor seguridad que este, cual es denominarlo como dato reservado. Y son la Constitución y las leyes especiales, como la Ley 57 de 1985, las que califican qué es o no información reservada. Por ejemplo, las investigaciones penales, las historias clínicas o médicas de una persona, etc.

Solo para ver hasta donde se extiende el concepto de dato privado, digamos lo siguiente:

Un ser humano desde antes de nacer, luego con su nacimiento, crecimiento, desarrollo, muerte, y aún después de esta, produce una serie de actos, hechos, sucesos, susceptibles de documentación (certificados de cualquier tipo y finalidad, registros públicos y privados, obligaciones y contratos, etc.); en fin, de informaciones y datos personales, familiares y sociales, los cuales, en mayor o menor grado, son sujeto u objeto del derecho y en mayores proporciones de la vida cotidiana, al ser puros y simples y reveladores de la venida, paso y extinción de la *vitae humanum*.

El estatus del *nasciturus* de la persona natural o física y el del *post mortem* en el derecho, genera gran cantidad de información o datos de carácter personal y familiar, tanto escritos, gráficos, auditivos, vídeo auditivos, como producidos, captados, reproducidos, transferidos o consultados por cualquier medio, dispositivo, aparato mecánico, eléctrico o electromagnético conocido o conocible, muchos de los cuales tienen relevancia en el derecho, dependiendo de diferentes variables que van desde las estrictamente biológicas (v.gr .nacimiento), pasando por las simplemente materiales u objetivas hasta las más sofisticadas que actualmente se conocen, cuando crean, modifican o extinguen situaciones jurídicas individuales o concretas, o generales y abstractas, produciendo derechos, deberes y obligaciones para una persona. Una auscultación médica mediante la técnica de rayos X o cualquiera otra de índole computarizada (por ejemplo, TAC) o de examen de líquidos humanos (orina, sangre, semen, etc.) o incluso de partes del cuerpo humano (como huellas digitales o plantares); cualquier número o símbolo que identifique o se le asigne a una persona (documento de identidad personal, profesional, documento de conducción, etc.); la información sobre la raza, origen étnico, color, religión, edad o estado civil o sobre la educación, su historial laboral, delictivo, incluso las ideas u opiniones personales sobre otra persona, salvo las vertidas con ocasión de un concurso, premio o subvención según la *Act Privacy Canadiense*; entre muchas otras relacionadas en un gran listado que no distingue categorías especiales entre aquellas, constituyen información personal, entendiendo como tal, la que le concierne

a una persona, cualesquiera sean los mecanismos o tecnologías de las que se obtengan o graben.

5.3 Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Según el literal j, del Proyecto de Ley Estatutaria nº 221/2007 de Cámara y nº 027/2006 de Senado, acumulado con el nº 05/2006 Senado,

> *se entenderá por información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, aquella referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen, así como la información relativa a las demás actividades propias del sector financiero o sobre el manejo financiero o los estados financieros del titular.*

Las definiciones de datos personales como las de dato público, privado y semiprivado, quedaron plasmadas en la Ley 1266 de 2008, en el artículo 3º, literales *e, f, g* y *h*.

5.4 Actores del habeas data financiero. Según el artículo 3º de la Ley 1266 de 2008, relacionaremos lo que se entiende por titular de los datos, fuentes de información, operadores de centrales de datos, usuarios.

a) Titular de la información. Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de habeas data y demás derechos y garantías a que se refiere la presente ley.

b) Fuente de información. Es la persona, entidad u organización que ***recibe o conoce datos*** personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de ***autorización legal*** o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos.

c) Operador de información. Se denomina operador de información a la persona, entidad u organización ***que recibe de la fuente datos personales*** sobre varios titulares de la información, ***los administra y los pone en conocimiento de los usuarios*** bajo los parámetros de la presente ley. Por tanto el operador, en cuanto tiene acceso a

información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente.

5.5 Principios de administración de datos financieros. Según el artículo 4º de la Ley 1266 de 2008, en los principios que rigen la administración de los datos, es decir, en el desarrollo, interpretación y aplicación de la presente ley, se tendrán en cuenta, de manera armónica e integral, los principios que a continuación se establecen:

a) Principio de veracidad o calidad de los registros o datos. La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error.

b) Principio de finalidad. La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto.

c) Principio de circulación restringida. La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos.

Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o los usuarios autorizados conforme a la presente ley.

d) Principio de temporalidad de la información. La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos.

e) Principio de interpretación integral de derechos constitucionales. La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el habeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de

los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables.

f) Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado.

g) Principio de confidencialidad. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

6. Tipos delictivos contra los datos personales y el habeas data

6.1 Acceso abusivo a un sistema informático

6.1.1 Fuente normativa. Artículo 269, literal a. El presente delito hacía parte del Título VII del Título X, del Código Penal del 2000, bajo el bien jurídico tutelado de la intimidad y la reserva en las comunicaciones. Sin embargo, mediante la Ley 1273 de 5 de enero de 2009, que reformó parcialmente el Código y creó el Titulo VII bis, intitulado *De los delitos contra la Información y los datos*, traspuso el artículo 195 al artículo 269, literal a, aunque algunos juristas interpretaron que se había derogado por dicha ley y nuevamente creado bajo el nuevo bien jurídico protegido.

La trasposición de tipos penales es una forma que utiliza el legislador para reubicar tipos que en su momento considera no están correctamente ubicados bajo dicho bien jurídico protegido y espera que bajo el nuevo que se ubique adquiera mayor potencialidad en la protección del bien jurídico y mayor punibilidad porque atenta a un bien jurídico más sensible.

También se aplican en este tipo penal básico las siguientes normas: (i) ley 1266 de 2008, o ley de habeas data. Conceptualización, entre otros términos del habeas data, titular de la información, dato personal, dato público, dato privado, dato semiprivado, usuario, fuente de información, agencia de información comercial, autoridades de vigilancia de los datos económicos, Superintendencia Financiera y

Superintendencia de Industria y Comercio, habeas data administrativo y habeas data jurisdiccional.

(ii) Convenio de Budapest del Consejo de Europa de 23 de diciembre de 2001, sobre ciberdelincuencia, sobre conceptualizaciones de sistema informático, datos informáticos, proveedor de servicios, datos sobre el tráfico. Además, sobre acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema, abuso de los dispositivos. Sobre los delitos informáticos en particular: falsificación informática, delitos de relación con el contenido, delitos relacionados con infracciones de la propiedad intelectual y de derechos afines, entre otros. Se relacionan también aspectos procesales, conservación rápida de datos informáticos almacenados, conservación y revelación parcial rápidas de datos sobre el tráfico, registro y confiscación de datos informáticos, obtención en tiempo real de datos informáticos, etc. Sobre cooperación internacional: principios generales: (i) relativos a la extradición, (ii) asistencia mutua, y (iii) información espontánea. Finalmente, sobre procedimiento relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.

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

6.1.3 Sujeto activo. El tipo penal acceso abusivo a un sistema informático no requiere cualificación del agente, por lo que puede ser sujeto comisivo del delito un particular o un servidor del Estado. Sin embargo, si se comente por un funcionario estatal, el tipo se agrava de conformidad con el artículo 269H-2 del Código Penal.

Hay que aclarar que estos ilícitos pueden ser cometidos por cualquier persona particular o por un usuario, en términos de la Ley 1266 de 2008 o Ley de Habeas Data. Usuario que lo haría sin el consentimiento del titular del dato o violando la medidas de seguridad de los datos adoptados por el operador de la información o el fuente-operador de la misma, no solo la clave de acceso (password) sino los elementos de seguridad interna del *software* o *hardware*, respectivamente.

Usuario, en términos de la ley, es

> *aquella persona natural o jurídica que, en los términos y circunstancias previstas en la ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por*

el titular de la información. El usuario en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En caso en que el usuario a su vez entregue la información directamente al operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos.

Por su parte, el Convenio de Budapest de 23 de diciembre de 2001, manifiesta que se entenderá por proveedor de servicios: (i) toda persona pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y (ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio.

El sujeto pasivo en esta clase de conductas es el Estado, pero también lo podrán ser las personas jurídicas o privadas que operen, administren o coordinen un sistema informático o base de datos cualquiera sea su finalidad, perfil o clase de banco de datos.

6.1.4 Conceptualizaciones necesarias para entender el tipo penal

En la conducta penal sobre conceptualizaciones tomaremos como norma extrapenal la Ley 1266 de 2008 o Ley de habeas data financiero y la terminología provista por el Convenio de Budapest de 2001, como referente doctrinal, al no haberse incorporado al derecho interno colombiano mediante ley.

En efecto, dato personal *es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica* (artículo 3, literal e, de la Ley de Habeas Data). Ahora bien, si ese dato personal ingresa a un tratamiento o sistema informático, se convertirá en dato informático. El Convenio de Budapest de 2001, en su artículo 1º define a los datos informáticos, como *cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado que un sistema informático ejecute una función.*

Las propuestas legislativas que cursaban en el Senado de la República —previas a la Ley 1273 de 2009 que adicionó el Código Penal con el título VII bis e incluyó nueve conductas delictivas y trasladó a este título denominado *de los delitos contra la información y los datos*, el acceso abusivo a un sistema informático—, traían un artículo 1º dedicado a las definiciones técnicas y relativas a los medios TIC que se utilizan en los artículos 269 literal a, a 269, literal i, y que ayudaban a la comprensión terminológica de cada conducta penal en el trámite final de la Ley 1273, que fue eliminado, entendiendo equívocamente que esa labor pertenecía a la Corte

Constitucional o a los tribunales y jueces en el momento de aplicabilidad de la norma específica. Aunque eso es parcialmente cierto, no debemos olvidar que en nuestro país, respecto del fenómeno informático, electrónico y telemático, muy poco se ha reglamentado con carácter ius civilista o administrativista o de *prima ratio* en donde se expliquen los varios términos tecnológicos TIC utilizados en las normas y se aplique una legislación pedagógica, preventiva y civilista a los variados casos permeados por las nuevas tecnologías de la comunicación y la información, así cuando esta no funcione o funcione indebidamente, se llega a una legislación penal o de *ultima ratio* y no al contrario, como está sucediendo actualmente al leer la Ley 1273 de 2009.

Pues bien, uno de tantos proyectos de ley previos a la ley 1273, definía como ***sistema informático*** *todo dispositivo aislado o conjunto de conectores interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa de ordenador*.

Mediante un sistema informático se pueden almacenar, procesar, registrar o transmitir datos personales o informáticos, bien sea que se encuentren en un mismo o en diferentes sitios geográficos, pues el sistema involucra *software* y *hardware* que permite desde almacenar hasta transmitir información datos, sean estos informáticos, electrónicos o telemáticos. Un sistema informático podría estar interconectado a otro sistema informático, según las posibilidades de interconexión facilitadas por los diferentes dispositivos y que la tecnología lo permita o viabilice.

Esto significa que en un sistema informático puede presentarse un acceso ilegal total o un acceso ilegal parcial, siempre que se vulnere una medida de seguridad, una contraseña, *password* (palabra o frase secreta de acceso a un sistema o base de datos) o clave de acceso, o bien se vulnere el acceso a una base o banco de datos.

6.1.5 Bien jurídico tutelado. La Ley 1273 de 2009, de 5 de enero, adicionó el Código Penal del 2000 con el *Título VII bis* denominado *de la protección de la Información y de los datos*, que constituye a su vez, el bien jurídico protegido en este aparte del Código Penal. El Título está conformado por dos capítulos, a saber: (i) de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; y (ii) de los atentados informáticos y otras infracciones. Cada uno de los cuales contiene varias conductas delictivas.

El delito de acceso abusivo a un sistema informático (artículo 269 A), pertenece al primer grupo de conductas delictivas y atenta a la confidencialidad de la información (el secreto o sigilo de la información) puesto que las actividades dolosas, ya que no admite formas culposas, van dirigidas al acceso ilegal o ilegítimo de los datos, la información o un sistema informático, en una primera acción instantánea, o bien a

mantenerse dentro de un sistema informático contra la voluntad de su legítimo usuario del sistema o titular de los datos.

Antes de la adición del Código Penal de 2000, la conducta delictiva de acceso abusivo a un sistema informático se hallaba localizada bajo el bien jurídico protegido de la Intimidad, el secreto a la correspondencia y las comunicaciones en el artículo 195 con una redacción parecida a la del artículo 269 A, pero se diferenciaba principalmente en lo siguiente: no especificaba cómo y de qué forma se podía acceder a un sistema informático, si era o no con autorización (aunque esto está implícito en la conducta penal, pues si es con autorización deviene la atipicidad del delito), y la sanción era apenas de multa, lo cual no se compadecía con la insidiosidad del tipo.

El artículo 195 del Código Penal del 2000, manifestaba: *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*.

El artículo 2º de la Ley 1273 de 2009, derogó expresamente el artículo 195 y en su lugar trasladó su contenido esencial del tipo al artículo 269 A, bajo el bien jurídico de la información y los datos personales, tal como se lo ha transcrito anteriormente.

Mediante la Ley 1288 de 2009 de 25 de marzo, el Congreso de la República modificó algunas penas para varios delitos del Código Penal del 2000. En efecto, en el artículo 25 se modificó la pena de multa del artículo 195, delito de acceso abusivo a un sistema informático, por pena de prisión de cinco (5) a ocho (8) años, puesto que al dictarse dicha ley perseguía *fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones*. El Capítulo V de dicha ley regula todo lo atinente a la *reserva de información en inteligencia y contrainteligencia* de los organismos del Estado que llevan a cabo dichas actividades. Según el artículo 3º de la mentada ley, son:

> *las dependencias de las Fuerzas Militares y la Policía Nacional reglamentados por estas para tal fin; el Departamento Administrativo de Seguridad (DAS) y la Unidad de Información y Análisis Financiero (UIAF). Estos cumplen su función a través de operaciones básicas y especializadas, utilizando medios humanos o técnicos. Estos organismos conforman la comunidad de inteligencia y son los únicos autorizados para desarrollar labores de inteligencia y contrainteligencia en el ámbito de la seguridad y la defensa nacional.*

En tal virtud, al modificar esta ley un tipo penal que estaba derogado previamente por la Ley 1273 de 2009, queda vigente el artículo 269 A, que de alguna forma

había mejorado la redacción del artículo 195 y había establecido una sanción más acorde con el nivel de *insidiosidad* estructurado en el tipo, pues la sanción pasó de multa a *prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 SMLMV*.

En tan pocos años de existencia de la conducta delictiva, el tipo penal ha cambiado de bien jurídico protegido, tanto solo por la ubicación probablemente más acorde con los denominados doctrinalmente delitos informáticos contra la información y los datos personales que por una de las tantas formas de vulnerar la intimidad de las personas o de la familia, a través de su visión iusinformática, como ut supra explicábamos.

6.1.6 La confidencialidad de la información. La Ley 1266 de 2008 o ley de habeas data, expone como principio fundamental de la administración de los datos personales el de confidencialidad, junto al de veracidad o calidad de los registros o datos, el de finalidad, de circulación restringida, temporalidad de la información, de interpretación integral de derechos constitucionales y el de seguridad.

Respecto a la confidencialidad, expresa que

> *todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma* (artículo 3º, literal g).

La confidencialidad, reserva o sigilo de la información es por lo tanto un principio rector en el acceso, procesamiento, manejo, administración y transmisión de datos personales. Constituye la regla general en el tratamiento informatizado (o automatizado) o no de la información perteneciente al ser humano que solo por excepción y bajo los apremios de ley, por autoridad competente (en nuestro país, la judicial) y para fines específicos (según el artículo 15 de la Constitución colombiana, para adquirir pruebas judiciales, para tasación tributaria e intervención estatal) podrá excepcionar dicha confidencialidad.

La docente universitaria Castro Ospina (2002, 15 de julio), al explicar las razones que le asisten para defender la postura del bien jurídico protegido de *la Información* por el Código Penal de 2000, sostiene que la confidencialidad... *en nuestra sociedad moderna, (en) la comunidad tiene derecho a la privacidad de los datos atinentes a la vida personal de sus miembros; a las estrategias comerciales, publicitarias o*

mercantiles; a los secretos industriales; y a las comunicaciones; entre otras. Este derecho se traduce en un sentimiento de seguridad y de tranquilidad en la convivencia social. Con lo cual hoy en día, la información de las personas o los datos del ser humano individual o familiarmente considerado en el mundo actual y en sus diferentes facetas del quehacer social, laboral, empresarial, educativo, profesional, etc., está permeada por el principio universal de la confidencialidad en aras de una convivencia pacífica, segura y alta civilidad.

La autora citada, dentro de un largo listado de conductas que lesionan la confidencialidad de la información, siguiendo al tratadista Reyna Alfaro, expone las siguientes: **1)** ***El espionaje informático*** (industrial y comercial) y dentro de ellos las siguientes conductas: (i) *fuga de datos (Data leake),* (ii) *puertas falsas (Trap Doors),* (iii) *las llaves maestras (Superzapping)*, (iv) *el pinchazo de líneas (Wiretapping);* (v) *la apropiación de informaciones residuales (scavenging)*[13], y, (ii) *el intrusismo informático*, es decir, la mera introducción a sistemas de información o computadoras, infringiendo medidas de seguridad destinadas a proteger los datos contenidos en ellos. Precisamente este segundo tipo penal es el que el Código Penal reformado en 2009, denomina acceso abusivo a un sistema informático, pues nuestro Código Penal tiene reguladas las conductas integrantes al espionaje informático bajo otro bien jurídico protegido del Orden Económico social y en el delito de violación a la reserva industrial y comercial (artículo 308) y cuyos medios comisivos comprenderían los informáticos, electrónicos o telemáticos (artículo 58-17 C.P., circunstancias de mayor punibilidad. Adicionado por el artículo 2º de la Ley 1273 de 2009).

Sin embargo, varias de las conductas aplicadas al espionaje industrial y comercial son perfectamente válidas, no solo para ejemplificar el acceso abusivo a un sistema informático, sino para los demás tipos delictivos previstos en los artículos 269 B a 269 I, como anotaremos en su momento oportuno.

6.1.7 Nomen iuris universal. El acceso ilícito a un sistema informático, a una base, fichero o banco de datos en línea o fuera de ella, a un programa de computador

---

[13] ***El Espionaje informático***, debe entenderse, en términos de la doctrinante citada, con ánimo de lucro y sin autorización, de datos de valor para el tráfico económico de la industria o comercio dentro de los comportamientos que encajarían en esta descripción, han sido identificados los siguientes: ***fuga de datos (Data leake),*** que las empresas o entidades guardan en sus archivos informáticos; ***puertas falsas (Trap Doors),*** consistentes en acceder a un sistema informático a través de entradas diversas a las que se utilizan normalmente dentro de los programas; las ***llaves maestras (Superzapping)***, que implican el uso no autorizado de programas con la finalidad de modificar, destruir, copiar, insertar, utilizar o impedir el uso de los datos archivados en los sistemas de información; ***el pinchazo de líneas (Wiretapping),*** que se concreta en interferir las líneas telefónicas o telemáticas, mediante las cuales se transmiten las informaciones procesadas; ***la apropiación de informaciones residuales (scavenging),*** que consiste en la obtención de información a partir de lo que desechan los usuarios legítimos de un sistema informático.

(software) o un grupo de *interconectores* de información, ha sido considerado como un tipo básico de *intrusión informática*, aunque en los diferentes países afecte bienes jurídicos protegidos distintos**.** En efecto, en Colombia inicialmente afectaba la intimidad y la reserva de las comunicaciones (Ley 559 de 2000), y ahora al bien jurídico de la información y los datos (Ley 1273 de 2009). En España se ubica como un tipo penal que afecta la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (C.P. español de 1995).

