MARCO LEGAL EN COLOMBIA, LA LEY ESTATUTARIA DE PROTECCIÓN DE DATOS Y EL TRATAMIENTO PENAL

4

Una de las formas, a través de las cuales se logra brindar protección a la intimidad personal, es por medio de la legislación encaminada a la protección de los datos personales, por medio de este tipo de medidas se pretende limitar el ámbito de acceso a la información personal de los individuos, y más importante aún establecer reglas para quienes tienen acceso a tales datos, evitando de esta forma que dicho contenido circule libremente y sin control alguno por parte de sus titulares. Como mencioné previamente, existe un marco constitucional y el marco legal se ha venido complementando, los avances más representativos se traducen en la reciente ley de protección de datos y en la mejora y refinamiento de los tipos penales relacionados con estos temas, cronológicamente, en primer lugar me ocuparé de citar las disposiciones penales en la materia, y las más recientes disposiciones en cuanto a la protección de datos dictadas en 2012 y 2013. Las normas, establecidas recientemente en nuestro país, reciben de manera clara la influencia del derecho español, y en muchos de los apartes y definiciones hemos acogido —en gran medida— la experiencia de ese país en particular, y los fundamentos propios de la experiencia adquirida por la Unión Europea en materia de protección de datos personales y derecho a la intimidad de los individuos (Davara, 1998).

Protección penal

La Ley 1.273 de 2009 complementó algunos tipos penales relativos a la protección de datos y los delitos informáticos, los cuales deseo transcribir y procedo a analizar a la luz de las reflexiones de este escrito:

> 1- Artículo 269a: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido —o no— con 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 una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Este artículo busca sancionar las intromisiones no autorizadas a las redes y los sistemas informáticos, el concepto de sistema informático es amplio y se puede tratar de una red privada o bien de cualquier servicio de administración de datos, el cual puede llegar a verse afectado por dichas intromisiones. Para entender el tipo penal, se hace necesario definir 'sistema informático': "Un sistema informático es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: *hardware*, *software* y las personas que lo usan" (Diccionario de Informática, 2015).

De la anterior definición podemos retomar varios aspectos que pueden volver aún más complejo el análisis del tipo penal, si entendemos que dentro del concepto de sistema informático existen varios elementos que son susceptibles de afectación, podemos notar la complejidad de este tipo penal y el sinnúmero de actividades que estarían sancionadas por esta norma. En primer lugar, quien intente entrometerse o exceder sus permisos de acceso a una máquina, es decir, *hardware*, incurre en el delito; igualmente, quien mediante maniobras electrónicas pretenda vulnerar la integridad de dicho sistema, atentando contra el *software*, incurriría en esta conducta, finalmente lo que llama más mi atención es el que quien para acceder al sistema informático emplea a las personas que hacen parte del sistema, sin duda este último elemento amplía el espectro del tipo penal.

A partir de la definición de "sistema informático" podemos entender que cualquiera de estos contaría con tres elementos que serían eventualmente objeto de ataque, y que en consecuencia, estarían protegidos por el tipo penal:

1- la máquina, *hardware* o computador,

2- el *software*, es decir, los programas y la información que se encuentra en ellos o que se administra a través de ellos y

3- la persona que se encuentra a cargo del manejo de dicho sistema.

Otro concepto importante que se relaciona con este tipo penal consiste en diferenciar "sistema informático" de "sistema de información", en este orden de ideas se pueden diferenciar así:

> Un sistema informático puede formar parte de un sistema de información; en este último la información, uso y acceso a la misma, no necesariamente está informatizada; por ejemplo, el sistema de archivo de libros de una biblioteca y su actividad en general es un sistema de información. Si dentro del sistema de información hay computadoras que ayudan en la tarea de organizar la biblioteca, entonces ese es un sistema informático (Diccionario Informático).

Las diferencias entre los dos conceptos son:

1. El sistema informático cuenta con una combinación de *hardware*, *software* y del ser humano que opera dicho sistema.

2. Los sistemas de información pueden contar —o no— con computadores o con un *software* para administrar el contenido del sistema, sin embargo, subsisten aun sistemas de información netamente físicos, como por ejemplo, los datos de tipo artístico que se encuentra en una pinacoteca.

3. Los dos conceptos coinciden en que se trata de sistemas complejos y ambos requieren la intervención de seres humanos para poder funcionar, a pesar de que se valgan de herramientas físicas o tecnológicas para operar.

> 2- Artículo 269b: obstaculización ilegítima del sistema informático o red de telecomunicación. 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 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Este tipo penal pretende sancionar las prácticas de los denominados *hackers*, quienes durante los últimos años han venido desarrollando actividades como las

descritas en el tipo penal, obstaculizando y saboteando sitios en internet por medio de diversos ataques informáticos que afectan no solamente al dueño del portal, sino a sus usuarios.

