Seguridad informática y tratamiento de datos en base a una protección integral de derechos en Colombia

Resumen: En este artículo se plantea la idea de que debe existir una comprensión dogmática general e integral que no separe de manera tajante el tema de la protección en los sistemas informáticos con el tema de la protección de datos. Una separación que se puede apreciar en el derecho penal colombiano pero que el derecho administrativo puede ayudar a suplir desde la dogmática. Por otra parte, se toma en consideración que desde la pandemia por Covid 19 el uso de tecnologías de la información se ha extendido de manera abrumadora, razón por la cual, si bien se ha potencializado la comunicación también ha sucedido lo mismo con el delito cibernético. Partiendo de ahí se plantea la pregunta de cuál sería la mejor forma de actualizar las leyes de protección de datos y de sistemas informáticos en Colombia teniendo en cuenta el actual uso extensivo de las Tics. Se propone que la protección de derechos fundamentales debe ser la guía a seguir y que en la comprensión de la seguridad digital se requiere tener en cuenta que en el tratamiento de datos o de sistemas informáticos ciertas pequeñas equivocaciones deliberadas o no pueden dar lugar a graves consecuencias para los usuarios.

Palabras clave: sistemas informáticos, protección de datos, seguridad informática, Derechos Fundamentales, delito informático.

Abstract: This article raises the idea that there should be a general and comprehensive dogmatic understanding that does not sharply separate the issue of protection in computer systems from the issue of data protection. A separation that can be seen in Colombian criminal law but that civil law can help to supply from dogmatics. On the other hand, it is taken into consideration that since the Covid 19 pandemic, the use of information technologies has spread overwhelmingly, which is why, although communication has been enhanced, the same has also happened with cybercrime. Starting from there, the question arises as to what would be the best way to update data protection laws and computer systems in Colombia, taking into account the current extensive use of ICTs. It is proposed that the protection of fundamental rights should be the guide to follow and that in the understanding of digital security it is necessary to take into account that in the processing of data or computer systems certain small deliberate mistakes or not can lead to serious consequences for the users.

Keywords: computer systems, data protection, Informatic security, fundamental rights, computer crime.

Introducción

La interacción digital y el uso de las tecnologías de la información se ha vuelto un aspecto de primer orden en la comunión contemporánea, de ahí que fenómenos digitales concretos como las finanzas digitales, las redes sociales, el internet de las cosas, las criptomonedas, las compras online o la digitalización de la justicia, entre otros fenómenos que tienen lugar en el ciberespacio, represente cada uno, por su novedad o complejidad, un desafío a las formas clásicas de reglamentación y normatividad. Una ampliación de los fenómenos sociales hacia lo digital que se ha potenciado mucho más desde la pandemia por Covid 19. Por ello mismo, al estar la información en un esquema digital, esta adquiere ciertas particularidades que deben ser estudiadas y comprendidas por el derecho (Estévez, 2020). Al respecto, cabe tener en cuenta que el tema de la seguridad digital puede ser abordada desde distintas ramas del derecho como el penal o el administrativo. En este artículo se pondrá en comunicación a dichas dos ramas, dando prioridad al momento de hablar de protección de datos personales a la parte administrativa y a las leyes y protocolos que la rigen en Colombia.

Hay que tener en cuenta que lo digital se encuentra tan presente en la vida contemporánea que dicho tipo de material tiene una gran injerencia en la vida real. Las evidencias digitales, por poner un ejemplo, son entendidas como toda información generada, almacenada o trasmitida a través de medios electrónicos y de las que se puede disponer o usar con algún fin (Toro, 2019), evidencias que pueden existir en forma de un video, una conversación de chat o una foto, y las cuales pueden ser piezas relevantes e imprescindibles de información (Gamboa, 2005; Nobles, Narváez y Rúgeles, 2020).

El avance de la comunicación en el terreno de la tecnología implica una mutación de los móviles que usan los delincuentes para consumar actos delictivos, razón por la cual el bien jurídico tutelado debe contar con una nueva comprensión de los fenómenos digitales, con unas nuevas tipificaciones que correspondan con las actuales acciones criminales que se dan a través de las tecnologías de la comunicación y con una dogmática que permita en un juicio hacer valoraciones correctas de los distintos actos delictivos.