El Convenio de Budapest de 2001, que rige para los Estados miembros de la UE, pero con claro ejemplo para el resto de Estados del mundo, regula el acceso ilícito a sistemas informáticos, ficheros o registros informáticos, en línea o fuera de esta, haciendo énfasis en que la figura delictiva tipificada en los ordenamientos internos debe considerar que esta puede cometerse bien *infringiendo medidas de seguridad (códigos, claves, contraseñas, filtros, etc.) con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático*

En la obra de Mitnick[14], nos muestra el mundo de los Hackers, que son aquellas personas que acceden, ingresan o actúan de forma intrusiva en los sistemas informáticos, bases o ficheros de datos en red o fuera de ella, y lo hacen por el solo hecho de transgredir las normas de seguridad informática y demostrarse a sí mismo y sobre todo a los demás que las medidas que impiden el ingreso a un extraño a un sistema de seguridad no es confiable, es altamente vulnerable y su fácil intrusión es casi un juego de niños. A esta clase de intrusos el autor los califica de *White Hacking*[15], por oposición diríamos nosotros a los *Black Hacking* que son aquellos intrusos en redes, sistemas o programas informáticos que además de buscar logros de envanecimiento personal van tras oscuras intenciones o con finalidades ilícitas, o provecho económico, financiero o de cualquier otro tipo en el que el intruso obtenga beneficio ilícito.

6.1.8 Verbos rectores alternativos (acceder-mantener). Conductas de ejecución instantánea y de permanencia

El acceso abusivo a un sistema informático previsto en el artículo 269 A del Código Penal, se entiende a todos aquellas acciones que no están incluidas en el artículo

---

[14] Mitnick, K. & Simon, W. L. (2007). Mitnick es uno de los Hackers más famosos de Estados Unidos, detenido varias veces por sus actividades intrusivas en los sistemas informáticos más seguros. En base a su vida se han hecho películas como ***Take down*** (2000) que relata su última detención en 1995 y su puesta en libertad en 2002. Actualmente Mitnick, como muchos otros Hackers, es reconvertido a ser consultor de compañías a quienes les ayuda a mejorar los sistemas de seguridad. Su compañía ***Mitnick Security*** anteriormente ***Defensive Thinking.***

[15] **Hacking:** procedimiento mediante el que se violan los códigos personales o el acceso a datos o sistemas informáticos sin autorización o conocimiento el titular.

257, referidas al acceso ilegal o prestación ilegal de los servicios de telecomunicaciones, al menos en su parte inicial relativa al acceso ilegal a los servicios de telecomunicaciones como los de telefonía móvil celular u otro servicio de comunicaciones. Este ilícito se encuentra el Título VII de los delitos contra el patrimonio económico, Capítulo VI, sobre las defraudaciones.

Como se dijo antes, el acceso ilícito a todo sistema informático incluye tanto los informáticos, electrónicos o telemáticos, y por supuesto la telefonía celular o fija se encuadraría dentro de los medios electrónicos. Sin embargo, el acceso ilegal que reprime el artículo 257 se refiere más a la intrusión en el servicio de telecomunicaciones con algún fin o provecho, que al acceso ilegal vulnerando medidas de seguridad por demostrar su capacidad y vulnerabilidad del sistema, tal como lo hacen los hackers, o bien para mantenerse en el sistema contra la voluntad del que tiene derecho legítimo a excluirlo. Sin embargo, una y otra conducta delictiva es intrusiva aunque las finalidades sean distintas y recaigan sobre medios electrónicos.

Según el Convenio de Budapest de 23 de diciembre de 2001, se previene a cada Estado miembro sobre el acceso ilícito, para que adopte medidas legislativas para evitarlo y que eleve a categoría de delitos el acceso deliberado o ilegítimo total o parcialmente. El acceso puede cometerse ya sea infringiendo medidas de seguridad, para obtener datos informáticos o con otro fin delictivo, o en relación con un sistema que esté conectado a otro sistema informático.

Por su parte, referente a los abusos de los dispositivos, la comisión deliberada o ilegítima podría darse en los siguientes actos:

1) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: (i) un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos de acceso ilícito, interceptación ilícita, interferencia en los datos o interferencia en el sistema; (ii) una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos mencionados anteriormente.

2) La posesión de alguno de los elementos contemplados en los anteriores apartados, con el fin de que sean utilizados para cometer cualquiera de los delitos previstos anteriormente.

El fenómeno tecnológico TIC permanentemente evoluciona, pues esa es la dinámica que le imprime no solo el mercado, los usuarios y proveedores, sino que por esencia las nuevas tecnologías tienen que estar continuamente reinventándose a sí

mismas porque la obsolescencia deviene en periodos cada vez más insignificantes. Obsérvese como alguien adquiere un equipo de computación de última generación, versión última y no han transcurrido algunos instantes, cuando sale la versión 2, luego 2 A y así sucesivamente, tal parece que ni siquiera el mercado puede estar al último grito de la moda, modelo, generación, versión o acápite de esa versión, porque simplemente la tecnología es apabullante y continuamente reactualizada.

Esa angustia de reinvención constante, permanente y penetrante, es transmitida al mundo jurídico que no estabiliza tipos, figuras o conductas delictivas realizadas con medios informáticos, electrónicos o telemáticos, por la complejidad evolutiva de la tecnología y las altas capacidades humanas de utilizarlos indebida o ilegalmente más que en forma legítima o acomodada al derecho. Podría sonar exagerado, pero puede acercarse a la realidad decir que mientras las actuaciones ilícitas crecen en forma geométrica, las legítimas crecen en forma aritmética, pese a los continuos sistemas, redes o programas informáticos protegidos por alta tecnología de seguridad. Mientras haya puertas, habrá quienes las traspasen.

Pues bien, ya cursan en el Parlamento varias propuestas de reforma el sui generis Capítulo VII bis de los delitos contra la información y los datos personales, no solo sobre el articulado, los tipos penales establecidos, el cambio de punición, la mejor utilización del lenguaje para la estructuración de los tipos penales básicos y agravados; sino la eliminación, refundición o aumento de tipos penales que engloben mejor el bien jurídico protegido, para que no siga apareciendo como un bien jurídico difuso o intermedio[16] o de referencia individual, como lo tildan juristas extranjeros como Ricardo M. Mata y Martín, citados por Castro Ospina.

Una de esas propuestas de reforma que referenciamos es el proyecto de ley que cursa en la Cámara de Representantes y en la que se reviven las definiciones técnicas aplicables a los diferentes tipos penales relativos a la protección de la información y los datos personales, entre otros, el acceso abusivo a un sistema informático. Dicha conceptualización es necesaria y coherente en una norma *iuscivilista* o *iusadministrativista*, pero no en una de carácter penal, al menos en la

[16] Bienes jurídicos intermedios son aquellos intereses colectivos tutelados penalmente de forma conjunta con bienes particulares, siendo ambos de carácter homogéneo o estando situados en la misma línea de ataque. Este tipo de bienes jurídicos son: (i) Suprapersonales, es decir que superan los intereses particulares, (ii) Están vinculados a un bien jurídico netamente personal; (iii) Pertenecen a los intereses de la comunidad y no al ámbito de los intereses del Estado, pues los primeros tienen una mayor relación con los bienes individuales; (iv) Son cualitativamente homogéneos con los intereses individuales que pueden resultar vulnerados; o se encuentran en una misma dirección de ataque del comportamiento punible; (v) Hay relación medial entre el bien colectivo y el bien individual; (vi) La lesión del bien jurídico intermedio representa un riesgo potencial para un número plural e indeterminado de víctimas; y (vii) La lesión al bien colectivo, como límite mínimo, no ha menoscabado de manera efectiva los bienes personales, que es el límite máximo. De esta forma se sobrepasa el estadio del peligro abstracto. (Castro, 2002, 15 de julio, p. 4).

parte especial del Código Penal, pues todo lo aplicable a un código punitivo con carácter general o sectorial debe ir en la parte general del código, para efectos de aplicabilidad y de sistematización temática y referencial.

Respecto de la propuesta de esta conducta delictiva que todavía no ha tenido aplicabilidad práctica visible en los estrados judiciales colombianos y menos aún de revisión de los organismos jurisdiccionales techo en materia penal (Corte Suprema de Justicia), formalmente con incidencia en el fondo de la conducta típica del acceso abusivo en un sistema informático, se ha planteado lo siguiente:

Mejorar la redacción del tipo a fin de evitar la estructuración de conductas en blanco y evitar la ambigüedad, falta de precisión terminológico-técnica a la hora de su aplicación a los casos concretos. Con ese objetivo se solicita la eliminación de los siguientes elementos normativos que se consideran innecesarios y ofrecen confusión: o por fuera de lo acordado, en todo en parte, protegido o no y legítimo utilizado en la redacción del tipo.

Aunque no contamos con la exposición de motivos de dicho proyecto, estamos de acuerdo con el planteamiento por las siguientes razones: (i) El término utilizado al inicio del tipo para cualificar el acceso a un sistema informático, sin autorización o por fuera de lo acordado, resulta ambiguo no sólo o por fuera de lo acordado, sino los mismos términos sin autorización, pues se entiende que el acceso con autorización destipifica el tipo penal y por lo tanto sobraría la expresión que hoy tiene y se mantiene en la reforma propuesta. El término por fuera de lo acordado, supone un convenio, acuerdo o contrato previo entre el que accede a un sistema informático y el usuario, lo que lo convertiría en un típico abusador de un sistema informático, pero eso también sobra porque quien accede a un sistema informático para encasillarse en la figura penal debe necesariamente no tener autorización de acceso alguna (v.gr. claves, contraseñas, permisión de acceso en ciertas horas, días, meses o medidas de tiempo de servicio del sistema), pues de lo contrario la atipicidad de la conducta sería plausible.

Consideramos que el término *en todo o en parte*, utilizado para indicar el nivel de acceso a un sistema informático, es innecesario, pese a que el Convenio de Budapest de 2001 utiliza unos términos similares para indicar que se debe punir el acceso deliberado e ilegítimo ***a la totalidad o a una parte de un sistema informático***. Es irrelevante cuantificar si el acceso a un sistema informático solo se hace a una parte o a la totalidad del sistema, porque lo que determina la configuración del tipo es el acceso mismo, violando las medidas de seguridad el sistema, e incluso también es irrelevante si el acceso se considera deliberado (voluntario o hecho a propósito), si es ilegítimo (pasar por legítimo quien no lo es) o abusivo (usar mal, excesiva, injusta, impropia o indebidamente de algo), pues la configuración de la conducta

punitiva, tal como está prevista en la parte general del Código debe ser típica, antijurídica y culpable, y, por supuesto, el acceso a un sistema se entiende que es ilegítimo, deliberado, abusivo o ilegal, de lo contrario devendría la atipicidad penal pero podría surgir configuración de una contravención especial o una infracción civil o administrativa según el grado de insidiosidad que tenga la conducta, y eso sí es probable en nuestro sistema jurídico, a pesar de no haber normativa al respecto.

El término legítimo, utilizado por la norma es innecesario porque la persona que tiene derecho a excluir el acceso o rechazar que permanezca en un sistema informático se entiende que es legítimo o conforme a derecho, pues de lo contrario no tendría facultad alguna de no permitir el acceso o rechazar la permanencia en el sistema. Eso pasaría con los operadores o fuentes de información específica que administran, controlan, vigilan o prestan servicios de consulta de información relevante en una base o fichero de datos en línea o fuera de ella. Estos administradores de la información tienen derechos y deberes que cumplir en el funcionamiento de esos sistemas informáticos y uno de ellos es precisamente es el *permitir el acceso a la información únicamente a las personas que, de conformidad con lo previsto en la ley, pueden tener acceso a ella* (artículo 7º de la Ley 1266 de 2008 o ley de Habeas Data financiera). Por su parte, el titular de la información tiene sus derechos y deberes y uno de éstos frente a los operadores de los bancos de datos es: *solicitar información acerca de los usuarios autorizados para obtener información* (art 6-1º Ibíd.).

Finalmente, se propone la inclusión de los términos o con otra finalidad ilícita para denotar que el acceso a un sistema informático puede tener la finalidad de obtener datos informáticos o con otra finalidad ilícita. Consideramos innecesario también el elemento normativo adicionado a la redacción de la conducta penal, aunque esa directriz la propone el Convenio de Budapest de 2001 en el artículo 2º, al ejemplarizar que el delito se comete infringiendo medidas de seguridad, con intención de obtener datos informáticos o ***con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático***.

Si bien la reforma aclara que el acceso a un sistema informático es para obtener datos informáticos que no lo hace el actual artículo 269 A del C.P., pues sólo la punición deviene del acceso mismo a un sistema informático, entendiendo que es no solo por violar las medidas de seguridad para demostrar su experticia en las nuevas tecnologías de la información y comunicación (*White hackers*) sino que implícitamente conlleva unas finalidades ilícitas que buscan algún provecho o beneficio para el agente o un tercero (Black Hackers) de lo contrario, solo en la obra literaria del Arte de la Intrusión de Mitnick, es creíble que los que los hackers reconvertidos ahora en asesores de medidas de seguridad a sistemas informáticos altamente sensibles para la seguridad y defensa de los Estados, o para salvaguardar información relevante financiera, económica, industrial, intelectual, etc., solo lo hagan por la vanagloria

personal, por el anonimato del pirata informático o por el voyerismo informático, pues detrás de cada acción humana está una reacción que algún efecto produce desde los más nimios o anodinos hasta los más complejos e intrincados o incluso a veces inexplicables.

6.2 Delito de obstaculización ilegítima de sistema informático o red de telecomunicaciones

6.2.1 Fuente normativa: artículo 269, literal b. En esta conducta también son aplicables las normas extrapenales siguientes:

(i) Ley 1266 de 2008 sobre el habeas data, pues se requieren las conceptualizaciones previstas en aquella norma sobre sistema informático y datos informáticos y dentro de esta última los términos titular de la información, dato personal, dato privado, dato público, dato semiprivado o financiero, así como usuario, fuente y operador de la información y finalmente, los principios que rigen a la administración de la información, sobre todo el de seguridad y de confidencialidad de la información.

(ii) La ley 1288 de 2009, 5 de marzo, relativo al fortalecimiento del marco legal que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia en el Estado colombiano para la seguridad y defensa nacional, puesto que toca con aspectos de acceso a información reservada por servidores públicos.

(iii) La Ley 1341 de 2009 de 30 de julio, por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones —TIC—, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Especialmente sobre el entendimiento de las nuevas tecnologías de la información y la comunicación o TIC (*son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes,* según el artículo 6º); el uso permitido, inspeccionado y controlado por el Estado a través del Ministerio de tecnologías de la Información y la comunicación o MinTIC y la Comisión de regulación de Comunicaciones (CRC) y la Agencia Nacional del Espectro (ANET), que es la competente para imponer sanciones a la vulneración del espectro electromagnético (artículos 63 y 64 Ibídem, excepto la previstas en el artículo 76, constitucional); así como también, los principios que rigen en las TIC, tales como que, *el derecho a la comunicación, la información y la educación y los servicios básicos de las TIC. En desarrollo de los artículos 20 y 67 de la Constitución Nacional el Estado propiciará a todo colombiano el derecho al acceso a las tecnologías de la información y las comunicaciones básicas, que permitan el ejercicio pleno de los siguientes derechos:*

La libertad de expresión y de difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, la educación y el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura.

La Corte Constitucional en Sentencia de C-403-2010, declaró inexequibles algunos artículos de esta ley. Estos son: apartes de los artículos 11, 72 y 22-4 y se declaró inhibida sobre el artículo 36 de la mencionada ley.

6.2.2. El tipo penal. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

6.2.3. Sujetos de la conducta punible. Será sujeto activo una persona sin calificación alguna y por lo tanto puede ser un particular o un servidor del Estado. Solo que en este último caso la sanción se agravará, por así contemplarlo el artículo 269 H-2, como una circunstancia de agravación punitiva si la conducta se comete por un servidor público, la pena se aumentará de la mitad a las tres cuartas partes.

El sujeto pasivo podrá ser el Estado, pero también las personas jurídicas o particulares con o sin funciones públicas que administren, manejen, coordinen un sistema informático, bases o ficheros de datos.

6.2.4 La confidencialidad y disponibilidad de la información. La conducta no solo afecta a la confidencialidad (el secreto o sigilo) de la información, puesto que las acciones comisivas también incluyen el acceso a la información que se halla recolectada o almacenada en una base de datos o sistema informático, sino también a la disponibilidad de la misma, porque las acciones comisivas del agente se extienden hasta impedir u obstaculizar el uso, manejo, fluidez o transmisión de los datos personales o informaciones, lo cual impide el ejercicio normal y corriente de los derechos que le asiste al titular de la información, tales como el derecho a la intimidad, el habeas data, el de información misma, el buen nombre e imagen, entre otros personalísimos y sociales. *La colectividad tiene derecho a la disponibilidad de la información sin perturbaciones ni trabas, pues ella les permite ejercer libremente sus derechos. Solo el conocimiento hace posible la libertad*[17].

[17] Castro cita como medios comisivos de los delitos contra disponibilidad de la información, las bombas lógicas y los virus, pues argumenta que transitoriamente (afecta) a la disponibilidad de la información sin destruirla. Otros son los ***Spam o el electronic-mail bombig*** que consiste en el envío de cientos o miles de mensajes de correo electrónico, no solicitados o autorizados, para bloquear a los sistemas. (Castro, 2002, 15 de julio).

6.2.5 Conceptualizaciones. El Convenio de Budapest de 2001, en su artículo 1º define a los datos informáticos, como *cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado que un sistema informático ejecute una función*.

El dato personal entendido como cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que pueden asociarse con una persona natural o jurídica (según el artículo 3º, lit. e, de la Ley 1266 de 2008), constituye una especie del dato informático que lo contiene, y aunque la legislación nacional no lo estipule en los términos del Convenio de Budapest, uno de los proyectos de ley previos a la expedición de la Ley 1273 de 2009, sí lo hizo en el artículo 1º, referido a las definiciones previas a la descripción puntualizada de las conductas punitivas que hoy conocemos insertas en el Capítulo VII Bis del Código Penal.

La definición que traía el mentado proyecto, sostenía que el dato informático estaba constituido por *cualquier representación de hechos, informaciones o conceptos de una forma que permita su tratamiento digital*. En esencia, este concepto es igual al provisto por el Convenio de Budapest, pero es desafortunado por la mutilación que se hace de la última parte la definición del proyecto de ley, pues el término tratamiento digital es omnicomprensivo del tratamiento informático, electrónico o telemático, antes todo lo contrario estos últimos tratamientos de la información sí contienen al tratamiento digital. En todo caso, lo que significa el dato informático es que es una unidad de información cualquiera (personal, económica, financiera, política, científica, etc.) visual, auditiva, telemática, digital, encriptado, numérica o alfanumérica.

6.2.6 Verbos rectores alternativos. Impedir, obstaculizar. La comisión del delito de obstaculización ilegítima de un sistema informático o red de telecomunicaciones, se configura por los verbos impedir u obstaculizar el funcionamiento o el acceso normal (el término es innecesario y ambiguo, de cara a la antijuridicidad del tipo penal) a un sistema informativo, a los datos informáticos allí contenidos, o una red de telecomunicaciones.

Quien impide u obstaculiza el funcionamiento o el acceso de un sistema informático, a los datos allí contenidos o a una red de telecomunicaciones queda inmerso en la figura penal del artículo 269 B. Quien impide u obstaculiza el funcionamiento o el acceso al sistema informático, los datos o redes de telecomunicaciones necesariamente es quien accede a un sistema informático (tipo penal del artículo 269 A), pues no se puede impedir u obstaculizar el funcionamiento de un sistema informático, si previamente no ha vulnerado los sistemas de seguridad del sistema informático para ingresar al mismo. Es una consecuencia del ingreso, el impedimento

u obstaculización del sistema informático, por ello, bien pudo el legislador establecer un tipo delictivo general que prevea las diferentes fases del procedimiento o tratamiento de datos desde la recolección, selección, almacenamiento hasta el registro, comunicación y transmisión de datos (Riascos, s.f., pág. web Akane) y en cada una de esas fases establecer los diferentes tipos penales que pudieren erigirse, a fin de acceder, impedir, obstaculizar, interrumpir, interferir, bloquear, cancelar, destruir, dañar, interceptar, etc., el procedimiento informático.