Aparece, nuevamente, el concepto de red de telecomunicaciones, el cual se puede definir como: *"Telecommunications network*: una red de telecomunicaciones es una red de enlaces y nodos ordenados para la comunicación a distancia, donde los mensajes pueden pasarse de una parte a otra de la red sobre múltiples enlaces y a través de varios nodos" (Diccionario Informático, 2015). A su vez, para poder entender el concepto es necesario definir el término "nodo", el cual significa: "Punto de intersección o unión de varios elementos que confluyen en el mismo lugar. En una red, cada computadora constituye un nodo".

Vistas las definiciones, otra forma de atentar contra la intimidad personal de un individuo será aquella descrita en el tipo penal, pues se atenta contra el sistema informático o también puede suceder que se ponga en riesgo la comunicación entre varios equipos electrónicos, la comisión del delito se presentará cuando ocurra la intromisión en la comunicación que impida al legítimo usuario de ella acceder al sistema o a la red informática.

> 3- Artículo 269c: interceptación de datos informáticos. 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) a setenta y dos (72) meses.

Este artículo es el que más se relaciona con el tema de la intimidad y el derecho a no ser intervenido o interceptado; como es bien sabido, la Constitución también garantiza el derecho a la inviolabilidad de la correspondencia y la confidencialidad de la información personal en el artículo 15 de la Constitución, además de los preceptuados por la Declaración Universal de los Derechos Humanos en su artículo 12; sin embargo, este tipo penal pretende abarcar otro tipo de comunicaciones que van más allá de la correspondencia tradicional, y que en consecuencia, estaban por fuera del presupuesto normativo para contemplar su sanción. Sin duda, la Ley se abre a una serie de nuevas formas y entornos en los cuales se puede entender que existe una necesaria protección al derecho a la intimidad, razón por la cual el esfuerzo normativo complementa la abundante jurisprudencia constitucional sobre dicho tema de intimidad personal.

> 4- Artículo 269d: daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

El artículo busca proteger un derecho derivado de la intimidad personal que consiste en el derecho a la protección del dato de la persona, en el caso particular se sanciona cualquier actividad que pueda conducir a la alteración o desaparición de datos sin el consentimiento del titular del mismo. Este concepto de dato personal puede considerarse como un nuevo atributo de la personalidad que surge con el siglo XXI, el derecho a conocer, actualizar y rectificar datos personales es un derecho de índole constitucional, y en consecuencia, este artículo permite desarrollar dicha protección en el ámbito penal.

> 5- Artículo 269e: uso de *software* malicioso. 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 1.000 salarios mínimos legales mensuales vigentes (Ley 1.273 de 2009, República de Colombia).

Nuevamente, este aparte de la norma busca ocuparse de otra actividad ilegal que no contemplaba una sanción clara en la legislación, esta es la utilización de programas de ordenador destinados a producir efectos dañinos a la información almacenada, o también aquel tipo de *software* destinado a extraer datos de una red o de un equipo de cómputo sin la autorización de su titular.

El tipo penal se ocupa de garantizar la protección ante aquellas eventuales transgresiones a la intimidad personal, el aspecto que toca este tipo penal se relaciona con la disponibilidad voluntaria de los datos personales, este punto coincide con la apreciación previamente citada del concepto mismo del derecho a la intimidad, el cual consiste en que solo el titular puede disponer de él; por tanto, cualquier intromisión o acción con tendencia a alterar esta disposición deberá ser sancionada por el ordenamiento jurídico, el involucrar esta conducta dándole consecuencias penales amplía el espectro de los delitos informáticos. El derecho responde a lo que la sociedad demanda, en este caso, la importancia de los datos

personales que circulan a través de los sistemas informáticos, hizo que apareciera una nueva modalidad de criminal, conocido como el delincuente informático y su principal objetivo consiste en extraer información sensible de los individuos; sin duda, la conducta descrita obedece a la necesidad de sancionar a desarrolladores de *software* que se dedican a crear virus informáticos que con frecuencia comprometen información sensible.

> 6- Artículo 269f: violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Al respecto, es importante aclarar que la Ley 1.266 de 2008 definió el término dato personal como "cualquier pieza de información vinculada a una o varias personas determinadas o determinables que puedan asociarse con una persona natural o jurídica". Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la Ley obliga a quien "sustraiga" e "intercepte" dichos datos a pedir autorización al titular de los mismos.

Este tipo penal se refiere de forma puntual a las actividades de manipulación fraudulenta de información, las cuales puedan resultar en la violación del derecho a la intimidad de una persona, en especial cuando se trata de sustraer o interceptar estos datos, la precisión que se hace frente a la noción de protección del dato personal conduce a establecer de forma clara, cómo la legislación busca brindar un marco de regulación para quienes administran estos datos, teniendo en cuenta la relevancia de este tipo de información.