En cuanto a lo que atañe a la seguridad informática, es importante hacer la distinción entre los delitos vinculados al internet en general y los delitos vinculados propiamente a los sistemas informáticos y de protección de datos, en cuanto que los primeros protegen otros bienes jurídicos constitucionales como el patrimonio, la

intimidad, el buen nombre, mientras que los segundos tratan sobre la calidad o buen funcionamiento de los sistemas informáticos y de la información en sí misma (Guarnizo, 2020). No obstante, en este texto se presentará la idea de que debe existir una comprensión integral que englobe ambos aspectos pues el derecho actual posee cierta tendencia a diferenciarlos y separarlos en exceso. Partiendo de ahí la pregunta a resolver es: ¿qué aspectos se deben tener en cuenta a fin de actualizar las leyes de protección de datos y de sistemas informáticos en Colombia ante la enorme presencia de lo digital y de las demandas de seguridad en la época poscovid 19?

A fin de indagar en la pregunta anterior se plantea el siguiente objetivo general: Analizar las luces y sombras de las actuales leyes de protección de datos a fin de determinar un esquema dogmático general que permita actualizarlas a la nueva época de predominio de las tecnologías de la información.

Con el objetivo general descrito como guía a seguir se tendrá en cuenta un primer objetivo específico el cual es el siguiente: Analizar las actuales leyes de protección de datos y de protección de sistemas informáticos. Dicho análisis se realizará principalmente en el apartado primero en el cual se presentará la ida de que dentro del derecho administrativo no se puede perder de vista el entendimiento que se hace en derecho penal de sistema informático, en cuanto que la seguridad de los sistemas informáticos es esencial para la misma protección de datos. Un objetivo que permite acercar el análisis de las regulaciones de datos y de sistemas informáticos.

En cuanto al segundo objetivo específico este consiste en analizar y describir las nuevas problemáticas propias del avance en nuevas tecnologías que presenta la Ley de protección de datos en Colombia. Un objetivo con cual se empezarán a trazar las luces y sombras que se desea indagar en el objetivo general. Finalmente, el tercer objetivo específico estriba en analizar posibles formas de actualización de las leyes de protección de datos y nuevas formas de comprensión integral dentro de las mismas disciplinas del derecho. En cuanto a la metodología se hará uso de revisión de fuentes académicas y de fuentes jurisprudenciales, por tanto, a nivel analítico se trazará una línea argumental desde el primer capítulo hasta el último en la cual se indaga en primer lugar, mediante contraste de fuente y teorías, en las bases que soportan lo que se entiende por sistema de datos y sistemas informáticos, para más adelante mediante el estudio jurisprudencial de leyes, ahondar en las posibles mejoras ya para el último capítulo que pueden proponerse para as actuales leyes de datos.

1. La seguridad digital y los sistemas informáticos en Colombia

Antes de analizar cómo el derecho debe abordar o actualizar la protección de datos en Colombia ante las nuevas demandas de seguridad que plantea la misma tecnología, hay que tener en cuenta que el tema de dicha protección se haya ligada con el tema de la protección de los sistemas informáticos. Es decir, seguridad digital en general y seguridad de los sistemas informáticos son dos temas que van de la mano. Dos temas que, en cuanto a su reglamentación, sobre todo en cuanto a lo que respecta a la protección de sistemas informáticos, ha sido abordada por el derecho penal y descuidada en gran parte por otras disciplinas del derecho. Por dicha razón, se analizará inicialmente la comprensión reglamentada que existe actualmente sobre la protección de los sistemas informáticos, para posteriormente enlazar dicho tipo de protección con la protección de datos, es decir, se llevará la comprensión penal a un espectro mucho más amplio en el cual se pueda tener una visión dese el derecho administrativo y, en general, una visión más general y en clave de derechos de la protección de datos y de sistemas informáticos.

Sobre la protección de sistemas informáticos, cabe tener en cuenta que con la Ley 1273 del 5 de enero de 2009 el Congreso de la República de Colombia modificó el Código Penal, creando un nuevo bien jurídico tutelado el cual pasó a denominar: *De la protección de la información y de los datos.* Dicho bien jurídico protegido engloba la seguridad de la información, los datos y el adecuado funcionamiento de los sistemas informáticos. El objetivo o razón de ser de tutelar dicho bien estriba en preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones a fin de evitar conductas criminales a través de dichas tecnologías.

Entre las nuevas tipificaciones que se pueden encontrar en dicho bien tutelado están, por ejemplo, los siguientes delitos: Interceptación de datos informáticos (art 269 C), Uso de software malicioso (artículo 269E), Violación de datos personales (269F), Acceso abusivo a un sistema informático (art 269 A), Daño Informático (art 269 D), Obstaculización ilegítima de sistema informático o red de telecomunicación (269B), entre otros delitos.