Por eso, se nos ocurre que todas las conductas que afecten el procedimiento informático deberían comenzar en el actual delito de *violación de datos personales, bases de datos, sistemas y procedimientos informáticos o redes de comunicación e información*. Y dentro de aquel, comenzar en el primer inciso con la conducta del artículo 269F (Violación de datos personales e informáticos); luego en el segundo, con el tipo del artículo 269 A (Acceso abusivo a un sistema informático); en el tercero con el tipo del artículo 269 B (Obstaculización ilegítima a un sistema informático se eliminaría a red de telecomunicaciones); en el cuarto con el tipo penal del artículo 269 C (Interceptación de datos informáticos); y en el quinto con el tipo penal del artículo 269 G (Suplantación de sitios web para capturar datos personales, que afectarían al acceso, almacenamiento y transmisión de datos).

Como tipo agravado de estos tipos básicos sería la actual conducta delictiva del artículo 269 D (Daño informático), porque afecta los datos personales, a un sistema informático, red informática o programa de computación (software).

El actual tipo delictivo básico de obstaculización ilegítima de sistema informático o red de telecomunicaciones, afecta en esta última parte a una red de telecomunicaciones. La Ley 1341 de 2009 o Estatuto de las TIC en Colombia, sostiene en el artículo 10º que *la provisión de redes y servicios de telecomunicaciones, … es un servicio público bajo la titularidad del Estado, (que) se habilita de manera general, y causará una contraprest*ación *periódica a favor del Fondo de las tecnologías de la información y las comunicaciones del Ministerio de Tecnologías de la Información y las comunicaciones*.

El término telecomunicación[18] cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de ordenadores a nivel de enlace. El estatuto de las TIC excluye de

[18] La **telecomunicación** (del prefijo griego *tele*, distancia o lejos, comunicación a distancia) es una técnica consistente en transmitir un mensaje desde un punto a otro, normalmente con el atributo típico adicional de ser bidireccional. (pág. Web wikipedia). Los datos personales, salvo la información pública, no podrán ser accedidos por internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley.

su regulación lo atinente a la televisión y al servicio postal, los cuales deberán seguir rigiéndose por las leyes especiales para cada medio de comunicación.

La obstaculización ilegítima en las redes de comunicación se diferencia de la interceptación en las comunicaciones en que la primera hace referencia a cualquier forma de interferencia en la emisión o recepción de la información a través de uno cualquiera de los medios de telecomunicación; en cambio, la interceptación es la acción precisa de captación de las comunicaciones entre el emisor y el receptor para conocer el contenido de las comunicaciones, a través de medios de grabación de sonidos, voz o imagen o de copia, xerocopia o transcripción del contenido de comunicaciones escritas mecánicas, electromecánicas o informáticas.

6.2.7 Sub tipo de intrusión: el superzapping. Según el tratadista Reyna Alfaro (citado por Castro, 2002, 15 de julio), una de las modalidades de impedir u obstaculizar el uso o acceso a sistemas, datos o redes de telecomunicaciones es mediante el uso de llaves maestras o programas computacionales no autorizados, lo cual se conoce como *Superzapping*. Esta especie de intrusismo informático afecta el acceso de la información, bien impidiendo ingresar por los canales establecidos en el programa, sistema o red de telecomunicación, o bien poniendo trabas tecnológicas para el correcto uso o utilización del sistema, base o red de redes de información.

6.2.8 Reforma: *ut supra* hemos planteado que la conducta comentada y prevista en el artículo 269 B del Código Penal, perfectamente puede insertarse en un tipo general de *violación de los datos, los sistemas informáticos o redes de información,* caso en el cual ocuparía el lugar del inciso 3º, por afectar a la tercera fase del proceso de tratamiento de datos luego de la recolección y almacenamiento, tratamiento propiamente dicho y registro y, finalmente la consulta y transmisión de datos.

El proyecto de ley presentado a la Cámara de Representantes para reformar el Título VII Bis del Código Penal, referido a la información y los datos personales, no propone reformas específicas al texto previsto en el artículo 269 B, pese a que el término normativo del tipo *sin estar facultado para ello*, refiriéndose a la persona que impide u obstaculiza el funcionamiento o el acceso normal a un sistema informático, o a los datos informáticos allí contenidos, o a una red de telecomunicaciones, resulta innecesario, por estar previsto dicho elemento de antijuridicidad en la parte general del Código, pues si actúa facultado para impedir u obstaculizar el funcionamiento o acceso a los sistemas o bases informáticas, devendría la atipicidad de la conducta y no estaríamos ante un hecho delictivo.

Es cuestionable el término utilizado por el legislador del 2009 al referirse al acceso normal, por cuanto el acceso es una actividad computacional que solo se viabiliza

si se tiene una clase, contraseña, filtro de ingreso o cualquiera otra medida de seguridad que permita o impida el acceso a secas, pues informáticamente no existen accesos anormales sino accede o no accede a un sistema o base informática. Esa función no es calificable de normal o anormal, sino de viabilización o no del acceso. Incluso los hackers, al ingresar a un sistema o base informática, lo hacen una vez se desencriptan los signos alfanuméricos, reconocen una clave o encuentran una contraseña con programas computacionales rastreadores, fisgones o reveladores de claves o destripadores (por lo de Jack el destripador), pero al fin y al cabo el acceso se produce.

6.3 Delito de interceptación de datos informáticos

6.3.1 Fuente normativa: artículo 269 C. Concordante con los artículos 192-196 Código Penal del 2000.

Son aplicables a este conducta algunas de las normas jurídicas mencionadas en el delito de violación ilícita de la comunicaciones, prevista en el artículo 192 del Código Penal, por tratarse de fenómenos tecnológicos parecidos y hasta actividades humanas sobre esos fenómenos homologables, si se tiene en cuenta que la interceptación no se hace de medios de comunicación tradicionales sino de aquellos permeados por las nuevas tecnologías TIC, con la diferencia concreta que el artículo 269 C, se refiere a la interceptación de datos informáticos que incluye datos personales inmersos o no en sistemas informáticos, bases de datos o redes de telecomunicaciones por medios informáticos, electrónicos o telemáticos. Estos son:

(i) La Ley 1341 de 2009, sobre la conceptualización de los nuevos medios de la información y la comunicación o TIC, régimen jurídico de la telefonía fija y móvil e infracciones contravencionales que afectan al derecho de la intimidad, el honor y demás libertades y derechos constitucionales cuando existen actuaciones ilícitas en las comunicaciones; (ii) El Decreto 075 de 2006, Por medio del cual se definen las obligaciones que le asisten a los operadores de servicios de telecomunicaciones en procura de optimizar la labor de investigación de los delitos por parte de las autoridades competentes. La Fiscalía General de la Nación es el organismo del Estado encargado de la coordinación con los organismos con funciones de Policía Judicial, del manejo de las actividades y procesos relacionados con la interceptación de los servicios de telecomunicaciones; (iii) El artículo 235 (C.P.P.), reformado por la Ley 1142 de 2007, reglamenta el procedimiento de interceptación de las comunicaciones telefónicas y similares, realizadas por la Fiscalía mediante la grabación magnetofónica o similares y el artículo 237 Id, sobre audiencia de control de legalidad posterior sobre la interceptación, por parte del juez de control de garantías.

6.3.2 El tipo penal. El que, sin orden judicial previa, intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) y setenta y dos (72) meses.

6.3.3 Sujetos de la conducta. El sujeto activo de la conducta es una persona sin calificación alguna y puede ser particular o servidor del Estado. Este último tendrá mayor punibilidad por su connotación de vinculación con el Estado, los privilegios y derechos que como funcionario tiene y su mayor insidiosidad frente a la conducta penal (artículo 269 H-2 del C.P.). También se puede decir que puede ser una persona particular o una jurídica, esta última por intermedio de su representante legal o miembro de aquella.

No solo el Estado, sino las agencias de información financiera o comercial, los operadores y las fuentes que administran, manejan o coordinan bases, ficheros o registros de datos, entre otros, pueden ser sujetos pasivos de la conducta.

6.3.4 La confidencialidad, la integridad y la disponibilidad de la información. Con esta conducta punible se afectan los tres estadios de la información: su confidencialidad, la integridad y la disponibilidad que son precisamente el núcleo esencial del bien jurídico tutelado de la Información y los datos personales.

Sobre la confidencialidad, el secreto o sigilo de la información; así como de la disponibilidad de la información, caracterizada por la restricción de la libre circulación de la misma (artículo 4-c[19], Ley 1266 de 2008), han quedado explicados en las anteriores conductas ilícitas, por eso en este aparte nos referiremos a la integridad de la información.

La integridad de la información está íntimamente relacionada con el principio de veracidad o calidad de los registros o datos, y significa *que la información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de los datos parciales, incompletos, fraccionados o que induzca a error* (art. 4-a, Ley 1266 de 2008).

Se afecta la integridad de la información, entonces, cuando se impide u obstaculiza

---

[19] La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad y la finalidad del banco de datos. Los datos personales, salvo la información pública, no podrán ser accedidos por internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley.

su funcionamiento o el acceso a la misma. Esa conducta la ejecutan los conocidos Hackers o intrusos. *Las modalidades más conocidas son las siguientes: las bombas lógicas (logic bombs), que se producen en un sistema informático y se activan con un comando especial (fecha, números, etc.), para destruir o dañar datos contenidos en un ordenador; ejemplo,… los conocidos virus Sycam y Dragón Rojo (…).*

6.3.5 Conceptualizaciones. La figura penal trae varios términos técnicos que merecen ser explicados. Algunos ya han sido explicados ut supra, tales como Interceptación de datos, sistema informático y datos informáticos; pero otros como el espectro electromagnético y origen o fuente de información, se aclaran así:

Espectro electromagnético. Es un bien público inenajenable e imprescriptible sujeto a la gestión y control del Estado. Se garantiza la igualdad de oportunidades en el acceso a su uso en los términos de ley (art.75 CN).

Ley 1341 de 2009, sobre principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC–, crea la Agencia Nacional de Espectro como una dependencia del Ministerio de tecnologías de la información y comunicación. La ANET, se encarga de permitir, inspeccionar, vigilar y controlar el uso del espectro electromagnético y sancionar a quienes lo vulneren o desconozcan. En efecto, constituye infracción hace un uso negativo del espectro es una infracción (art.64-13).

Técnicamente, también podemos entender el espectro electromagnético de la siguiente forma: la *Franja de espacio alrededor de la tierra a través de la cuales se desplazan las ondas radioeléctricas que portan diversos mensajes sonoros o visuales* y son reproducidas, transmitidas o transportadas por medios de comunicación tradicionales o por medios pertenecientes a las nuevas tecnologías de la información y la comunicación TIC, es decir, por medios informáticos, electrónicos o telemáticos.

Según el artículo 4-a, Ley 1266 de 2008, fuente de información es

> *la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador, la cual en cuanto tiene acceso y suministra información personal de terceros, se ajusta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos.*

Con estos conceptos se aclara que la interceptación de datos se puede dar en su origen (fuentes de información), en su destino (operadores de la información), o en el interior de la misma (operador que administra y pone en conocimiento la información a los diferentes usuarios autorizados para ello).

6.3.6 Verbo rector: interceptar. Todo lo mencionado al comentar el entendimiento del verbo rector interceptar, medios de comunicación y telecomunicación, en el delito de violación ilícita de las comunicaciones previsto en el artículo 288 del Código Penal de 1980, así como en el punible del mismo nombre en el artículo 192 del Código Penal del 2000, son válidos en este aparte en toda su plenitud. La diferencia en la conducta punible del artículo 269C, como se comentó antes, consistía en que la interceptación de los medios tecnológicos de información y comunicación, TIC, a través de la informática, electrónica y telemática se da exclusivamente sobre datos personales visuales, auditivos, de voz o imágenes. Muy a pesar de ello, ya en esa oportunidad dijimos que dicha interceptación de medios de comunicación perfectamente podía interpretarse que se extendía a los medios TIC, aun antes de que existiera esta forma delictiva específica del artículo 269 C.

6.3.7 Tipo básico de control visual o auditivo clandestino. En el derecho español, la conducta de interceptación de datos informáticos hace parte de un tipo básico de control visual o auditivo clandestino y de las conductas de control ilícito de señales de comunicación. Esto quiere decir que la conducta prevista en el artículo 269 C, hace más referencia a la *incriminación de conductas de interceptación, grabación o reproducción ilícita de otros medios de comunicación, como por ejemplo las comunicaciones por telefax o por correspondencia informática* (Morales, 1997, p. 303), o también de los medios de comunicación que envían o reciben datos personales a través de canales informáticos, electrónicos o telemáticos.

La tratadista Castro Ospina (2002, 15 de julio), ubica al pinchado de líneas (*Wiretapping*) como una conducta delictiva que afecta la confidencialidad de la información, y quizá junto a otras conductas como la introducción de datos falsos (*data diddling*), la fuga de datos (data leakage), uso de llaves maestras (*superzapping*), son los *ataques más graves del derecho de la información, como bien colectivo y que ponen en peligro derechos individuales (...)* como la intimidad, el honor, la imagen, el buen nombre, el habeas data y el propio derecho a la información.

6.3.8 Reforma: la propuesta de reforma al delito de interceptación de datos informáticos es significativa no solo por el mejoramiento en la redacción del tipo penal básico, sino por ampliar la cobertura del tipo con la utilización de nuevos verbos rectores y el aumento de la punibilidad acorde con la mayor insidiosidad de la figura delictiva y las acciones del agente del delito.

La nueva conducta delictiva que se propone es la siguiente:

> ***Interceptación, control o sustracción de datos informáticos.*** *El que, sin la existencia de orden judicial previa intercepte, controle o sustraiga datos informáticos en su origen, destino, transmisión o en un sistema informático o telemático, o las emisiones electromagnéticas provenientes de un sistema informático o telemático que las transporte, incurrirá en pena de prisión cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) Salarios mínimos legales mensuales vigentes*

Desde el mismo intitulado de la conducta penal cambia, pues ya no solo es punible la mera interceptación, sino el control o sustracción de los datos, es decir, el apoderamiento de los datos informáticos, siempre que se haga sin orden judicial previa. Esta conducta ilícita afecta la confidencialidad, integridad y disponibilidad de la información.

En el derecho español, al redactar el tipo penal básico del *descubrimiento y revelación de secretos* del artículo 197 del Código Penal español de 1995, en la primera parte del inciso primero se tipificó el delito de apoderamiento de documentos, papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o de efectos personales, dirigido a desvelar la intimidad de las personas; y en la segunda parte del primer inciso, se tipificó la interceptación de telecomunicaciones o utilización de artificios técnicos de escucha, transmisión, grabación o reproducción de sonido o de la imagen, o de cualquier otra señal de comunicación, con el objeto de desvelar la intimidad de las personas contenidas en datos personales escritos, auditivos, visuales o telemáticos (imagen, voz y audio). En uno y otro caso, se establece una actividad delictiva de control auditivo o visual clandestino, tras el apoderamiento físico de los datos o por la captación, grabación o filmación de aquellos datos.

Sin embargo, el tratadista ibérico Morales Prats (1997, p. 303) sostiene que debía darse un trato punitivo distinto al simple apoderamiento de los datos personales para desvelar la intimidad de las personas, de aquella en la cual se utilizan *sofisticados aparatos de control auditivo o visual clandestino* (grabación, escucha o interceptación de comunicaciones habladas o filmación-captación de imágenes)*; estos últimos proporcionan un control certero y sistemático, más penetrante que pasa inadvertido para la víctima*. Esto significaría una mayor sanción punitiva para el control auditivo o visual clandestino que para el mero apoderamiento físico de los datos, documentos o efectos personales.

Ahora bien, en el derecho colombiano tras la proposición de la reforma al artículo 269 C, se coloca en el mismo plano punitivo tanto la interceptación de datos, como el apoderamiento de datos informáticos, aunque la acción punitiva sea alternativa

al utilizar los verbos interceptar, controlar o sustraer, hubiese sido más conveniente que se excluyera la sustracción, por ser un término equívoco que puede significar apoderamiento o hurto de datos que desnaturaliza la interceptación y control de datos, pues se entiende que quien intercepta datos de alguna manera los está aprehendiendo visualmente (es decir en pantalla, si se trata de datos informáticos interceptados en un equipo de computador propio o de terceros), documentalmente (si se imprimen los datos a través de equipos idóneos para esa tarea), auditivamente (si se escuchan directamente en la interceptación, o una vez se han grabado mediante los aparatos específicos para esta tarea) o visual auditivamente (si se observan y escuchan en un aparato de vídeo o vídeo-filmadora, o en una presentación de vídeo en un aparato de computador, esté o no en línea o red de redes de comunicación).

La Convención de Budapest de 2001, recomienda a los países miembros de la Unión Europea, UE, tipificar la interceptación ilícita (deliberada o ilegítima), por medios técnicos de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático a otro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Se recomienda además, que el tipo delictivo que se erija en estas condiciones, se sostenga que se haga con intención delictiva o *en relación con un sistema informático conectado a otro sistema informático*.

Si bien en el derecho colombiano se siguieron las pautas generales al elevar a tipo penal las conductas de interceptación de señales de comunicación y emisiones electromagnéticas o radioeléctricas, no se cumplió con la estructuración de la interceptación ilícita como tal, sin adiciones del control y menos aún de la sustracción, pues por lo general los datos informáticos bienes intangibles que pueden tangibilizarse en la medida que se saquen de la red, el sistema informático o el banco de datos, mediante aparatos idóneos (impresoras, escáner, cámaras de video o fotográficas, etc.). Si bien no sobra tanto el término control en el tipo penal colombiano, ya hemos dicho antes que la interceptación presupone que al aprehenderse los datos de alguna forma (visual, audiovisual o auditiva) se ejerce un control sobre los mismos con fines ilícitos, por ello la sola interceptación es suficiente para indicar la insidiosidad de la conducta y los fines que se persigue, más cuando en el artículo 269 H, sobre circunstancias de agravación punitiva se dice que los tipos penales básicos perteneciente al Capítulo VII bis del Código Penal, y entre ellos el del artículo 269C (que el Congreso de la República se ha propuesto reformar, mediante la figura que comentamos), se comete obteniendo provecho para sí o para un tercero (numeral 5), o con fines terroristas o generando riesgo para la seguridad o defensa nacional (numeral 6), o utilizando como instrumento a un tercero de buena fe (numeral 7). Estos terceros se conocen, eufemísticamente, como mulas informáticas, las cuales actuando de buena fe y sin conocimiento del ilícito en el que participan no son punibles.

Es acertada la reforma del tipo penal del artículo 269C, en lo referido a la utilización de los elementos normativos de transmisión o en un sistema informático o telemático para referirse a la forma como puede interceptarse un dato informático, en el origen, destino o transmisión (que reemplaza al término en el interior de un sistema informático, que producía ajenidad con el fenómeno o tratamiento de datos). Igual, la adición del término telemático para indicar que un sistema informático también lo puede ser telemático (audio, sonido e imagen), tanto para transmitir datos informáticos como para ser contenedor de datos auditivos, sonoros o de imagen. Sin embargo, recuérdese que un sistema informático es omnicomprensivo de datos, hechos o circunstancias contenidos en un tratamiento o procesamiento de datos e interconectados entre sí, por dispositivos computacionales de *hardware* y *software*, y, como es obvio, los datos pueden ser informáticos, electrónicos o telemáticos.