> 7- Artículo 269g: […] suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente

en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya un delito sancionado con la pena más grave […] (Ley 1.266 de 2008, República de Colombia).

La conducta descrita se denomina *phishing*, esta práctica común trata de delitos financieros y es una de las conductas que vulnera de forma clara el derecho a la intimidad y la privacidad de los datos de las personas; usualmente, por medio de falsos mensajes de entidades bancarias, o a través de redes sociales se engaña a quien termina suministrando información financiera confidencial, la cual es utilizada por los delincuentes para adquirir bienes y servicios sin autorización del verdadero titular. Entre las prácticas más frecuentes se encuentra la instalación de *software* destinado a capturar las claves del usuario, y posteriormente emplearlas para captar información o acceder a datos financieros para sustraer y hacerle fraude al usuario. Esta modalidad ocurre con bastante frecuencia en el sector bancario, los delincuentes envían correos electrónicos simulando una trasgresión a la cuenta del titular y le indican en el cuerpo del correo que deben acceder a un vínculo que imita a la página de ingreso seguro del banco, una vez allí el usuario suministra sus datos y así se perfecciona el delito.

La ley 1.273 agrega como circunstancia de mayor punibilidad, en el artículo 58 del Código Penal (República de Colombia, 2000), el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos o telemáticos.

La ley de protección de datos

El avance más reciente en este sentido proviene —en nuestro país— de la Ley Estatutaria 1.581 de 2012, la Ley pretende desarrollar, de acuerdo a su objeto, un aspecto esencial del derecho al *habeas data*, en particular, el derecho a conocer, actualizar y rectificar información personal. Conforme a lo expresado previamente en el análisis sobre el artículo 15 constitucional, esta norma aporta su aplicación en conjunto con la garantía del artículo 20, conjugando la libertad de expresión y el derecho a la intimidad personal y familiar, la expedición de esta Ley obedece a la necesidad de responder y dar un tratamiento legislativo a la problemática que en párrafos precedentes había sido analizada por medio de la jurisprudencia.

Mecanismos legales de protección

Entre los aportes más destacados de la Ley, es importante señalar que se incorporan algunas definiciones legales que se esperan —a partir de su vigencia— marquen una importante diferencia en el manejo de la información personal.

a) **Titular**: persona natural cuyos datos personales sean objeto de Tratamiento. Llama la atención de esta definición que la misma excluye —en consecuencia— como titular a las personas jurídicas, indicando que el ejercicio de las atribuciones relativas al derecho a conocer, actualizar y rectificar información radica esencialmente en personas físicas, y se excluye a las personas jurídicas. Esta definición legal podría considerarse contraria a alguna jurisprudencia de la Corte Constitucional, la cual había indicado que el derecho a conocer, actualizar y rectificar información en los términos del artículo 15 Superior era un derecho que podría ejercerse también por personas jurídicas (Sentencia T-552, 1997).

b) **Encargado del Tratamiento**: persona natural o jurídica, pública o privada, que por sí misma o en asociación con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

c) **Dato personal**: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, sobre esta definición y siendo coherentes con el concepto previo, la Ley señala que el concepto de dato personal obedece a la información que se pueda asociar o vincular a un titular.

d) **Tratamiento**: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. La definición de Tratamiento que brinda la ley es omnicomprensiva y como se puede interpretar de la misma ley, ha excluido intencionalmente al parecer a las personas jurídicas como titulares, pues en el tráfico jurídico quienes se encargan del manejo de este tipo de datos son las personas jurídicas, y aquellos que deben de administrar y crear las bases de datos en las cuales reposan los datos de las personas naturales, es decir, el objeto mismo de la ley.

e) **Base de datos**: conjunto organizado de información personal que es objeto de Tratamiento. Sobre este concepto de base de datos, habría sido interesante que la Ley hiciera remisión a la Ley 23 de 1982 y a lo pertinente en materia de derechos de autor, de manera que la legislación en materia de protección de datos fuera convergente con la normatividad en materia de los objetos de protección por parte del derecho de autor.

f) **Responsable del Tratamiento**: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos o el Tratamiento de los datos. Sobre este punto la definición señala quién es el sujeto activo de la Ley, desde el punto de vista de que el responsable del tratamiento será el obligado principal en virtud de las disposiciones de las cuales trata la Ley.