Cabe decir que las tipificaciones de dicho nuevo bien jurídico tutelado corresponden al hecho de que existen múltiples formas de hacer uso o de alterar un sistema informático con fines perniciosos, por ello mismo se habla del daño a un sistema informático en cuanto que puede haber ocasiones en las que con dicho daño se haga, por ejemplo, perder información valiosa para una persona natural o jurídica. Se habla de acceso abusivo, pues con dicha modalidad se pueden violentar muchos otros bienes jurídicos tutelados (Huete, 2010; Davara, 2016). A fin de brindar un ejemplo mucho más concreto, cabe mencionar el delito de obstaculización ilegitima

de sistema informático (artículo 269B del Código Penal colombiano), la cual se tipifica de la siguiente manera:

> 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 mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

En otras palabras, dentro de la nueva esfera de delitos una acción como obstaculizar o impedir el acceso a un delito informático se puede tipificar como delito en virtud de que es una acción que atenta contra el derecho de acceso a la información. Cabe añadir que dicha obstaculización perniciosa tiene un fin y un propósito que es el que debe evaluar el derecho, es decir, se impide el acceso a la información o a un sistema a fin de violentar los derechos de una persona natura o jurídica. De esa forma, la obstaculización, deviene en un delito que es de mera conducta, un delito que entraña un acto de voluntad dentro de la esfera del comportamiento humano. También es un delito de modalidad permanente en cuanto que comprende una técnica en su ejecución en un entorno informático que se extiende en el tiempo hasta que el atacante decida finalizar su acción delictiva, la cual atenta contra la disponibilidad de la información al obstaculizar el funcionamiento normal y habitual de un sistema informático (Montañez, 2017).

Se trata por tanto de un delito que opera hoy día con dos presupuestos básicos: el primero de ellos, la tipificación normativa y en segundo lugar que mediante sentencia condenatoria se demuestre la existencia de una conducta típica, antijurídica y culpable; presupuestos que se traducen en la atipicidad de una conducta delictiva (Nobles, Narváez y Rúgeles, 2020).

El lapso en el cual transcurre la obstaculización del sistema informático y que atenta contra la disponibilidad de datos e información, es fundamental, en virtud de que, para una persona o una organización determinada, en ocasiones resulta decisivo cuánto tiempo sus sistemas están por fuera, puesto que entre más tiempo se genere dicha indisponibilidad, se podrían percibir mayores pérdidas en cuanto a dinero o recursos. Se podría incluso interrumpir todo el funcionamiento de una empresa u organización hasta el punto de ser acreedora de sanciones como podría pasar por ejemplo en el sector bancario (Montañez, 2017).

Con otros delitos atrás mencionados como el acceso abusivo o el daño informático también se puede interrumpir el funcionamiento de una organización, y se puede

exponer incluso datos contables privados o dañar momentánea o permanentemente dichos datos. La información es un aspecto vital del mucho contemporáneo por lo que interrumpir los cursos normales de esta bien puede ligarse a la violación de derechos, más aún considerando que la información y la comunicación potencian las capacidades de personas, colectivos y gobiernos (Conde, 2016). De ahí la importancia de tutelar el bien jurídico mencionado en la Ley 1273 de 2009. En el apartado siguiente, al momento de ahondar en las leyes y jurisprudencia, se dará un ejemplo de caso juzgado donde interviene la obstaculización de sistema informático.

La extensión comunicacional en torno a la tecnología implica asimismo una mutación de los móviles que usan los delincuentes para consumar actos delictivos, no obstante los delitos tipificados que se han mencionado corresponden al año 2009 con la Ley 1273 de dicho año, por lo que puede decirse que dichos delitos tienen una existencia bastante reciente en Colombia y que han tenido que afrontar además el hecho de que los cambios tecnológicos y los usos sociales de las Tics se dan a ritmos vertiginosos.

2. Redes y sistemas informáticos y los desafíos que plantean al derecho contemporáneo

De acuerdo con Nobles Pérez, Narváez Chala y Rúgeles Montoya (2020), la Ley 1273 con la cual Colombia adquiere un esquema de tipificación y un nuevo bien jurídico que son los sistemas informáticos, se construyó para:

> …dar herramientas a la política criminal para afrontar los retos riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos, procurando la protección de los datos personales y los bienes jurídicos titulados de la confidencialidad, integridad de los datos y sistemas informáticos. Es menester considerar lo previsto en la ley 1273 de 2009, que busco definir los tipos penales, las consideraciones, agravantes y atenuantes en conexión con los principios de necesidad, proporcionalidad y razonabilidad de las penas descritas.