6.4 Delito de daño informático

6.4.1 Fuente normativa: artículo 269D sobre el daño informático. Concordante con este, los artículos 265 sobre el delito de daño, el 272-3 sobre violación de los mecanismos de protección de los derechos patrimoniales de autor, y el artículo 58-17 sobre causales de mayor punibilidad, cuando se realiza una conducta penal con medios informáticos, electrónicos o telemáticos. Además, el Convenio de Budapest de 2001.

El artículo 265 del actual Código Penal estructura el delito de *daño en bien ajeno*, así: *El que destruya, inutilice, haga desaparecer o de cualquier otro modo dañe bien ajeno, mueble o inmueble incurrirá en prisión (...)*.

Si se resarciere el daño ocasionado al ofendido o perjudicado antes de proferirse sentencia de primera o única instancia, ocurrirá resolución inhibitoria, preclusión de la investigación o cesación de procedimiento.

Se dice con alguna razón que sobraba erigir como delito el daño informático, porque no era más que compatibilizar el artículo 265 con el artículo 58-17 de la parte general del Código Penal, pues perfectamente de la aplicación sistemática resultaba el daño informático con una dosimetría de punición mayor a la que plantea el artículo 269 D.

Más aún, el actual artículo 272 del Código Penal, al tipificar la *Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones*, estructura penalmente una especie de daño informático ocasionado a los componentes lógicos de un programa de computación (software) o sistema informático o tratamiento de datos que hace parte teleológica del delito de daños informático. En efecto, quien: *3. Fabrique, importe, venda, arriende o de cualquier*

forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal, o de cualquier forma de eludir, evadir, ***inutilizar o suprimir un dispositivo o sistema que permita a los titulares del derecho controlar la utilización de sus obras o producciones, o impedir o restringir cualquier uso no autorizado de éstos*** (cursivas y negrillas nuestras).

El Convenio de Budapest de 2001, cuando solicita a los Estados miembros erigir en conducta penal, la ***interferencia en los datos*** (diferente a la interferencia en el sistema que nuestro país se reguló como obstaculización en el sistema informático o red de telecomunicaciones, artículo 269 B), consiste en la *comisión deliberada e ilegítima de actos que dañen, borren, deterioren o supriman datos informáticos,* y se recomienda además que se estipule no solo los daños ocasionados, sino graves daños en los datos.

En tal virtud, dicho convenio propone como más ajustado a la realidad del tratamiento o procesamiento de datos, la interferencia en los datos, puesto que aquí caben todas las acciones contra los datos, sean o no sinónimos de daños: borrar, deteriorar o suprimir datos informáticos.

El Código Penal colombiano en el artículo 269 D, utiliza un mayor número de acciones, verbos rectores para ejemplificar el delito de daño informático, así: destruir, borrar, deteriorar, alterar, suprimir y dañar.

6.4.2 El tipo penal. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48)

6.4.3 Sujetos de la conducta delictiva. Por la utilización de la partícula *El que*, significa que puede ser agente del delito cualquier persona particular o servidor del Estado, solo que en éste último caso, por las connotaciones, derechos, deberes y privilegios del servidor del Estado en la rama, organismo, dependencia o destino público donde labore será mayor la sanción punitiva, según lo determina el artículo 269 H, del Título VII Bis del Código Penal.

Los sujetos pasivos del ilícito serán el Estado, pero también las personas naturales o jurídicas que administren, dirijan o coordinen bases o bancos de datos, sistemas informáticos o registros informáticos dentro o fuera de la red de redes de comunicación.

6.4.4 La integridad y disponibilidad de la información. La conducta delictiva

por los verbos utilizados para su estructuración, afecta la información a la integridad y la disponibilidad de la información. Vale decir, afecta la esencia misma de la información, el contenido de la misma, su validez (contrario al dato erróneo), certeza (contrario al dato falso), eficacia (contrario al dato desactualizado), calidad y completud (contraria al fraccionamiento, al dato incompleto) de la información.

Respecto de la disponibilidad de la información, la conducta evita que la información y los datos se puedan transmitir, comunicar o circular en forma incompleta, errónea, confusa, inválida, ineficaz o desactualizada o sea falsa, pues todas estas formas de disponibilidad de la información constituyen una interferencia en los datos o daño informático en términos del derecho penal colombiano.

6.4.5 Conceptualizaciones. El tipo penal de daño informático, contiene varios términos técnicos propios de la informática jurídica (Riascos, 1997, p. 10 y ss) y aplicables al derecho penal. Unos de esos términos ya los hemos comentado ut supra, tales como datos informáticos y sistema informático. Otros resultan propios del artículo 269 D., son: Sistema de tratamiento de información y componentes lógicos. Uno y otros términos no han sido abordados por la Ley 1266 de 2008, ni por los proyectos anteriores a la Ley 1273 de 2009, que en su artículo 1º relacionaban algunos términos técnico-informáticos utilizados por la ley en la descripción de cada tipo penal.

La Directiva Europea 96/45/CE, relativa al procedimiento informático de los datos personales y en defensa de derechos como la intimidad, relaciona lo que debemos entender por *sistema de tratamiento de información*, así:

> *Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimiento automatizados, y aplicables a los datos personales, como la recogida, registro, organización, conservación, elaboración, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquiera otra que facilite el acceso a los mismos, el cotejo o interconexión, así como su bloqueo, supresión o destrucción*.

En otros términos, se consideran las diferentes fases o etapas por las cuales deben pasar los datos personales o informáticos para su debido tratamiento dentro y fuera de una red de redes, o en un sistema informático o base o banco de datos desde la recolección, almacenamiento, registro, comunicación, circulación transferencia de datos (flujo internacional de datos, se conoce en normas internas europeas, como en la Ley 15 de 1999 o ley de tratamiento automatizado de datos personales en España).

El término *o sus partes,* relatado a continuación del sistema de tratamiento de información es ajeno a una explicación informática, pues si el sistema es un

procedimiento informático de tratamiento de datos, es lógico que se pueda afectar a una parte o todo el procedimiento, pero eso en informática poco importa, pues los procedimientos son concatenaciones casi inseparables y si falta alguna no funciona la estructura total, salvo el caso que el tratamiento lo realicen diferentes personas.

Los componentes lógicos son los programas de computador o *software*. Este término en español o en inglés debió utilizarse por ser menos equívoco que aquel.

Todo tratamiento informatizado de datos incluye dos componentes inseparables como son el *hardware* y el *software*, es decir, la parte física y lógica del computador, por eso el daño informático al que se refiere la norma en el presente delito, es el daño logicial que se produce a los datos informáticos, aunque existen algunos programas de computador, conocidos como Bombas Lógicas y Variados Virus, que no solo afectan a la parte lógica de los programas y a los datos en ellos contenidos, sino que existen verdaderos daños materiales al disco duro y unidades periféricas informáticas, porque los inutilizan o hacen que no sea posible volverlos a utilizar, solo por excepción pueden ser recuperables mediante mantenimiento técnico.

Pensamos que si el daño ocasionado al *hardware* o parte material del computador no está cubierto con esta conducta delictiva del artículo 269 D, bien podría aplicarse el artículo 265 del Código Penal, del delito de daño aplicable a todo bien, incluidos los informáticos.

6.4.6 Verbos rectores alternativos. Los verbos rectores son: dañar, destruir, borrar, deteriorar, alterar o suprimir.

Hemos dicho que el tipo básico de daño Informático, se configura con una serie de verbos consecutivos o alternativos que en el diccionario de la lengua española resultan ser sinónimos algunos y por tanto no necesariamente deberían incluirse por estar supuestos en la sinonimia. V.gr. dañar, destruir, deteriorar. Inclusive, según dicho diccionario, sinónimo de dañar es inutilizar, estropear, arruinar, menoscabar, entre otros. Sin embargo, los tipos penales deberían, a fin de hacer un honor al idioma, no poner todos los términos sinónimos si con el principal (dañar) se subentienden los demás.

Se asimilan a *daño*, aunque no siéndolo en estricto rigor, pero sí comprensible en la informática jurídica, los verbos borrar, alterar o suprimir. Estos términos son entendibles en informática, porque borrar o eliminar un dato informático, significa sacarlo de la memoria de un programa, pero con programas de computador avanzados se puede recuperar (desborradoras o recuperadores de los datos borrados en la memoria de un PC, e incluso de los correos electrónicos borrados de un buzón personal o institucional. En todo caso son recuperables y por tanto el daño

podría ser temporal. Es tal la magnitud de la tecnología informática, que existen programas que recuperan información de discos duros formateados o inicializados, que se entiende que el borrado de datos es casi definitivo.

La alteración (sinónimo de destruir, descomponer) de un dato informático, significaría el cambio de contenido, previo ingreso mediante el acceso al mismo, levantando la medida de seguridad o clave que este tenga.

Suprimir es sinónimo de borrar o eliminar un dato o información general o específica.

6.4.7 Revisión. El delito de daño, en el derecho penal español, se ubica bajo el bien jurídico protegido de los delitos contra el patrimonio y contra el orden económico social, artículos 263 a 267. En el artículo 264-2 (C.P.), como tipo penal agravado presenta el delito de daño informático *al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informático*, que resulta más coherente, pues al fin y al cabo el delito de daño realizado sobre bienes lógicos (software) o bienes físicos (hardware) utilizados en informática, en esencia no cambia con el daño que se puede infligir a cualquier otro bien, salvo como parece ser la intención del tipo de daño informático en nuestro derecho, que se justifica el tipo penal específico de daño informático porque va dirigido a los datos informáticos, a la esencia misma de la información que por supuesto esté contenida en un soporte lógico (CD, Disquete, memoria USB, memoria de un disco duro o flexible, etc.), pues de lo contrario no se justificaría su estructuración. Sin embargo, es tan débil la cuerda de distinción entre producir daño a la parte logicial de un programa y los datos informáticos allí contenidos, porque es inescindible una de los otros, que el daño ocasionado a uno deviene indefectiblemente al otro y por tanto, la estructuración del delito de daño informático (sin decirlo así expresamente el C.P. español, tan solo redactarlo como se ha transcrito) es perfectamente aplicable al daño logicial y físico computacional.

En el derecho penal español, el tratadista Quintero Olivares (1997, p. 560) explica por qué el legislador reglamentó *los daños sobre programas o documentos electrónicos ajenos,* por fuera de los específicos bienes jurídicos que protegían otros derechos. Manifiesta:

> *Esta expresa tipificación obedece al temor del legislador a que el mencionado objeto (datos, programas electrónicos ajenos obtenidos en redes o sistemas informáticos), especial por su naturaleza y por su ubicación (informática) no tuviera una completa protección penal, ya que, si el Código cuenta con una expresa mención a estos objetos, frente a sustracciones o apoderamientos en los delitos relativos al mercado y los consumidores (artículo 278-1 CP), así*

como la que pueda corresponder en cuanto propiedad intelectual (artículo 270 CP), también era precisa la regulación de su destrucción o inutilización, que a su vez, se puede cometer tanto por una actuación como a través de las vías del propio sistema informático.

6.4.8 Reforma. El proyecto de ley reformatoria del Título VII Bis del Código Penal colombiano, propone la eliminación de los siguientes elementos normativos del tipo: *sin estar facultado para ello*, por cuanto resulta presupuesto en la antijuridicidad del tipo penal, tal como se expone en la parte general del Código Penal. En efecto, si está facultado para realizar las acciones descritas en el tipo, deviene entonces la atipicidad del delito. Igualmente, si quien realiza esas labores o acciones (verbos rectores del tipo), tiene el consentimiento del titular de los datos informáticos, también se desnaturaliza la figura delictiva.

También se propone la eliminación de demasiados verbos rectores y dejarlos en *dañar, destruir o alterar* de modo sustancial datos informáticos, sistemas informáticos (…) Esto es acorde con lo que decíamos anteriormente. Pese a ello, sigue sobrando el término *alterar de modo sustancial datos informativos y otros medios informáticos o telemáticos*, pues si se cambia o suprimen, borran o dañan, la destrucción del dato o el sistema siempre es significativa aunque parezca que es insignificante materialmente, pero desde el punto de vista informático lo es.

6.5 Delito de uso de software malicioso

6.5.1 Fuente normativa. Artículo 269E del Código Penal, adicionado por la Ley 1273 de 2009

6.5.2 El tipo penal. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional *software* malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios legales mensuales vigentes.

6.5.3 Sujetos de la conducta penal: el agente de la conducta puede ser cualquier persona sin calificación alguna, es decir, un particular como un servidor de Estado. En iguales condiciones y observaciones que para los anteriores tipos delictivos, el servidor del Estado responde más severamente por sus actuaciones, en vista de que tener la calidad de servidores del Estado es causal de agravación punitiva, según el artículo 269 H-2 (C.P.). Iguales razonamientos se dan en el caso de los sujetos pasivos que pueden ser el Estado, o las personas naturales o jurídicas, públicas o privadas, según fueren administradores, directores de agencias de información comercial u operadores de bases o bancos de datos.

6.5.4 La integridad y la disponibilidad de la información

La conducta delictiva del uso de *software* malicioso, tan criticado desde el *nomen iuris* por los propios legisladores colombianos[20], afecta la integridad o esencia misma de la información, como la transmisión, comunicación o circulación de la información por las vías y canales informáticos o telemáticos.

6.5.5 Conceptualizaciones

La conducta contiene dos términos técnico-informáticos que en realidad son uno. Estos son: *software* malicioso y programas de computación. En efecto, *software*, según traducción al español generalizada, es programa de computador o parte lógica de un programa computacional. De ahí que sobra repetir *software* y programa de computación.

La diferencia entre los dos es la utilización equívoca e innecesaria en el tipo penal de malicioso, todo por la traducción literal que se da a *Malware* sinónimo de *Bad ware*.

En efecto, *Malware* proviene del inglés malicius o malicioso (sinónimo de pícaro, bellaco, astuto, ladino, sagaz, etc.). Características todas que se predican de una persona humana, no de un objeto inanimado como sería un programa de computador. Quizá esa sea la crítica válida al sobrenombre de *software* de malicioso, porque no concuerda el objeto (programa de computador) con el sobrenombre propio de las personas (malicioso); pero lo correcto sería entender que se quiere significar con *software* malicioso y darle una significación no literal al término.

Software[21] en principio se entiende como (soporte o equipamiento lógico), *la suma total de programas de cómputo, procedimientos, reglas, documentación, manuales*

---

[20] Decía el Senador Parmenio Cuellar Bastidas, al proponer el archivo del proyecto 281 de 2008, relativo a la modificación del C.P., al crear un nuevo bien jurídico denominado de la Información y de los datos, que una de entre otras debilidades de dicho proyecto era que estas conductas… ni siquiera tienen una equivalencia en nuestra lengua materna (castellano) y no resulta de recibo hacer depender las consecuencias, de la traducción de las palabras inglesas; mucho menos pueden hacerse tipos que describan conductas que solo tienen sentido en su denominación en inglés. Eso es cierto, pero hoy por hoy el fenómeno informático, electrónico y telemático es universal, como universales son los términos ingleses en la informática general y en particular en la jurídica que obligan a todos los profesionales del derecho a actualizarse cada día en estos menesteres pues la universalización también ya llegó al derecho permeado por las nuevas tecnologías de la información o comunicación TIC y ya no es extraño encontrar en textos jurídicos citas textuales, contextuales y mucho más términos específicos en otro idioma al materno y eso es una forma explícita de la universalización del derecho que ha entrado ahora a leyes, códigos, estatutos de diferentes ramas del derecho. (2008, 14 de mayo, p. 5).

[21] Esta conceptualización se estipulaba en el artículo 1º del proyecto de ley previo a la Ley 1273 de 2009. Además, **Troyanos,** programa malicioso o dañino disfrazado de software inofensivo, que puede llegar a tomar control de la computadora, con miras a provocar el daño para el que fue

y datos asociados que forman parte de las operaciones de un sistema de cómputo. Esta conceptualización ya se tenía en Colombia desde la expedición del Decreto 1360 de 1989, de 23 de junio.

Malicioso o *Bad ware*, es aquel *software* que tiene como objetivo infiltrarse en una computadora o dañarla sin el consentimiento de su propietario o usuario. Existen diferentes tipos de *malware*: virus informáticos, troyanos, gusanos, programas de *Spyware/adware* e incluso los *bots*, *Crash programs* y *cancer routines*, así como cualquier otra técnica igual o similar que se desarrolle en el futuro.

El *Spyware* que es una especie de *software* malicioso (que mejor sería decir uso o utilización ilícitos de programas de computador). El *Spyware* son programas de computador que se instalan sin el conocimiento del usuario para recolectar y enviar información de manera no legítima. A su vez, una subespecie de *Spyware* es el *Bulo u Hoax*[22], con los cuales mediante una forma engañosa y atrayente vía correo electrónico o invitación a utilizar un programa por el cual puede reenviar dicha información falsa o engañosa con diferentes fines alarmistas pero no para sacar provecho alguno.

Si eso es así, bastaba en el derecho colombiano con elevar a rango delictivo las conductas que realizaran las personas que hacen *uso ilícito o indebido de los programas de computador*, diferentes a los que ya estaban legislados para la propiedad intelectual, industrial o empresarial. Eso si se quieren abarcar todos los

---

creado. **Virus.** Programa o código de programación transmitido como un adjunto de mail o dispositivo que permite su réplica, copiándose o iniciando su copia o reproducción en otro programa de ordenador o equipo de cómputo. **Gusano.** Programa o código de programación transmitido como un conjunto de mail que se replica copiándose o iniciando su copia en otro programa, sector de booteo de una computadora, o documento, peroque no requiere de un portador para poder replicarse.

[22] Un **bulo** u Hoax es la noticia falsa es un intento de hacer creer a un grupo de personas que algo falso es real. En el idioma español el término se popularizó principalmente al referirse a engaños masivos por medios electrónicos especialmente internet./ Las personas que crean bulos tienen diversas motivaciones dentro de las que se encuentran el satisfacer su amor propio, la intención de hacer una broma para avergonzar o señalar a alguien o la pretensión de provocar un cambio social haciendo que la gente se sienta prevenida frente a algo o alguien; también suele ser característico dentro de los autores de bulo el querer mofarse y hacer evidente la credulidad de las personas y de los medios de comunicación. ***El bulo informático.*** Es un mensaje de correo electrónico con contenido falso o engañoso y atrayente. Normalmente es distribuido en cadena por sus sucesivos receptores debido a su contenido impactante que parece provenir de una fuente seria y fiable o porque el mismo mensaje pide ser reenviado. /Las personas que crean **bulo** suelen tener alguno de los siguientes objetivos: (i) Captar direcciones de correo (para mandar spam, virus, mensajes con phishing o más bulo a gran escala); (ii) Intentar engañar al destinatario para que revele su contraseña o acepte un archivo de malware; (iii) Confundir a la opinión pública de la sociedad. Básicamente, los bulos se dividen en las siguientes categorías: 1. Alertas sobre virus incurables, 2. Mensajes de temática religiosa, 3. Cadenas de solidaridad, 4. Cadenas de la suerte, 5. Métodos para hacerse millonario, 6. Regalos de grandes compañías, 7. Leyendas urbanas, y 8. Otras cadenas. (http://es.wikipedia.org/wiki/Bulo).

verbos rectores que trae el actual artículo 269 E, en el delito de uso de *software* malicioso, pues de lo contrario, el estricto uso ilícito de programas lo que provoca es una especie de daño específico en los programas de computador o en la parte logicial de los ordenadores, y para ello, no hacía falta sino erigir como tipo penal agravado del delito de daño informático, en un inciso 2º del artículo 269 D, el uso ilícito de programas de computador que tiendan a dañar datos personales, sistemas informáticos o sistemas de tratamiento informático en bases o bancos de datos, con una pena mayor a la estipulada en dicho artículo.