g) **Autorización**: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales; el concepto aquí expresado, sencillamente pone de presente la esencia del derecho a la intimidad, el cual es —como se indicó en párrafos precedentes— un derecho de carácter disponible. Sobre el punto, la jurisprudencia Constitucional ha indicado: "Reiteradamente esta corporación ha señalado que el derecho a la intimidad permite y garantiza en los asociados, el poder contar con una esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerado un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico". En ese orden de ideas, y al no ser un espacio que forme parte del dominio público, obedece al estricto interés de la persona titular del derecho y por consiguiente no puede ser invadido por los demás. Por esta razón, ese espacio personal y ontológico, sólo "puede ser objeto de limitaciones" o de interferencias "en guarda de un verdadero interés general que responda a los presupuestos establecidos por el artículo 1 de la Constitución". La jurisprudencia de la Corte Constitucional, tal y como se ha dicho, ha señalado que el derecho a la intimidad es entonces inalienable, imprescriptible y solo susceptible de limitación por razones legítimas y debidamente justificadas constitucionalmente" (Sentencia T-517 1998).

Además de las definiciones, un mecanismo esencial es el previsto en el artículo 9 del Decreto 1.377 de 2013 (el cual reglamentó la Ley 1.581), el cual consagra el derecho a revocar o restringir la autorización para el tratamiento de datos. De este artículo se desprende que las autorizaciones para la disposición de datos no constituyen un permiso atemporal, sino que al contrario, se trata de un derecho que conlleva en sí mismo por esencia la posibilidad de constante disposición por parte del titular.

Otro mecanismo esencial de protección se deriva de la creación de dos categorías de datos sensibles a saber:

1- Datos que puedan ser empleados para generar discriminación, tales como los que indican preferencia política, origen étnico, pertenencia a agrupaciones religiosas o sindicales o a organizaciones de derechos humanos.

2- La otra gran categoría de datos sensibles es la que contiene datos de menores de edad, los cuales constituyen especial objeto de protección. Cabe aquí la posibilidad de cuestionar el consentimiento de menores de edad que hoy en día citen en cuentas en redes sociales tales como Facebook o Twitter y el permiso sobre la disponibilidad de dichos datos, el cual estaría viciado.

Como garantía, se consagran responsables y encargados del tratamiento de información, quienes tienen el deber de dar respuesta sobre las solicitudes de conocer, actualizar o rectificar información personal en un término máximo de 15 días hábiles, contados después de haber recibido la solicitud por parte del titular del dato. A continuación presento —de forma sucinta— las sanciones previstas por la ley ante el incumplimiento de las disposiciones legales

Sanciones previstas por la ley

La legislación nacional contempla como sanción de carácter administrativo además de los tipos penales arriba descritos, a imponer dependiendo de la gravedad de la conducta:

- Multas de carácter personal e institucional hasta por 2.000 SMLMV.
- Suspensión de actividades relacionadas con el Tratamiento hasta por seis meses. En acto de cierre se indicaran los correctivos.
- Cierre temporal de las operaciones si no se adoptan los correctivos.
- Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

El órgano que designa la Ley para imponer estas sanciones, así como para ejercer las facultades relativas a la vigilancia y control de los encargados y responsables de datos personales, es la Superintendencia de Industria y Comercio.

Otra de las obligaciones que surgen a partir de la creación del Decreto consiste en que la Superintendencia tendrá a su cargo también el Registro Nacional de Bases de Datos, en ejercicio de sus funciones debe crear un directorio público de las bases de datos sujetas a tratamiento que operan en el país, el objetivo de este directorio será conocer:

- Realidad de las bases de datos del país
- Flujo y tipo de datos
- Quién o quiénes adelantan su tratamiento
- Finalidad
- Políticas de tratamiento

El registro de bases de datos, así como el directorio, aún no han sido objeto de reglamentación. Para implementar estas funciones de administración, seguimiento, control y sanción se crea la Delegatura para la Protección de Datos Personales dentro de la Superintendencia de Industria y Comercio.

El gran objetivo que se busca con esta iniciativa consiste en organizar, a través del directorio, las numerosas y diferentes bases de datos que hoy coexisten en el país. El centro de este proyecto radica justamente en proteger el derecho a la intimidad de los miembros del Estado colombiano, quienes a partir de la información contenida en este directorio, tendrán la oportunidad de acudir ante un órgano estatal como lo es la Superintendencia, que en desarrollo de sus funciones de vigilancia, contará con amplias facultades para regular y sancionar a los encargados del tratamiento de datos cuando excedan u omitan alguna de las obligaciones constitucionales o legales que se han inscrito en nuestro ordenamiento jurídico, las cuales conducen a una garantía efectiva del derecho a la intimidad.

Las facultades otorgadas a la Superintendencia de Industria y Comercio, especialmente la de imponer sanciones pecuniarias, constituyen una herramienta importante para crear un ambiente de buenas prácticas respecto a las personas naturales y jurídicas, encargados del tratamiento de datos personales, en vista de su relación directa con la protección del núcleo esencial mismo del derecho a la intimidad.