6.5.6 Verbos alternativos: el tipo penal de uso de *software* malicioso, utiliza una serie de verbos rectores que en nuestro sentir desbordan el verdadero intitulado de la conducta o simplemente no es significativa de todas las implicaciones que le suministran los elementos normativos del tipo. En efecto, los verbos alternativos utilizados para la construcción de la figura delictiva son: *producir, traficar, adquirir, distribuir, vender, enviar, introducir, extraer*. Curiosamente no utiliza el verbo usar que le da el título al ilícito penal, lo que hace más sospechosa la estructuración del tipo y la ajenidad de la redacción del tipo con el título del delito que lo contiene. Más aún, se pensaría que tal como está redactado debería estar mejor ubicado entre los delitos que protegen la propiedad intelectual y previstos en el artículo 52 de la Ley 44 de 1993, pues se trata de proteger no los datos personales —que es la esencia del Título VII bis—, sino evitar la producción, tráfico, distribución o comercialización de programas de computador que tengan efectos dañinos, que fácilmente se puede deducir que son programas no autorizados, ilegales, piratas, etc., y que además producen daños logiciales en sistemas informáticos, datos informáticos o tratamiento de datos o bases datos.

Una reforma oportuna a los delitos contra la propiedad intelectual que abarque los nuevos fenómenos de la informática y las tecnologías TIC, debería aprovecharse para que los tipos penales que atentan contra la propiedad intelectual en el derecho colombiano pasaran a conformar un capítulo específico dentro del Título correspondiente a los delitos contra la propiedad, para integrar mejor la protección del bien jurídico de los diferentes tipos de propiedad (tales como la general y la industrial, que sí están integradas al C.P. vigente. Esta integración la tiene el C.P., español de 1995 y se protege con demasiado ahínco la propiedad intelectual -artículos 270 a 272-).

Por lo tanto, es muy cuestionable la redacción de este tipo penal, los fines contrarios al título del tipo penal que persigue y sobre todo si la figura penal está bien ubicada entre los delitos que protegen la información y los datos.

Probablemente algunos de estos cuestionamientos se pueden explicar, además de las razones jurídicas anteriormente sostenidas, en que los hechos o circunstancias

que surgen de atentados contra la información día a día y devenidos de las nuevas tecnologías de la información y la comunicación TIC, por abarcarlos todos y reprimirlos con una conducta típica, antijurídica y culpable, se redactan atendiendo más al fenómeno informático y sus efectos dañinos en la práctica diaria con sistemas informáticos o sistemas de tratamiento informático o bases de datos (todas las especies de *software* mal llamado malicioso) que a la estructuración de un tipo penal con conceptos jurídicos claros, precisos, pero basados en el hecho tecnológico y no al revés.

6.5.7 Reforma: la propuesta de reforma al artículo 269 E, elimina el término normativo constitutivo del ilícito sin estar facultado para ello y lo cambia a *con fines ilícitos* para referirse al cúmulo de verbos rectores que estructuran el delito. Este cambio no parece ser significativo, porque el primer término, como hemos dicho en otras figuras delictivas, era innecesario, puesto que en la primera parte del Código Penal, al referirse a la antijuridicidad de los tipos penales se prevé que las conductas se realizan sin facultades para ello, sin autorización, sin permiso, etc., pues de lo contrario las conductas dejan de ser típicas.

El término *con fines ilícitos*, utilizado para estructurar el tipo, si bien mejora la redacción y el entendimiento del delito, la verdad es que la ajenidad sigue produciéndose entre el *nomen iuris* del delito y la redacción total del tipo, aunque se haya incluido ahora el verbo *usar* que no estaba previsto en el artículo 269 E, y se hayan eliminado los términos (del territorio nacional y otros programas de computación de efectos dañinos) y verbos innecesarios (introducir o extraer) y se haya adicionado equívocamente (o intrusivo y al final del tipo siempre que la conducta no constituya delito sancionado con pena mayor).

En efecto, la propuesta del nuevo artículo es la siguiente: *Uso de software malicioso. El que, con fines ilícitos, produzca, trafique, adquiera, distribuya, venda, use o envíe software malicioso o intrusivo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor*.

Al introducir el término intrusivo luego de *software* malicioso o, el tipo cambió de ser un subtipo agravado del delito de daño informático, tal como lo habíamos propuesto *ut supra,* para convertirse en un subtipo agravado del delito de acceso abusivo a un sistema informático, previsto en el artículo 269 A. Y esto último es precisamente lo que traicionó el subconsciente de los legisladores reformadores del tipo del artículo 269 E, al escribir *in fine* del tipo, la frase: *siempre que la conducta no constituya delito sancionado con pena mayor*.

Paradójicamente, la pena imponible para el delito 269A y la propuesta de reforma del artículo 269 E, son exactamente iguales y por lo tanto, la frase *in fine* del tipo reformador será letra muerta.

6.6 Delito de violación de los datos personales

6.6.1 Fuente normativa: artículo 269F del Código Penal, adicionado por la Ley 1273 de 2009.

6.6.2 El tipo penal. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 a 1000 S.M.M.V.

6.6.3 Sujetos de la conducta penal. El agente de la conducta puede ser cualquier persona sin calificación alguna, es decir, un particular o un servidor de Estado. En iguales condiciones y observaciones que para los anteriores tipos delictivos, el servidor del Estado responde más severamente por sus actuaciones, ya que el tener la calidad de servidores del Estado es causal de agravación punitiva, según el artículo 269 H-2, del Código Penal.

Iguales razonamientos se dan en el caso de los sujetos pasivos que pueden ser el Estado, o las personas naturales o jurídicas, de derecho público o privado, según fuesen administradores, directores de agencias de información comercial u operadores de bases o bancos de datos, en los términos de la Ley 1266 de 2008 o Ley de Habeas Data.

6.6.4 Confidencialidad, integridad y disponibilidad de la información. Esta conducta penal afecta los tres aspectos objeto de protección del Título VII Bis, por cuanto se prevé el acceso, almacenamiento, transmisión, interceptación y divulgación de los datos personales, bases de datos y sistemas informáticos y de tratamiento de datos. En estas circunstancias, la confidencialidad, integridad y disponibilidad de la información se ve afectada por cualquiera de estas acciones que realice el agente en forma sucesiva o alternativa. Este tipo penal, como antes se dijo, es el que debería iniciar el presente Título VII Bis de los delitos contra la información y los datos, porque abarca todo el procedimiento o tratamiento de datos personales que son una especie del género datos informáticos y por cuanto prevé varios verbos rectores que afectan a las diferentes etapas o fases de dicho procedimiento (desde la recolección, almacenamiento, registro, transmisión o circulación de datos). A

partir de esta figura delictiva debieron organizarse los demás tipos, como quedó expuesto anteriormente.

6.6.5 Conceptualizaciones. El tipo penal de violación de datos personales previsto en el artículo 269 F, contiene varios términos normativos estructurales del tipo de carácter técnico que ya hemos aclarado anteriormente (v.gr. datos personales), pero también contempla unos nuevos, tales como códigos personales, ficheros, archivos, bases de datos o medios semejantes.

Para asumir dichos conceptos, debemos consultar la norma extrapenal prevista en la Ley 1266 de 2008, la cual en su artículo 3, literales *e*, a *h*, nos define:
Datos Personales. *Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de la ley. Datos pueden ser públicos, semiprivados o privados.*

Dato público. *Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;*

Dato semiprivado. *Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley*. Estos servicios en el título y a lo largo de toda la ley no se especifican, por lo que debemos entender que son en principio los estipulados en la Ley 142 de 1994, es decir, los servicios públicos domiciliarios (electricidad, agua, telefonía y gas).

Dato privado. *Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular*.

Los términos ficheros (del francés *ficheirs*) y bases de datos, son sinónimos, pues son utilizados en el derecho español indistintamente en sus leyes protectoras de datos personales o de tratamiento automatizado de datos; en cambio, en el derecho francés por supuesto es utilizado solamente el término *ficheirs*.

En consecuencia, ***fichero o bases de datos (database)*,** significa cualquier conjunto de informaciones que sea objeto de un tratamiento o procedimiento informatizado, así geográficamente estén dispersos pero interconectados.

El término *o medios semejantes*, se entenderían: además de los que en el futuro se inventen para almacenar, transmitir o circular datos entre diferentes puntos geográficos y por diversos medios tecnológicos informáticos, electrónicos o telemáticos, los que actualmente se conocen. V.gr. los ***sistemas informáticos***, entendidos como todo dispositivo aislado o conjunto de conectores interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa de ordenador o computador.

Los ***códigos personales*** (o medidas de seguridad de acceso a la información instaladas por el titular de los datos para guardar la confidencialidad o secreto de la información que le concierne) son contraseñas, claves o *passwords* utilizados por la persona para acceder a un programa o sistema informático sin que otras personas puedan hacerlo por ella, ya que estos son secretos, únicos y sirven de autenticación del ingreso para su titular. Estas contraseñas suelen ser fáciles de adivinar porque utilizan nombres de personas más queridas, de mascotas, de objetos preciados, de personajes de cine, novela o de ciencia ficción, dioses de la mitología griega, de animales exóticos, números telefónicos conocidos, direcciones residenciales, fechas de nacimiento o muerte de seres queridos o cualquier otra fecha relevante, nombres de ciudades o países donde se ha vivido y hasta palabras en idiomas extranjeros que se conozcan o no; o en fin, situaciones, hechos o circunstancias que rodean la vida personal del titular de los datos o las que por defecto vienen de fábrica en programas comercializados v.gr. 1234, 0000, 9999 o 5555. Las contraseñas medianas o difíciles de averiguar, son aquellas que no están asociadas a ninguna de las anteriores situaciones, hechos o circunstancias y utilizan signos alfanuméricos y pasan de seis letras con sus dígitos numéricos adicionales. Sin embargo, estas últimas son las de más difícil recuerdo para el usuario y por regla general se anotan en alguna parte (libretas, libros, agendas, archivos informáticos o documentos electrónicos, puestos en la red de redes, etc.) y terminan siendo más vulnerables que las primeras, si se encuentran por Hackers (White and Black), sobre todo las que se ponen irresponsablemente en archivos o documentos electrónicos expuestos a que un pirata cibernético los halle más fácilmente que si se hubiese escondido en un vetusto libro empolvado olvidado en algún rincón de la casa, pues en este punto al menos sigue predicándose que: *my home is my castle*.

Mitnick, en su libro *El Arte de la Intrusión* (2007), dedica un capítulo eufemísticamente titulado: *Anécdotas breves*, en las cuales comenta ocho novelescos casos en los cuales las contraseñas en programas de computador son tan irrisorias que cualquier principiante podría adivinarlas, por ejemplo, un programa de computador que maneja una máquina de refrescos, pudo ser manipulado por un hacker, porque utilizaron como clave, el título de la marca de la competencia. Si el propietario de la máquina de refrescos es Coca-Cola, ¿Cuál es la clave del programa utilizado por estos? Increíble: Pepsi.

Una **contraseña** o **clave** (en inglés ***password***) es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. Aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información, según sea el caso (http://es.wikipedia.org/wiki/Contrase%C3%B1a)

6.6.6. Verbos alternativos. La conducta punitiva de violación de datos personales prevista en el artículo 269F, utiliza varios verbos rectores consecutivos y alternativos para estructurar el tipo. Estos son: obtener, sustraer, ofrecer, compilar, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear. Esta amplia gama de *acciones humanas* inmersas en un solo tipo, si bien abarcan diferentes posibilidades en las que puede incurrir una persona que actúa frente a los *códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes*, no es menos cierto que pueden presentarse equívocos en la acertada utilización de los mismos que podrían llevar a indebidas incriminaciones, como mínimo. Otro aspecto negativo de este excesivo número de verbos resulta de utilizar acciones propias de los dispositivos informáticos, electrónicos o telemáticos como compilar, enviar, intercambiar, interceptar, divulgar, con actividades humanas como comprar, sustraer, ofrecer, obtener y emplear, o que pueden realizar unos y otras, como: enviar, comprar o vender, porque habrá momentos en que una u otra acción se solape a través de los dispositivos informáticos y se desnaturalice el tipo penal.

Para evitar estas excesivas listas de verbos rectores en los tipos penales referidos a la informática, es mejor seguir las pautas de los Estados que vienen estructurándolos y poniendo en funcionamiento no solo textual sino en la práctica diaria, porque tienen varios casos que han judicializado y sentenciado y porque además tienen estadísticas de lo sucedido y aprenden del error y acierto de normas jurídicas tanto comunitarias como internas en cada Estado miembro de la UE.

El Convenio de Budapest de 2001, después de analizar las varias propuestas para tipificar delitos que protejan penalmente los datos personales, pues se entiende que existe una normatividad *iuscivilista y iusadministrativa* de *prima ratio* para protegerlos preventivamente, propuso a los Estados Miembros, erigir como delito la *comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos*, en lo que llama interferencia en los datos (artículo 4º), para distinguirla de *la interferencia en el sistema*, consistente en *la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático, mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración y supresión de datos informáticos* (artículo 5º).

6.6.7 Reforma. La propuesta de reforma del delito de violación de datos personales no propone cambio alguno. Sin embargo, creemos que al igual que en las anteriores conductas delictivas, es conveniente excluir de la redacción los siguientes elementos normativos de estructuración del tipo penal: *sin estar facultado para ello* y adicionar el término omnicomprensivo pero menos criticable que el anterior: *con fines ilícitos*. También deberían eliminarse los términos: *con provecho propio o de un tercero*, puesto que según el artículo 269H, relativo a las circunstancias de agravación punitiva para todos los tipos penales básicos del Título VII bis, le son aplicables y por supuesto, la causal quinta de dicho artículo es realizar la conducta *obteniendo provecho para sí o para un tercero,* que al ser aplicada al ilícito del artículo 269 F, se entendería que el legislador de 2009 ya había regulado un tipo penal básico como si fuera agravado desde su origen y eso significa cuando menos, una falta de técnica legislativa y una incoherencia jurídico-criminológica que para los demás tipos penales deja un estructura básica con la posibilidad de ser agravada si se dan las causales del artículo 269 H, en dos etapas comisivas del ilícito y no en una sola para el caso comentado.

Por otra parte, téngase en cuenta que la violación de los datos personales contenidos en archivos, bases de datos o sistemas informáticos, podrían involucrar aquellos datos que en legislaciones europeas (el Convenio de Europa de 1980, artículo 7º y la Ley 15 de 1999 o Ley de tratamiento automatizado de datos personales en España, por ejemplo), prohíben o restringen al máximo hacerlo, puesto que se afecta el llamado núcleo duro de la privacidad, como son los datos personales sobre el origen racial o étnico, las creencias, la salud, la vida sexual o afiliación política, ideológica o laboral.

Algunas de las razones de esta prohibición o máxima restricción a la recolección, almacenamiento, registro o transmisión o flujo internacional de datos personales son proteger los derechos de la persona, tales como la intimidad personal y familia, el honor y la buena imagen, que en todas las Constituciones europeas se han elevado a rango constitucional y por tanto, de potenciada protección. Además, porque al afectar el núcleo duro de la privacidad, las legislaciones internas deberán reduplicar las medidas de seguridad, si deciden no prohibir definitivamente la recolección o cualquier otro tratamiento informatizado identificado o identificable de datos, sino permitir someter a tratamiento informatizado de datos dichos datos sensibles de la persona, con el pleno de garantías sustantivas o procesales para proteger integralmente los derechos y libertades fundamentales de la persona. En ambos casos, la protección efectiva del Estado y de los mismos particulares, será evidente y altamente reforzada en el plano jurídico de *prima* y de *ultima ratio* (Riascos, 1999).

En nuestro país, en el ámbito de *prima ratio*, no existe una protección integral, aunque sí mínima de los datos personales pertenecientes al núcleo duro de la

privacidad, pues la legislación interna no ha producido normas iuscivilistas o iusadministrativistas dirigidas a la protección del derecho a la intimidad, el honor, la imagen, el buen nombre, aunque sí sobre el derecho a la información (Ley 57 de 1985, Estatuto de la Información; Ley 190 de 1995, Estatuto anticorrupción; Ley 527 de 1999, Documentos e Información electrónica; Ley 594 de 2000, Estatuto de Archivos públicos y privados; y, Ley 962 de 2004, Estatuto antitrámites) y el derecho fundamental del habeas data (con una demora imperdonable en el contexto latinoamericano, el legislador colombiano expidió —tras las reiteradas invitaciones de la Corte Constitucional para hacerlo en sus fallos de tutela sobre el habeas data—, una ley sectorial e incompleta, conocida en la doctrina como Ley del habeas data financiero o comercial, Ley 1266 de 2008 [Riascos, 2009, p. 32]).

En el ámbito de *ultima ratio*, el legislador colombiano ha proferido normas contravencionales contenidas en el Código Nacional de Policía de 1970 y 1971, para proteger el derecho a la intimidad domiciliaria, así como la vida íntima y vida privada de las personas en los artículos 46 a 49 y 52, al elevar a contravenciones especiales los atentados contra la inviolabilidad de domicilio personal y familiar, como el del sitio de trabajo, así como la inviolabilidad de la vida íntima o privada de las personas en el seno de su hogar o sitio de trabajo, ya sea que se atente con aparatos tradicionales o subrepticios de grabación o filmación de sonidos, imágenes o voces. Tal como quedó reseñado y comentado anteriormente.

En el Código Penal de 1980, dentro de las causales de agravación punitiva, no se vislumbraba causal alguna que se refiriera a los aspectos integrantes del núcleo duro de la privacidad en el artículo 66, que posibilitara agravar la sanción si se cometía delito que incorporara aspectos o datos personales sobre el origen racial o étnico, las creencias, la salud, la vida sexual o afiliación política, ideológica o laboral.

En la parte general del Código Penal del 2000, el artículo 58 hizo eco de las legislaciones universales al respecto y por fin estipuló unas causales de mayor punibilidad del tipo penal básico, si *la ejecución de la conducta punible esté inspirada en móviles de intolerancia y discriminación referidos a la raza, la etnia, la ideología, la religión, o las creencias, sexo u orientación sexual, o alguna enfermedad o minusvalía de la víctima*.

En consecuencia, cualquier conducta punible que se cometa inspirada en los anteriores móviles de intolerancia y discriminación, tal como denomina a los datos sensibles o integrantes del núcleo duro de la privacidad o intimidad nuestro Código Penal vigente, la sanción tendrá una mayor punibilidad, máxime si la comisión se realiza con medios informáticos, electrónicos y telemáticos (artículo 58, numerales 3 y 17, respectivamente).

En el actual artículo 269 F, –pues las propuestas de reforma a este tipo penal básico no fueron tomadas en cuenta– como circunstancia de agravación punitiva se podrán aplicar las previsiones del artículo 58, numerales 3 y 17, por ser perfectamente viables e idóneas para crear un tipo penal complementario de agravación punitiva que requiere la existencia del tipo básico y la concurrencia de las circunstancias de mayor punibilidad ya mencionadas.

7.7 Delito de suplantación de sitios web para capturar datos personales

6.7.1 Fuente normativa: artículo 269G, adicionado al Código Penal del 2000 por la Ley 1273 de 2009.

6.7.2 El tipo penal. El que, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 SMMV, siempre que la conducta no constituya delito sancionado con pena más grave.

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

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

6.7.3 Sujetos de la conducta penal

El agente de la conducta puede ser cualquier persona sin calificación alguna, es decir, un particular como un servidor de Estado. En iguales condiciones y observaciones que para los anteriores tipos delictivos, el servidor del Estado responde más severamente por sus actuaciones, puesto que el tener la calidad de servidores del Estado es causal de agravación punitiva, según el artículo 269 H-2, del Código Penal.

Iguales razonamientos se hacen en el caso de los sujetos pasivos, que pueden ser el Estado, o las personas naturales o jurídicas, de derecho público o privado, según fueren administradores, directores de agencias de información comercial u operadores de bases o bancos de datos, en los términos de la Ley 1266 de 2008 o Ley de Habeas Data.

6.7.4 La confidencialidad, integridad y la disponibilidad de la información

La conducta sui géneris de suplantación de sitios de web para capturar datos personales, afecta los tres aspectos objeto de protección del Código Penal en el título VII bis, puesto que abarca todo el ciclo informático desde la recolección, almacenamiento, registro, transmisión o flujo de datos personales, y por lo tanto, se pretende prevenir el acceso, la revelación, la comercialización y la transmisión de los datos que le conciernen a la persona.

La conducta es sui géneris, porque trasplanta el fenómeno tecnológico tal y como sucede en la vida diaria para convertirlo en conducta punible y no las acciones humanas que vayan encaminadas a salvaguardar el bien jurídico contemplado en este título: la información y los datos personales, o, más aún, los derechos fundamentales de la intimidad, el buen nombre, la imagen y el habeas data. De esta forma se procede en los incisos 1º y 2º.

Cierto es que el fenómeno tecnológico posibilitado mediante medios informáticos, electrónicos y telemáticos, se conoce ampliamente, no solo la suplantación de sitios web con miras a diversas actividades ilícitas, sino además el solapamiento de sitios web, el *superzapping* en los sistemas informáticos, etc., que violan medidas de seguridad de acceso, claves, contraseñas o códigos personales y que se conocen genéricamente como formas de *intrusismo informático en red de redes o internet* que persiguen finalidades ilícitas.

Si para suplantar un sitio web y capturar datos, hay que previamente acceder o ingresar al sitio violando las medidas de seguridad tecnológica, bien estructurado legislativamente este delito de intrusión informática para capturar datos estaría en un inciso del anterior delito *violación de datos personales*, pues al fin y al cabo el contenido que cambia en el presente delito es la forma e insidiosidad de ingresar a los sitios web con el propósito de capturar datos personales, aunque este fin ilícito solo esté previsto en el intitulado del delito y en el inciso 2º, cuando avanza a capturar datos personales o financieros. Por ello, resulta innecesario la tipificación de esta forma delictual si para ello solo se transpola el fenómeno tecnológico a la conducta punitiva que persigue proteger la confidencialidad, integridad y disponibilidad de la información con una serie de verbos rectores que se compadecen con el intitulado del delito, como precisaremos *ut infra*.

Cierto es igualmente que, como lo indica el inciso 2º del artículo 269 G, también se convierte en actividad punible con igual sanción a la del tipo básico de suplantación de sitios web, aquel que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que

accede a su banco o a otro sitio personal o de confianza. Es decir, aquella persona que acceda a un sistema informático, base de datos o sistema de tratamiento de datos personales o financieros modificando los nombres de dominio[23] o direcciones electrónicas asignadas autorizada y debidamente en forma tecnológica a las personas naturales o jurídicas, para poder navegar por la Internet e identificarse con nombres o abreviaturas, por ejemplo, los dominios de los gobiernos estatales con ***.gov***, los de las universidades e instituciones de educación con ***.edu;*** los de las empresas, industrias con ***.com;*** las instituciones y entidades militares, con ***.mil;*** las organizaciones***,*** organismos de tipo, objetivos y actividades diferentes a las anteriores, con ***.org***, etc.

En este segundo inciso, el legislador del 2009 excedió su capacidad de trasplantar el fenómeno tecnológico a la tipificación de conductas delictivas porque especificó que la modificación de los nombres de dominio estarían dirigidos a ilicitudes en *bancos o a otro sitio personal o de confianza* (que más fácil y omnicomprensivo debió decir a datos financieros o personales), y aunque no indica que sea con fines y provechos ilícitos, se entiende que el mero *vouyerismo informático* que comentábamos anteriormente en el delito de acceso abusivo a un sistema informático (artículo 269 A), no es lo que mueve al intruso informático o *White hacker*. Entonces, si quien modifica el nombre de dominio hace ingresar equívocamente a una persona a un sitio web de un banco u otro personal o de confianza, incurriría en la figura penal del inciso 2º del artículo 269 G, pero si además consigue una transferencia de activos en perjuicio de un tercero, incurrirá en el delito de transferencia no consentida de activos, prevista en el artículo 269J del Código Penal, y esto significaría que es innecesario haber tipificado el fenómeno tecnológico simplemente de acceso de los nombres de dominios solo con el propósito explícito de modificarlo, sin saber para qué hacerlo. Menos mal que este tipo penal mutilado remite en blanco, al decir: siempre que la conducta no constituya delito sancionado con pena más grave. En efecto, esa frase hace que debamos remitirnos al artículo 269 J, que tiene una punibilidad mayor y complementa el tipo penal incompleto del artículo 269 G, inciso 2º.

El inciso 3º del artículo 269 G, prevé un tipo penal agravado de los anteriores tipos penales, básico (inciso 1º) y el mutilado (inciso 2º), cuando para la consumación

---

[23] Un **dominio de Internet** es una etiqueta de identificación asociada a un grupo de dispositivos o equipos conectados a la red internet. El propósito principal de los nombres de dominio en internet y del sistema de nombres de dominio (DNS), es traducir las direcciones IP de cada modo activo en la red, a términos memorizables y fáciles de encontrar. Esta abstracción hace posible que cualquier servicio (de red) pueda moverse de un lugar geográfico a otro en la red internet, aún cuando el cambio implique que tendrá una dirección IP diferente. Sin la ayuda del sistema de nombres de dominio, los usuarios de internet tendrían que acceder a cada servicio web utilizando la dirección IP del nodo (Ej. Sería necesario utilizar http://74.125.45.100 en vez de http://google.com). Recuperado de http://es.wikipedia.org/wiki/Dominio_de_Internet

del ilícito se requiere que *el agente (haya) reclutado víctimas en la cadena del delito*, es decir, una especie de mula informática, que es aquel tercero que obra de buena fe y es utilizado como instrumento en la consumación del delito. Esta actividad ya está prevista como causal de agravación punitiva en el artículo 269 H, numeral 7º, entendiendo que este tercero si actúa en esas condiciones, estaría exento de responsabilidad penal, de lo contrario deberá evaluarse su grado de participación en el ilícito.

Pese a lo dicho, el legislador penal de 2009, en el aparte transcrito del artículo 269 G, no habla de tercero sino de víctima, calificando a priori que todos los que se encuentren en la calidad de reclutados en la consumación del tipo penal automáticamente serán víctimas y eso en el mundo de la informática jurídica es como mínimo no cierto, pues en el mundo de las nuevas tecnologías TIC, muchas veces se confunde la víctima con el victimario. Baste leer el libro *Arte del Intruso* de Kevin Mitnick, uno de los principales hackers —enjuiciado y condenado en los Estados unidos—, para comprender lo dicho.

6.7.5. Conceptualizaciones. La sui géneris conducta delictiva de suplantación de sitios web para capturar datos personales con propósito ilícito genérico, contiene una serie de términos técnico-informáticos que en determinado momento soslaya la redacción del tipo penal en tal grado que no parece estar leyendo un conducta penal sino un reporte de cómo se puede realizar, negociar o enviar una página web y qué efectos tiene hacerlo.

Los términos utilizados en informática jurídica son: (i) sitios de web, páginas electrónicas, o sitio personal o de confianza; (ii) enlaces o ventanas emergentes; (iii) nombres de dominio; y, (iv) IP.

Para entender el concepto de páginas WWW o Web, debemos hablar del llamado hipertexto (HTML: HyperText Markup Language), al cual nos referimos en otra de nuestras obras jurídicas (Riascos, 1999, p. 453)

El hipertexto es el hijo primogénito y más genuino de la información y comunicación electrónica y telemática. Con el nacimiento del hipertexto no solo se han establecido nuevas formas tecnológicas TIC en unión con la informática, sino una estructura de comunicación electrónica sui géneris*:* interactiva, global, sin límites geográficos y de trasmisión (emisión/recepción) de información de todo tipo, por universidades, instituciones, centros u organismos privados y públicos en formatos, con funciones, características y velocidades electrónicas, siempre y cuando se cuente con un *software* y *hardware* idóneos.

El hipertexto, como otros medios de comunicación electrónica, está basado en los

términos anglosajones apocopados de *Hyper Text Markup Language* (HTML) (Torben, 1998, p. 128), que gramaticalmente significa: lenguaje textual gradualmente incrementado, aunque se ha difundido universalmente como hipertexto, que subsume las características de gradualidad, vinculación e incremento, entendibles en nuestra lengua castellana con el prefijo *hiper*. Igualmente se ha considerado el HTML, como el formato utilizado por las páginas de texto creadas exclusivamente para ser colocadas en una red de redes de información por el proveedor respectivo.

El hipertexto tiene una forma (interna y externa) y un fondo. La forma externa del hipertexto hace relación a la construcción textual con formatos de página WEB, es decir, con metodología World Wide Web (WWW); en tanto que la forma interna hace referencia a la parte técnica y configuración del *sotfware* apto para elaborar dichas páginas. Aquí, por obvias razones, nos referiremos a la forma externa, pues la interna es objeto de la informática estructural. En efecto, para que un ordenador muestre toda la información en pantalla, y luego un usuario pueda emplearla informáticamente como cualquier información digital: almacenar (storage), editar (edit), transferir o simplemente consultarla en el monitor del ordenador, debe crearse por parte de los proveedores de información (universidades, centros, etc.), las denominadas páginas web dentro de un espacio de un servidor de Internet denominado *Webspace*. La publicación de páginas en el mundo virtual del WWW, conocida como *Webpublishing,* siguen los pasos siguientes que determinan los diferentes *software* expertos: a) disponer de un espacio necesario en internet (Webspace), previamente determinado por un proveedor de servicios de comunicación electrónica; b) con el *software* idóneo se crean las páginas web de información según las pautas, principios, características y funciones del proveedor de la información respectiva. Las páginas se escriben como si fuese con cualquier programa de ordenador que procesa texto común y corriente, pero con algunas diferencias técnico-estructurales, que no son del caso comentarlas ahora. Las páginas creadas y diseñadas de conformidad con los fines y objetivos del informador, se almacenan en memoria central y auxiliar del ordenador; y c) las páginas creadas y almacenadas conforman lo que se denomina el *homepage*, o sea, las páginas matrices de la información que ofrece el proveedor correspondiente. El proveedor de la información la enviará luego mediante su servidor de comunicación electrónica a la red de información (v.gr. Internet), para que comience a navegar en las autopistas de la información y sean utilizadas por los usuarios o internautas, previo el acceso a la dirección y sitio de la red prefijado por el proveedor de la información.

Otras formas externas del hipertexto, incluyen las posibilidades que tienen las páginas web, para incorporar imágenes fijas y en movimiento (vídeo), ilustraciones o gráficos (dibujos multifacéticos) e incluso sonidos (voz, música o cualquiera otra fuente que genere sonido). Esta forma, que constituye a la vez una de las principales características de las páginas web, configura un ambiente especial de comunicación

electrónica que une las ventajas y características de la multimedia[24] y las del hipertexto. Algunos iusinformáticos han llamado a este sui géneris y especial matrimonio tecnológico TIC e informática, como *hipermultimedia* o simplemente *hipermedia,* según Marshall Brain (citado por Katsh, s.f.). Quizá la principal virtud del hipertexto sea la alta capacidad para incorporar en sus páginas información textual, visual y de sonido, pues como nunca antes, la información se presenta ante el usuario que está tranquilamente sentado frente a su ordenador situado en una aula de la universidad, en su casa, en su empresa; en fin, en cualquier lugar donde haya un computador conectado a una red de información capaz de emitir y recibir señales de comunicación electrónica. La información producida y recibida por el usuario o internauta constituye el espejo de la realidad (realidad virtual), en tiempo real, concomitante o diferido, según factor pro témpore en el que es recibida. Todo ello sin moverse físicamente del sitio de trasmisión o consulta de la información, pues el navegante electrónico es un caminante sin desplazamiento en el espacio geográfico.

Otro aspecto de forma externo del hipertexto, lo constituye la interactividad de los escritos, páginas web, y sobre todo, documentos electrónicos construidos con el lenguaje HTML. La interactividad posibilita al usuario enlazar documentos electrónicamente con cualquiera otro que guarde relación con aquel, no solo como lo hace el documento tradicional escrito con las referencias bibliográficas, citas de pie de página o remisiones internas o externas en un libro, sino y además, en forma dinámica, cuando puede consultar concomitantemente con el documento en pantalla las referencias bibliográficas, citas o remisiones en todo su contexto, y a la vez, las que aquel documento consultado refiere, y así sucesivamente en forma escalonada o gradual, hasta donde el interés del usuario-consultante se halle satisfecho (y muchas veces más allá) e ir a las mismas fuentes de producción de los documentos consultados por el enlace, sin importar el sitio geográfico donde se hallen, el tiempo horario real en el que se hace; el ambiente locativo en el que se halle (biblioteca privada o pública, siempre que no haya restricción al acceso electrónico); todo ello, con sólo identificar una dirección, ruta, camino electrónico (http:// WWW.,— http:**H**ypertext **T**ransfer **P**rotocol, es decir, la trasmisión de documentos electrónicos por hipertexto— v.gr. Http:www.elcano.com. Buscador para páginas en español), o también conocido como *sitio en el WEB* o URL (**U**niform **R**essource **L**ocator) (Torben, 1998, p. 248).

---

[24] Normalmente se entiende por multimedia, a la utilización de los nuevos medios de comunicación basados en productos digitales o servicios que integran texto, gráficos, audio, película o vídeo, fotografía o animación, combinados con herramientas de software, los cuales permiten a los usuarios actuar de forma recíproca con estos. La multimedia puede presentarse en forma de productos de CD-ROM, en programas de ordenador ofrecidas en los kioscos, en servicios *on line* en los sitios de la red de redes de información mundial (WWW), y en las tecnologías de realidad virtuales. (Jarvlepp, fall, 1997).

Los vínculos (Torben, 1998) o enlaces electrónicos de un escrito o documento ibídem, pueden ser tantos como desee hacerlos el creador del documento, el usuario o consultante o el almacenador de la información. Los vínculos en una página web de hipertexto no solo une documentos textuales, sino que también permite insertar imágenes fijas o de vídeo (formatos BMP), gráficos en formatos GIF (***G**rafic **I**nterchange **F**ile*) o JPG (***J**oint **P**hotography **G**roup*) que potencian la presentación de documentos electrónicos e igualmente una amplia variedad de sonidos en diversos formatos (WAV, MIC, etc.). Esa potencialidad de vinculación de multimedia y texto, se denomina *hipervínculo* (Katsh, s.f.).

Una **dirección IP** (http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP) es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del protocolo TCP/IP. Esta dirección puede cambiar cada vez que se conecta; y a esta forma de asignación de dirección IP se denomina una *dirección IP dinámica* (normalmente se abrevia como *IP dinámica*).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una *dirección IP fija* (se aplica la misma reducción por *IP fija* o *IP estática*), es decir, 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.

A través de Internet, los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar y utilizar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS.

El ***pop up***: denota un elemento (ventana) emergente que se utiliza generalmente dentro de terminología web, y finalmente, el ***link:*** es un enlace o acoplamiento informático.

6.7.6 Verbos rectores utilizados por el tipo penal básico, el mutilado y el agravado

El tipo penal básico utiliza varios verbos para estructurar la conducta, tales como diseñar, desarrollar, vender, ejecutar, programar, enviar (páginas electrónicas, enlaces o ventanas emergentes). Todas estas acciones están precedidas de los términos normativos del tipo: con objeto ilícito y sin estar facultado para ello. Los

dos términos, como hemos sostenido en otras figuras penales de este Título VII bis, son innecesarios por estar previstos en la parte general del Código al estructurar la antijuridicidad de la conducta, pues se entiende que si no se realizan con fines ilícitos, la conducta sería atípica.

Quizá el legislador penal del 2009 estimó conveniente anteponer el término *objeto ilícito* para no caer en contradicción evidente de punir actividades lícitas como diseñar, desarrollar o programar una página de Internet o vender datos personales sin el consentimiento de su titular, por ejemplo. La ilicitud de la conducta debió afincarse en la falta o vicio del consentimiento del titular de los datos, el cual es vulnerado por el agente de la conducta para realizar cualquier actuación ilícita con los sitios, páginas o portales de web o electrónicas, incluido el acceso, almacenamiento, trasmisión o circulación de datos personales o, peor aún, sensibles o pertenecientes al núcleo duro de la intimidad.

Como también se ha dicho en otros tipos penales de este título, la falta de técnica legislativa se debe principalmente a la aplicación de los ciclos o etapas del procesamiento de datos, conocido universalmente en la informática jurídica y que el constituyente de 1991, lo plasmó en el inciso 2º del artículo 15, al sostener: en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. En efecto, importaba destacar el procedimiento o tratamiento informático para entender que en cada etapa pueden vulnerarse derechos y libertades públicas, como la intimidad, el buen nombre, la imagen, el habeas data y la libertad de información. Sin embargo, el legislador acudió a trasplantar los fenómenos tecnológicos e informáticos que en muchas de las veces producen ajenidad con la conducta típica, antijurídica y culpable que se está estructurando; más aún podría quedar en desuso la conducta, porque el fenómeno tecnológico deja en poquísimo tiempo de ser útil para transmitir y circular información y datos porque se inventa una forma mucho más versátil —informáticamente hablando— para transmitir imágenes, audio y texto a través del hipertexto (HTML) y la página web contenida en esta. Legislar con los fenómenos tecnológicos TIC en entronque con la informática, hoy en día tiene un alto riesgo de vetustez casi inmediata. La prueba está, como veremos más adelante, que ni siquiera se alcanza a poner en funcionamiento real la conducta penal del artículo 269 G, cuando ya existen propuestas que deambulan en el Congreso de la República, para reformarla.

El tipo penal mutilado o incompleto previsto en el inciso 2º, contiene los verbos modificar y acceder. El primero se utiliza para indicar que se modifica el sistema de resolución de nombres de dominio; y el segundo, para significar que se hace creer a un usuario que entra en una dirección electrónica que identifica una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el

protocolo IP (*Internet Protocol*), diferente a la que él estima es la de su entidad bancaria o sitio personal o de confianza.

En el primer momento de este tipo penal, la utilización de los términos lleva a la confusión terminológica, ya que *modificar el sistema de resolución de nombre de dominio*, sobran los términos *el sistema de resolución de*, pues son equívocos y no ayudan en nada a dar claridad a la frase, que debió ser *el que, modifique los nombres de dominio*…. Esto sí da claridad a la acción ilícita que se pretende, pues los nombres de dominio, como se dijo antes, son identificaciones electrónicas (nombres, abreviaturas, alias) ya no de la interfaz de dispositivo (IP) sino del usuario o titular informático del dominio (aunque se discute si uno puede o no tener propiedad en estricto rigor jurídico y no una especie de posesión en la red de redes que le posibilite navegar plenamente identificado). Si alguien modifica, altera o se apodera de esos nombres de dominio para, con base en ellos, cometer actos ilícitos, se encasilla en la figura penal descrita en el primer momento.

En el segundo momento del tipo penal, es acceder a un sitio de dominio diferente al que supone el usuario, pero innecesariamente el legislador penal de 2009 solamente cree que puede ser delito ingresar (o *accesar*, como incorrectamente dicen algunos) a un dominio de una entidad bancaria. Cierto es que la información financiera hoy en día es altamente sensible y puede interesar en grado sumo a los titulares de los mismos, que se extravíe, pierda o simplemente se esfume, sin más acciones que la informática a través de cajeros electrónicos o banca electrónica en red (que es el caso del presente punible). Sin embargo, también es cierto que hay otro tipo de información personal o perteneciente al núcleo duro de la intimidad que debería importar al legislador penal proteger y que puede hallarse no solo en otro sitio personal o de confianza, sino en bases de datos, sistemas informáticos o archivos informáticos de dominios privados o públicos que merecen una protección reduplicada, tal como se estila en el derecho comparado.

El tipo penal del inciso 2º del artículo 269G, es mutilado, además de lo dicho anteriormente, porque su comprensión total no se entiende, si no es remitiéndose al tipo penal del artículo 269J (transferencia no consentida de activos), al menos cuando se refiere al ingreso a un dominio diferente al que cree haberlo hecho el usuario de buena fe a un entidad bancaria, pues en cuanto a ingresar a un sitio de dominio privado o público, perfectamente tendría que remitirse al tipo penal del artículo 269 A, acceso abusivo a un sistema informático, el cual presupone una base de datos o un tratamiento de datos interconectado o no.

El privilegio de la información financiera en el derecho colombiano ha sido evidente con los reiterados fallos de tutela de la Corte Constitucional para protegerla desde 1992 hasta hoy, pues si los «*tutelantes*» solicitaban protección judicial efectiva era

porque existía una transferencia irregular bancaria, mora en los pagos, inconsistencias en los datos bancarios, desconocimiento de derechos fundamentales como la intimidad, el buen nombre, imagen, información y habeas data por datos incompletos, erróneos o falsos, etc. Precisamente eso potenció que hoy en día, tengamos una ley de habeas data sectorial o financiera y no una ley estatutaria de habeas data integral, tal como lo propuso la Defensoría del Pueblo en el año 2005.

Este privilegio de la información financiera fue recogido por el legislador penal de 2009 y por eso se revela la inclinación de alta sensibilidad a este tipo de información o datos financieros sancionados penalmente cuando se encuentra en las circunstancias del inciso 2º *in fine* del artículo 269 G.

Por su parte, el inciso 3º del artículo 269 G, plantea un tipo penal agravado de los tipos previstos en los incisos 1º y 2º, y utiliza el verbo *reclutar* para indicar que el agente del delito —para llevar a cabo la conducta de los tipos básicos—, incorpore o enganche a víctimas en la cadena del delito. Ese sui géneris reclutamiento o enganche debería tener unas connotaciones para que esas personas (no víctimas, pues a priori la califica el legislador): (i) que los enganchados no tengan conocimiento de la ilicitud; (ii) que su participación no sea necesaria para la consumación del ilícito; (iii) que actúe de buena fe; y, (iv) que no se considere víctima sino usuario de la red de redes. Tal vez por esto eufemísticamente se le ha denominado mula informática o «*Phisher mula*», al incauto cibernauta enganchado en una actividad cuya ilicitud él desconoce, y por tanto, se considera exento de responsabilidad penal, si efectivamente desconoce la ilicitud de su actuación, y esto en informática o el mundo virtual, sí es posible, a diferencia de la vida real.

6.7.7 El phishing. El artículo 1º del proyecto de ley que luego se convirtiera en Ley 1273 de 2009, considera que el *Phishing* es la máscara, usualmente implementada por SPAM, mediante la que se busca apoderarse de manera ilegítima de la identidad o de los datos de una persona otorgados por un sistema de información.

Phishing (por *fishing*: pescar), proviene de cambiar la letra **f** por las dos letras: **P** y **h** que significan: **p** de password (contraseña) y la **h** de hacker (pirata informático); pues esta labor de *Phising* la realizan los *hackers* (White and Black).

La conducta penal del artículo 269 G, trató de trasplantar el fenómeno informático del *Phishing* tanto en la versión de apoderamiento de la identidad de nombres de dominios como de los datos personales presentes en un sistema informático, base de datos o tratamiento informático, esté en red de redes o intranet. Sin embargo, no lo acondicionó al apoderamiento que es un acto abusivo de un sistema informático, sino a la suplantación de sitios web, lo que deformó la esencia de la actividad informática y creó una conducta penal sui géneris que bien pudo haberse ubicado

en otras figuras delictivas como la prevista en el artículo 269 A, o en un inciso del delito de violación de los datos personales del artículo 269 F.

6.7.8 Reformar. La propuesta de reforma al delito de suplantación de sitio web para captar datos, previsto en el artículo 269 G, retoca la estructura de la conducta punible en los incisos 1º y 2º y elimina el 3º, pero le deja el mismo intitulado al delito. Eso sí, mejora la redacción e invierte el contenido del inciso 1º y lo pone de 2º, y viceversa.

En principio, se propone eliminar los términos *y sin estar facultado para ello*, y se cambia el término normativo inicial que estructura el delito *con objeto ilícito* a *con finalidad de obtener…*, del inciso 1º, creemos por las razones que hemos expuesto para otros tipos delictivos del presente Título VII bis. Eso está bien. Igualmente elimina todos los verbos que aparecían en este inciso, porque aparentemente invierte el contenido del inciso 2º, lo pone en el primero y viceversa.

La redacción se mejora en el inciso 1º, que antes era el 2º, y queda así:

> *El que, con la finalidad de obtener datos personales y/o* [*sic*] *protegidos, mediante páginas electrónicas, enlaces o ventanas emergentes, consiga que un usuario informático acceda por error a una dirección IP distinta a la IP de un portal o Web real, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes*.

En la nueva redacción se destaca que la finalidad del ilícito es proteger los datos personales, y por el uso del término *protegidos*, entendemos aquellos datos sensibles o del núcleo duro de la intimidad. Con este actuar, la propuesta de reforma elimina el tipo penal mutilado que presenta el artículo 269 G, en su inciso 2º, en la propuesta inciso 1º.

Este actuar no solo presenta el fenómeno tecnológico de la especie de apoderamiento de las páginas electrónicas y de la información contenida en ellas (de tipo textual, auditivo, imágenes y video), mediante el acceso por error a una dirección electrónica de IP que no le pertenece al usuario, sino la captura de datos personales o protegidos, que es al fin y al cabo lo que se protege por la conducta y el Titulo VII bis del Código Penal.

El inciso 2º del proyecto, dice:

> *El que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes para la realización de cualquiera de las conductas punibles descritas en éste título, incurrirá en pena de prisión*

de veintiocho a cuarenta y seis meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya otro delito sancionado con pena mayor.

Convierte el antiguo inciso 1º, siendo un tipo penal básico, en un inciso 2º como tipo penal agravado no solo del tipo penal básico del artículo 269G, sino de las seis (6) conductas típicas previstas en los artículos 269A a 269F. Ahora tendría que analizarse si dicha duplicación de agravación ya se presenta en algunos tipos, o está inmersa en las causales de agravación de los tipos penales del Título VII bis prevista en el artículo 269H. Y, esto es posible porque lo que diferencia este tipo agravado de los demás tipos básicos y agravados presentes en los artículos 269A a 269F, es que el presente se refiere en concreto a páginas o portales electrónicas o sitios web, pues los enlaces y ventanas emergentes son vínculos e hipervínculos que posibilita una hipertexto (páginas HTML) que contiene una página WWW o web, y por tanto, esos tecnicismos (enlaces o *Link, o* ventanas emergentes o *Pop up*) siguen sobrando para clarificar la conducta típica, antijurídica y culpable que se piensa crear.

6.8 Tipos agravados contra confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos

En nuestro derecho penal, por costumbre legislativa, en los diferentes códigos penales siempre se han estructurado tipos penales básicos y tipos penales agravados en la misma norma jurídica.

Igualmente, se estructuran causales de agravación punitiva aplicables a todos los tipos penales ubicados en cada capítulo o título del bien jurídico protegido respectivo. Esas causales de agravación son variopintas y se fundan en aspectos, hechos o circunstancias de carácter subjetivo u objetivo adicionados o complementados a la conducta comisiva del tipo principal. El tipo penal básico tiene autonomía en la configuración de los elementos normativos que lo estructuran; el tipo penal agravado, en cambio, debe su estructuración al tipo penal básico para su existencia, la configuración de este es una consecuencia lógica y jurídica de la ocurrencia del tipo penal básico, y es por eso que el legislador penal atendiendo a esos aspectos subjetivos u objetivos adicionales con los cuales se comete el delito y lo agrava, crea unos incisos según las necesidades de tipificación agravada correspondientes.

Esta técnica legislativa se ha utilizado en los delitos contra la información y los datos personales, en particular en cada conducta delictiva de los artículos 269A a 269 I del Título VII bis, capítulos I y II.

En el capítulo I, *De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos*, se estructuran como

tipos penales básicos los siguientes: (i) Acceso abusivo a un sistema informático; (ii) Obstaculización ilegítima de sistema informático o red de telecomunicación; (iii) Interceptación de datos informáticos; (iv) Daño Informático; (v) Uso de *software* malicioso; (vi) Violación de Datos; y (vii) Suplantación de sitios web para capturar datos personales.

Como tipo penal agravado se estructura la suplantación de sitios web para capturar datos personales, cuando en la consumación del ilícito se han reclutado víctimas en la cadena del delito (artículo 269 G, inciso 3º del C.P.)

En el capítulo II, *De los atentados informáticos y otras infracciones*, se estructuran como tipos penales básicos los siguientes: (i) El hurto por medios informáticos, electrónicos y telemáticos; y (ii) Transferencia no consentida de activos.

Como tipo penal agravado se estructura la transferencia no consentida de activos, cuando la conducta penal tiene una cuantía superior a 200 SMLM.

Aparte de estos tipos penales básicos y agravados, el legislador penal ha estructurado una causal de agravación punitiva para los delitos previstos en cada capítulo o título del Código Penal. Estas causales de agravación, en el caso de los delitos contra la información y los datos, solo operan en los delitos que atentan la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos, es decir, los delitos de acceso abusivo a un sistema informático; obstaculización ilegítima de sistema informático o red de telecomunicación; interceptación de datos informáticos; (iv) daño informático; uso de *software* malicioso; violación de datos; y suplantación de sitios web para capturar datos personales (artículos 269 A a 269G del C.P.).

Sin embargo, parece desproporcionada la actuación del legislador penal de 2009, al establecer solamente estas causales de agravación punitiva para los delitos del capítulo I, del Título VII bis, y no para los delitos previstos en el capítulo II, de los atentados informáticos y otras infracciones que son igual o más insidiosos que los previstos en el capítulo I, pues no solo atentan contra los datos personales, sensibles, sino también los de índole financiero. Las causales de agravación debieron ubicarse al final del Título VII bis, para que abarquen los dos capítulos y todos los delitos que atentan contra la información y los datos.

Las causales de agravación punitiva[25] de estos delitos, según el artículo 269H, son las siguientes: (i) Sobre redes o sistemas informáticos o de comunicaciones estatales

[25] En la Sentencia C-038-1998, la Corte Constitucional sostuvo: *Desde el punto de vista material la orma no consagra una causal de agravación punitiva que pueda tildarse de injusta o discriminatoria,*

u oficiales o del sector financiero, nacionales o extranjeros; (ii) Por servidor público en ejercicio de sus funciones; (iii) Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este; (iv) Revelando o dando a conocer el contenido de la información en perjuicio de otro; (v) Obteniendo provecho para sí o para un tercero; (vi) Con fines terroristas o generando riesgo para la seguridad o defensa nacional; (vii) Utilizando como instrumento a un tercero de buena fe; y, (vii) Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

El legislador penal de 2009, respecto de estas causales de agravación y la estructuración de los diferentes tipos penales básicos y agravados del Título VII bis, hizo una reiteración, como mínimo, de tipos penales (básicos y agravados) conjuntamente con causales de agravación punitiva, que en determinados casos concretos, el juez competente deberá saber cuál de ellas aplicar o si por el contrario se estaría violando el llamado principio del *ne bis in idem,* si da aplicación al tipo penal básico o agravado y además la causal de agravación.

Es el caso, por ejemplo, del tipo penal básico denominado *violación de datos personales*, previsto en el artículo 269 F del Código Penal, que se estructura *ab initio* con los elementos normativos del tipo …*con provecho propio o de un tercero*… y la causal de agravación punitiva 5ª del artículo 269 H, aplicable a este tipo penal básico, que es: Obteniendo provecho para sí o para un tercero, con lo cual existe una reiteración de las conductas comisivas que en el mejor de los casos, solo se deberá aplicar la figura penal básica sin la agravante, pues el tipo penal básico ya está configurado como tipo penal agravado.

Iguales argumentos se presentan con el tipo penal agravado de suplantación de sitios web para capturar datos personales, cuando para consumarlo el agente ha reclutado víctimas en la cadena del delito, previsto en el artículo 269 G, inciso 3º

---

ya que, si bien hace más difícil la situación de ciertas personas ante la aplicación de la ley penal, no lo establece así gratuitamente sino a partir de diferencias relevantes que precisamente llevan a considerar que, dentro de la sociedad, los individuos de quienes se trata son precisamente los distinguidos, esto es, los que sobresalen por cualquiera de los factores enunciados, colocándolos en un nivel privilegiado frente a los demás. Es precisamente de ellos -a quienes más se ha dado- de quienes más se espera en lo relativo a la observancia de la ley y el respeto al orden jurídico. No puede ser mirada ni evaluada en la misma forma por el legislador ni por el juez la conducta de un individuo común que la de aquél que, precisamente por su puesto dentro de la escala social, tiene una mayor responsabilidad hacia el conglomerado y a quien se mira por muchos como paradigma y guía de conducta. Si, no obstante su jerarquía o su importancia, vulnera las reglas de convivencia, con mucho mayor conocimiento acerca del daño que su comportamiento causa, es natural que se le aplique una mayor severidad en el juicio y en la tasación de la pena.

del Código Penal. La causal de agravación 8ª, reza: utilizando como instrumento a un tercero de buena fe. Aunque los términos empleados sean diferentes, la esencia de la actuación de esos terceros o víctimas es idéntica y aquí observamos otra reiteración de tipificación delictiva, o acaso una violación al principio del *ne bis in idem*.

La Corte Constitucional en la sentencia C-870-2002, que compiló la jurisprudencia constitucional sobre aquel principio, expresó: *El principio non bis in idem prohíbe que una persona, por el mismo hecho, (i) sea sometida a juicios sucesivos o (ii) le sean impuestas varias sanciones en el mismo juicio, salvo que una sea tan solo accesoria a la otra*

6.9 Delitos previstos en el capítulo II, del título VII bis del Código Penal

6.9.1 Hurto por medios informáticos y semejantes

6.9.1.1 Fuente normativa. Artículo 269 I. concordante con los artículos 239 y 240 del Código Penal, relativos al delito de hurto.

6.9.1.2 El tipo penal. *El que, superando medidas de seguridad informáticas, realice la conducta señalada en el art. 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurra en las penas señaladas en el artículo 240 de este código*.

El legislador penal de 2009, al intitular el delito de hurto por medios informáticos y semejantes, debió ser más concreto y especificar que se trata del delito de hurto por medios informáticos, electrónicos y telemáticos, que son los únicos posibles de semejanza con los informáticos actualmente, máxime si la ley penal ha aceptado que los medios informáticos, electrónicos y telemáticos son circunstancias de mayor punibilidad en el artículo 58 de la parte general del Código Penal.

6.9.1.3 Ubicación del tipo penal. En el Título VII Bis: *De la protección de la Información y los datos* personales. Capítulo II: *De los atentados informáticos y otras infracciones*.

En una de los propuestas de reforma al Código Penal, y la creación del Título VII bis[26], referido a los delitos contra la información y los datos, se proponía además

[26] Nos referimos a la propuesta presentada a la Comisión Primera Constitucional, del texto aprobado en Comisión Primera de la Cámara de Representantes del proyecto de Ley número 042/07 Cámara, acumulado con el 123/07 Cámara, por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado *De la protección de la información y de los datos*–y se

de elevar a conducta delictiva el hurto por medios informáticos y semejantes, la falsedad informática[27], la transferencia no consentida de activos, el espionaje informático[28], la violación de reserva industrial o comercial valiéndose de medios informáticos[29]. Después de expedida la Ley 1273 de 2009, se ha propuesto la creación del delito de enmascaramiento ilícito[30].

6.9.1.4 Sujetos de la conducta penal. El delito de hurto por medios informáticos y semejantes, tiene como sujeto activo a personas particulares como a servidores del Estado. Sujetos pasivos del ilícito serán el Estado, pero también personas naturales o jurídicas que administren, coordinen o dirijan bases de datos, sistemas informáticos o sistemas de tratamiento informático, o bien sean operadores o fuentes de información, al tenor de la ley 1266 de 2008.

6.9.1.5 Conceptualizaciones. El artículo 269, literal i, del Código Penal, trae varios términos técnico-informáticos para la construcción del tipo penal mutilado de dos actos (remisiones al artículo 239 y 240 del C.P, sobre estructuración del tipo básico de hurto y las sanciones impuestas al mismo).

---

preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Vía Internet.

[27] **La propuesta inicial de reforma al C.P., del Juez Segundo Promiscuo Municipal de Rovira (Tolima), Alexander García, sostenía. ARTÍCULO 269I: Falsedad informática.** El que sin autorización para ello y valiéndose de cualquier medio electrónico, borre, altere, suprima, modifique o inutilice los datos registrados en una computadora, incurrirá en prisión de cuatro (4) a ocho (8) años y en multa de 50 a 500 salarios mínimos legales mensuales vigentes. La propuesta presentada a la Comisión Primera Constitucional ya se cambiaba así: FALSEDAD INFORMATICA. El que, sin estar facultado para ello, introduzca, altere, borre, inutilice o suprima datos informáticos, generando datos no auténticos, con la finalidad de que sean percibidos o utilizados a efectos legales como genuinos, 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.

[28] **Articulo 269L. *Espionaje informático.*** El que, sin estar facultado para ello, se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida o recicle datos informáticos de valor para el tráfico económico de la industria, el comercio, o datos de carácter político y/o militar relacionados con la seguridad del Estado, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes, siempre que la conducta no esté castigada con una pena mayor.

[29] **Artículo 269M. *Violación de reserva industrial o comercial valiéndose medios informáticos.*** El que, sin estar facultado para ello, realice una cualquiera de las conductas señaladas en el artículo 308 de este Código, valiéndose de medios informáticos y superando las seguridades existentes, 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, siempre que la conducta no esté castigada con una pena mayor.

[30] ***Enmascaramiento ilícito*** (IP *spoofing*). El que, sin estar facultado para ello, con el propósito de obtener provecho ilícito para sí o para un tercero o para usar y disfrutar servicios informáticos a los cuales no tiene derecho o para causar daño, sustituya o suplante a otro o se atribuya una identidad informática o una calidad que pueda tener efectos jurídicos, incurrirá en pena de prisión de veintiocho (28) a cuarenta y seis (46) meses y en multa de cien (100) a mil (1000) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya otro delito sancionado con pena mayor. Las penas señaladas en el inciso anterior se aumentarán hasta en la mitad, cuando se realicen dichas conductas con fines terroristas o de carácter extorsivo.

Los siguientes términos aparecen en el artículo 1º del proyecto de ley de la que luego fuera la Ley 1273 de 2009, y esta eliminará dicho artículo que traía estas definiciones:

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Sistema electrónico: es un conjunto de circuitos que interactúan entre sí para obtener un resultado.

Sistema telemático: es el formado por equipos informáticos interconectados por una red de comunicaciones o telecomunicaciones que, a su vez, está constituida por circuitos, equipos de transmisión y equipos de conmutación.

Sistema de autenticación: cualquier procedimiento que se emplee para identificar, de manera inequívoca, a un usuario de un sistema informático.

6.9.1.6 El hurto informático: un delito mutilado de dos actos

El delito de hurto por medios informáticos, electrónicos o telemáticos, al interpretar sus semejantes (artículos 269 i y 58 del C.P.), es un tipo penal mutilado de dos tiempos. En un primer momento, porque para su construcción se debe contar esencialmente con la estructura del delito de hurto simple previsto en el artículo 239 del Código Penal; y en un segundo momento, en cuanto a la dosimetría punitiva de la sanción, ha de contarse con las sanciones previstas en el artículo 240 del Código Penal.

Por estas razones, había una postura de asimilación de la conducta a los tipos penales existentes de hurto y hurto calificado; y otra devenida de alguno de los ponentes del proyecto de ley, que luego fuera la Ley 1273 de 2009, que propugnaba por la eliminación de la propuesta del hurto por medios informáticos.

En efecto, sobre la primera postura se dice que según la redacción del artículo 269i, parece que hubiese sido más fácil adicionar el artículo 239 relativo al delito de hurto, con un tipo penal agravado que recoja las acciones previstas en el artículo 269, literal i, como son: *manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, …*, y dejando el tipo penal básico del hurto, es decir, *el que se apodere de una cosa mueble ajena, con*

el propósito de obtener provecho para sí o para otro; o incluso adicionar un numeral al artículo 240, relativo al delito de hurto calificado, cualquiera de las dos opciones, pero no como se procedió al proteger el bien jurídico de la información y los datos, en la conducta penal del artículo 269, literal i, en el Titulo VII bis. Esto, por cuanto en la redacción no queda claro que el agente de la conducta se quiera apropiar de los datos personales contenidos en un sistema informático, electrónico o telemático u otro semejante, sino que habla de maniobras indebidas: manipulación o suplantación de sistemas de autenticación y de autorización establecidos, que típicas acciones de daños informáticos más que de acciones de apropiación o hurto informático.

El término clave que debió aparecer como determinante del delito debió ser el dato personal, porque ese es el objeto mueble intangible ajeno susceptible de apropiación y no los sistemas informáticos y demás medios informáticos, electrónicos o telemáticos compuestos por elementos físicos o de *hardware* o lógicos, programas de computador o *software*, pues la apropiación de estos podría constituir un delito de hurto simple o calificado, según los elementos constitutivos y acciones humanas contra dichos elementos, o en casos excepcionales de delitos contra la propiedad intelectual, si se apoderan de los derechos morales contenidos en los programas de computación; pero en todo caso, nada tendrían que ver con el delito de hurto informático aquí previsto.

Por eso, la estructuración de este delito tiene serios reparos, por los mismos ponentes del proyecto de reforma al Código Penal[31]. En efecto, planteaba entre otras cosas, que la conducta penal ya estaba prevista como hurto agravado en el numeral 4 del artículo 240, al decir: *… llave…falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes*.

Efectivamente, los términos llaves falsas entre otras, son *las tarjetas electrónicas, tarjetas perforadas y los mandos o instrumentos de apertura a distancia* (artículo 239 *in fine* del C.P. español de 1995). Igualmente, se dice que se comete el delito de hurto *violando o superando seguridades electrónicas o semejantes*. Las medidas de seguridad electrónica son todos aquellos dispositivos de físicos o lógicos computacionales que no permiten el acceso, mantenimiento, transmisión o flujo de informaciones o datos personales, para quien no está autorizado o reconocido debidamente mediante claves, contraseñas, *login*, IP, etc.

En ambos casos, está perfectamente previsto el hurto informático, independiente de que el apoderamiento de datos o informaciones se realice con medios informáticos,

---

[31] Ponencia del Senador Parmenio Cuellar Bastidas en la Comisión Primera Constitucional del Senado. Congreso de la República, Bogotá, 14 de mayo de 2008.

electrónicos o telemáticos, que son considerados agravantes del tipo penal y que hoy en día, son las nuevas tecnologías TIC, aplicadas conjuntamente con la informática.

6.9.1.7 Reforma. La propuesta de reforma al artículo 269i, hurto por medios informáticos, electrónicos o telemáticos, no se pronunció sobre el particular, pues lo dejó en las mismas condiciones de estructuración y tipificación inicialmente planteadas.

Sin embargo, debió aprovecharse esta oportunidad para mejorar la redacción y adecuarlo al bien jurídico tutelado de la información y los datos, pues tal como está redactado, existe una ajenidad evidente porque más parece que se protegieran los bienes muebles físicos o de *hardware* e incluso los de *software*, que la información o datos personales o sensibles o del núcleo duro de la intimidad.

En el Código Penal español de 1995, se estructuró el tipo penal de apoderamiento subrepticio de documentos o efectos personales (art. 197-1), que incluye papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos (v.gr. documentos electrónicos, informáticos y telemáticos), que contienen datos personales y dirigidos a vulnerar la intimidad y la propia imagen, con lo cual se observa que el bien jurídico protegido son los derechos fundamentales de la persona por el descubrimiento de la confidencialidad o el secreto que contienen dichos datos personales.

Sin embargo, en nuestro medio, al contrario, nos preocupamos por estructurar los llamados delitos informáticos atendiendo al fenómeno tecnológico, la estructura, la funcionalidad y los efectos que produce en las acciones humanas, y por ello la lluvia de críticas de quienes sostienen que los medios informáticos, electrónicos y telemáticos deben permear todas las actividades de la vida cotidiana pero no desplazar la actividad humana que se sirve de aquellos. El Código Penal debe regular conductas humanas que se consideren ilícitas, independientemente de los medios que se utilicen y no viceversa.

6.9.2 Delito de transferencia no consentida de activos

6.9.2.1 Fuente normativa. Artículo 269, literal J, del Código Penal.

En alguna ponencia ante la Comisión Primera del Senado, sobre el ilícito de transferencia no consentida de activos se manifestó eufemísticamente: *este artículo es simplemente un* ***hurto agravado*** *por el numeral 4 del artículo 240 en relación con el artículo 239 del Código Penal*.

El Convenio de Budapest de 2001 recomendó a los Estados miembros de la UE, elevar a conducta delictiva *los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a) cualquier introducción, alteración, borrado o supresión de datos informáticos, y b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona*.

Esta tipificación de fraude informático subsume el tipo penal de transferencia no consentida de activos y plantea otras posibles conductas que se hallarían inmersas dentro de las premisas terminológicas del tipo, pues no se concentra en el fenómeno de transmisión de datos financieros sino muchos antes en el sistema de tratamiento informatizado de datos, o sea, desde el acceso (introducción), alteración, borrado o supresión de datos que se dan en la etapa de recolección, almacenamiento, registro y circulación de datos.

6.9.2.2 El tipo penal. *El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 SMMV.*

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.
Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 SMMV, la sanción allí señalada se incrementará en la mitad.

El fraude informático para los Estados europeos que siguen las directrices del Convenio de Budapest de 2001, plasmadas en el artículo 8º, o la *Estafa informática,* mediante manipulaciones informáticas de *hardware* y *software*, para el derecho español, o el *hurto agravado* con medios electrónicos, informáticos o telemáticos, para uno de los ponentes del proyecto de ley, previo a la Ley 1273 de 2009, el Código Penal colombiano, reformado en 2009, instituyó esta figura penal como transferencia no consentida de activos en el artículo 269 J, bajo el bien jurídico de la información y los datos y en protección contra los atentados informáticos y otras infracciones.

El fraude informático propuesto en el Convenio de Budapest, tiende a proteger los datos personales con relevancia patrimonial, igual al objetivo que persigue el delito de transferencia no consentida de activos del derecho colombiano; en cambio, en

el ámbito español, el bien jurídico tutelado es el patrimonio y el orden económico social, pero con una aclaración: que la estafa informática es de carácter específico y se persiguen los resultados materiales finales no por el engaño a otra persona, sino a través de la manipulación informática o el engaño virtual producido a los dispositivos computacionales (físicos o de *hardware* o lógicos o de *software*).

6.9.2.3 Sujetos de la conducta punible. Debido a la utilización de los términos «El que …», en el tipo penal, se entiende que puede ser sujeto activo toda persona particular o servidor del Estado, entendiendo que en este último caso, la agravación de la punibilidad sobrevendrá por las causales previstas en la parte general del Código Penal, previstas en el artículo 58.

Sujeto pasivo de la conducta será el Estado, pero al igual que otras conductas penales del Título VII bis, también lo podrán ser personas naturales o jurídicas, particulares o públicas, así como los administradores de bancos de datos personales y financieros (bancarios, de corporaciones de ahorro, tributarios, fiscales y de valores de bolsa) y operadores de información, directores de agencia de información comercial, en los términos que estipula la Ley 1266 de 2008 o ley de habeas data financiero.

6.9.2.4. El delito de transferencia no consentida de activos. El artículo 269J del Código Penal, estructura el tipo penal básico en los siguientes elementos normativos: (i) el ánimo de lucro; (ii) la manipulación informática o artificio semejante; y (iii) la transferencia no consentida de cualquier activo en perjuicio de un tercero.

Estos tres elementos son consecutivos para que la conducta de resultados se produzca, aunque el elemento del consentimiento bien pudo haberse omitido por estar regulado en la parte general del Código Penal, al mencionar la antijuridicidad de la conducta.

El provecho económico es un elemento de la esencia del tipo, pues al ser una conducta de resultado se entiende que debe estar previsto para que se configure el tipo penal.

Respecto de las manipulaciones informáticas, se entiende toda alteración o modificación de datos –ya sea suprimiéndolos, introduciendo datos nuevos y falsos–, colocar datos en distinto momento o lugar, variar las instrucciones de elaboración, etc.

> *Se diferencia en las estafas informáticas de las cometidas dentro del sistema y las cometidas fuera del sistema. Las primeras son las manipulaciones realizadas directamente sobre el sistema operativo y no existe ningún engaño ni error sobre un ser humano. Las estafas cometidas fuera del sistema, son las*

manipulaciones de datos hechas antes, durante y después de la elaboración de los programas, siendo éstas las causantes del engaño que determina de disposición patrimonial[32].

Por la ubicación y bien jurídico protegido (la información y los datos) del delito de transferencia no consentida de activos, las manipulaciones informáticas que se presentan en los datos son aplicables a la conducta penal mencionada en el derecho colombiano.

6.9.2.5 Visión integracionista de conductas penales vistas en la transferencia no consentida de activos

La *transferencia no consentida de activos* ocurre por una de tres razones: *torpeza, exceso de confianza* o *novatada* de quien ingresa con su computador a la red.

Normalmente esa transferencia no consentida va precedida de la aceptación del dueño del computador conectado a la **Internet** (potencial víctima)**,** que acepta recibir el archivo que contiene encriptado el programa malicioso (**malware**), o que desestima imprudentemente el consejo de no aceptar comunicación con quien no conoce, y no abrir mensajes de correo electrónico provenientes de direcciones desconocidas (evita el **hacking**), o que desecha la recomendación de digitar en el navegador, directamente y tantas veces como sea necesario, el nombre de la página que desea visitar (la página del banco, por ejemplo) en lugar de apelar al recurso de completado automático de direcciones o sitios web, aplicación que ofrece la mayoría de los navegadores (Internet Explorer, Opera, Mozilla, Netscape), así como de los sistemas operativos, ya sean pagados (como Windows-DOS, Windows-MAC, etc.) o gratuito, llamado comúnmente *software* libre, que es Linux; y caen en la *suplantación de sitios web*, *(phishing)* dotados de apariencia similar a la de la entidad que se desea visitar, y donde se digitan las claves personales de cuentas bancarias que luego son utilizadas para hacer transferencias de dinero a otras cuentas[33].

6.9.2.6 Tipo básico de transferencia valores económicos (Defraudaciones y estafa): (i) Transferencia no consentida de activos por manipulación informática o artificios semejantes (hardware); (ii) Transferencia no consentida de activos por manipulación de *software* de computador. Estafa Informática o telemática

---

[32] AA.VV. *Inclusión de los delitos informáticos dentro del Código Penal del Estado*. (www.monografías.com).

[33] Informe de ponencia para primer debate al Proyecto de Ley 281 de 2008 Senado, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado *De la protección de la información y de los datos*- y se preservan integralmente los sistemas que utilicen las tecnologías en la información y las comunicaciones, entre otras disposiciones.

En el Código Penal español de 1995, se elevaron a conducta penal *las manipulaciones informáticas dirigidas a conseguir una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero* (artículo 248-2), como una forma de delito de estafa y bajo el capítulo VI, De las defraudaciones, y el Título XIII de los delitos contra el patrimonio y el orden económico social.

> *Nos encontramos frente a un tipo defraudatorio que no comparte la dinámica comitiva de la estafa tradicional y, en consecuencia, ajeno a la elaboración doctrinal y jurisprudencial de los elementos esenciales que la configuran. Es más, no solo se trata de constatar que el concepto general de estafa no ejerce aquí una función de criterio rector interpretativo de las conductas penalmente relevantes, sino que, precisamente esa ha sido la ratio legis del precepto: criminalizar conductas lesivas para el patrimonio ajeno extramuros de la dinámica comitiva presidida por el engaño*

No obstante, debe tenerse en cuenta que la nueva figura presenta importantes similitudes con la estafa. En efecto, el bien jurídico protegido es el patrimonio, y no, por tanto, tan solo la posesión o la propiedad de cosas muebles ajenas. La transferencia a cualquier activo patrimonial como objeto material sobre el que deba recaer la acción típica, así lo avala. Por otra parte, la actividad comitiva a través de manipulaciones informáticas tiende a conseguir una ´transferencia´ no consentida de activos patrimoniales. Es decir, si bien es evidente que no supone la provocación de un acto de disposición viciado como medio de ataque al patrimonio, probablemente deban descartarse las conductas de sustracción de algún elemento integrante del mismo.

(…) el fraude informático regulado en el apartado 2º del artículo 248 del Código Penal, no contempla las hipótesis de sustracción de dinero a través de la utilización no autorizada de tarjetas magnéticas sobre los denominados ´cajeros automáticos´: (…) no se trata de transferencia de activos patrimoniales, sino de sustracción de dinero mediante el uso por un tercero del medio específico adecuado para acceder al mismo (…).

En definitiva, la criminalización de las manipulaciones informáticas tendentes a provocar la transferencia no consentida de cualquier activo patrimonial (…) nos encontramos ante una estafa específica, ajena al concepto general de estafa, es un tipo penal de resultado material que exige para su consumación el efectivo perjuicio económico en el patrimonio ajeno, a través de la transferencia no consentida de un determinado activo patrimonial… (Quintero, 1997, p. 489)

7. A manera de colofón

1. Se adiciona un nuevo Título (VII Bis) al Código Penal de 2000, que protege **la**

información y los datos personales, los cuales parcialmente se habían regulado en el capítulo VII, Delitos contra la intimidad, reserva e interceptación de comunicaciones (arts. 192 a 197) del Título III, Delitos contra la libertad Individual y otras garantías.

2. La confidencialidad, la integridad y la disponibilidad de los datos personales son principios o características intrínsecas del derecho a la intimidad que se materializan en el ejercicio del habeas data.

3. Se crea un bien jurídico específico de la **información y los datos personales** del género habeas data.

4. Se traslada el delito **acceso abusivo a un sistema informático** contra la intimidad (art. 195) a tutelar la Información y los datos (art. 269 A), en este nuevo Título.

5. Se penalizan todas las fases del proceso informático, desde el acceso, almacenamiento y registro de la información hasta la circulación, transmisión o comunicación informática, electrónica y telemática de los datos personales.

6. El capítulo II del Título VII bis, **resulta exótico en la ubicación que le asigna**, a no ser porque la informática se toma como medio para consumar los tipos delictivos de hurto y de transferencia no consentida de activos, pues mejor ubicados estarían en los delitos contra el patrimonio económico, toda vez que estos son delitos de resultado.

7. Se eliminaron en el texto definitivo de la ley, **las definiciones de los términos técnicos** que utilizan los diferentes tipos, por ajenidad jurídica de la norma.

8. Se establecen unas **causales de agravación punitiva** para los delitos del título VII bis: (i) Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros, (ii) Por servidor público en ejercicio de sus funciones, (iii) Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este, (iv) Revelando o dando a conocer el contenido de la información en perjuicio de otro, (v) Obteniendo provecho para sí o para un tercero, (vi) Con fines terroristas o generando riesgo para la seguridad o defensa nacional, (vii) Utilizando como instrumento a un tercero de buena fe, y (viii) Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

9. Se establecen **penas** de prisión que van desde los treinta y seis (36) hasta los

ciento veinte (120) meses y multas de 100 a 1.000 salarios mínimos legales mensuales vigentes, según el tipo delictivo básico.

10. Se relacionan tipos delictivos básicos y agravados de **carácter doloso no culposos**. Así mismo, delitos alternativos o consecutivos, según la forma copulativa o disyuntiva de los verbos rectores.

11. Los tipos delictivos del presente título son de **conocimiento de los jueces municipales** según los procedimientos generales previstos en el Código de Procedimiento Penal. Se eliminó un procedimiento especial que estaba consagrado en el anteproyecto de la Ley 1273.

12. El Sector **financiero y económico** público y privado, como las **entidades estatales** en nuestro país, son los más beneficiados con la tipificación de estas conductas delictivas.

Lista de Referencias

AA.VV. (s.f.). *Ley sobre protección a la vida privada o protección de datos de carácter personal*. Recuperado de http://www.sernac.cl/leyes/

Castro, S. J. (2002, 15 de julio) *La información como bien jurídico y los delitos informáticos en el nuevo Código Penal colombiano*. Bogotá: Universidad Externado de Colombia.

Corte Constitucional. (1992). Sentencia T-002.

Definición de Bulo. Recuperado de http://es.wikipedia.org/wiki/Bulo

Definición de dominio de Internet. Recuperado de http://es.wikipedia.org/wiki/Dominio_de_Internet

Definición de Telecomunicación. Recuperado de http://es.wikipedia.org/wiki/Telecomunicaci%C3%B3n

Jarvlepp. (1997, Fall). B.A., LL.B., M.B.A. Information technology and new media law. *KnowledgeBase. An information Technology Law Bulletin*. Retrieved from www.umontreal.edu.ca

Katsh, E. (s.f.). *Rigths, camera, action*. Retrieved from www.umontreal.edu.ca

Livellara, S. (s.f.). *Habeas Data e información crediticia. La eventual responsabilidad civil de las entidades financieras y del banco central de la*

República argentina por cesión y publicidad de datos inexactos. Recuperado de www.eldial.com

Mitnick, K. & Simon, W. L. (2007). *El arte de la intrusión. Cómo ser un hacker o evitarlos*. (1ª ed.). s.l.: Alfaomega, Ra-ma.

Morales, F. (1997). *Comentarios a la parte especial del derecho penal. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*. Pamplona, España: Aranzadi.

Palazzi, P. (1998, noviembre). El habeas data en el derecho argentino. *Revista de Derecho Informático*, (4).

Puccinelli, O. (s.f.). El habeas data en el Brasil. Recuperado de www.astrea.com

Quintero, G. (1997). *Comentarios a la parte especial del derecho penal. Delitos contra el patrimonio y el orden económico social*. Pamplona, España: Aranzadi.

Riascos, L. O. (s.f.). *El habeas data: visión constitucional, legal y punitiva.* Pasto, Colombia: UNED, Universidad de Nariño.

RIascos, L. O. *Los datos personales informatizados en el derecho foráneo y colombiano. Análisis de las fases del Proceso Informático***.** Recuperado de http://akane.udenar.edu.co/derechopublico.

Riascos, L. O. (1997). La Constitución de 1991 y la informática jurídica. Pasto, Colombia: UNED, Universidad de Nariño.

Riascos, L. (1999). *EL derecho a la intimidad, la visión iusinformática y los delitos relativos a los datos personales***.** Tesis Doctoral, Universidad de Lleida, España.

Riascos, L. O. (2009). El habeas Data: Visión Constitucional, visión legal y en proyectos de ley estatutaria. En proceso de publicación. Pasto, Colombia: Universidad de Nariño.

Superintendencia Financiera. *Guías informativas*. Recuperado de http:// www.superfinanciera.gov.co/GuiasInformativas/educa-centralesriesgo.htm

Torben, M. (1998). *Todo sobre el internet explorer 4.* Barcelona: Marcombo.