Las redes informáticas pueden ser utilizadas para cometer delitos, como se observa en el párrafo anterior, siendo esa una de las principales novedades y evoluciones jurídicas en los últimos años en Colombia, razón por la cual se plantea de forma general, es decir, sin mencionar quiénes las pueden utilizar con dichos fines y cómo afectan la integralidad de derechos fundamentales. Del reconocimiento de la

potencialidad delictiva se desprende como presupuesto necesario para del delito, la existencia previa de un sistema de datos o de información. El elemento u objeto material sería la persona u objeto sobre la cual recae directamente el daño causado por la acción delictiva. Cuando se trata de una persona, ésta se identifica con el sujeto pasivo (Guarnizo, 2020).

En cuanto a lo que atañe al concepto de sistema informático, este puede entenderse como un conjunto de dispositivos y aplicaciones que hacen parte de una determinada red de datos la cual puede clasificarse en redes tipo LAN, MAN o WAN, dependiendo de la extensión física que abarque la red (Montañez, 2017). La red LAN (Local Área Network), o de área local, abarca un espacio físico de 200 metros a 1 Kilometro, por lo que suelen formar parte de casas o edificaciones, y suelen estar constituidas por equipos de cómputo alámbricos y/o inalámbricos. La red MAN (Metropolitan Área Network) o de área metropolitana, comprende un espacio de unos 50 Kilómetros, su función consiste en conectar las diferentes LAN mediante medios de transmisión como la fibra óptica o el microondas. Finalmente, la Red WAN (Wide Área Network), o de área amplia, posee una amplia cobertura geográfica; en cuanto que puede cubrir una ciudad o un país con el uso de medios más potentes como el satelital (España, 2003; Montañez, 2017). Por tanto, el acceso o la obstaculización de un sistema informático implicaría el acceso u obstaculización de dispositivos o aplicaciones conectados en una red.

.

Uno de los aspectos que hacen complejo a este nuevo tipo de derecho, es el hecho de que hay personas naturales o jurídicas que sí pueden acceder u obstaculizar un sistema informático en sus labores esporádicas o en sus labores cotidianas. De forma, que al momento de tipificar se hace necesario realizar una serie de diferenciaciones contextuales. Por ejemplo, en ocasiones es importante emplear el término “sin estar facultado para ello” más si se tiene en cuenta que alguien en cumplimiento de una actividad lícita genere, de forma premeditada o no, la posibilidad jurídica de obstaculizar el acceso a un sistema informático. En todo caso, como se mencionaba, se debe analizar el contexto y determinar los elementos de tipicidad, antijuridicidad y culpabilidad para determinar el delito (Montañez, 2017).

Además del ámbito penal, en lo que respecta al ámbito administrativo del derecho, cabe resaltar que la seguridad informática se engloba en un aspecto mucho más amplio que la comunicación como derecho. Un derecho con ciertas prerrogativas contemporáneas como la del hecho de que la comunicación sea potenciada en cuanto que permite la exigencia de otros derechos a la razón de la interconexión de la misma comunicación con otros aspectos de lo humano, de forma tal que la comunicación es una necesidad primaria del ser social (Loreti, 2005; Atarama, 2013). Por otra parte, las tecnologías de la información resultan tan relevantes hoy día, que estas han llegado muchas veces a convertirse en elementos de discriminación y exclusión en determinados contextos sociales o posibilitan la

misma discriminación, de ahí términos como el de brecha digital, o ciberbullyng (Cabero y Ruiz, 2018). Además de ello, en el plano delictivo también han incrementado y se han potencializado las formas de atentar contra los bienes jurídicos protegidos por la ley.

3. Otros aspectos de los delitos informáticos respecto a su tipicidad

Según el Tribunal Superior de Medellín, Radicado Nro. 2014-22638 del 27 de abril de 2017, los delitos que aparecen tipificados en la Ley 1273 de 2009, son de Tipo penal de naturaleza subordinada y compuesta, en cuanto que estructuran medios para consumar otros delitos. Por dicha razón, la Obstaculización ilegítima de sistema informático o red de telecomunicación o el acceso abusivo a un sistema informático, son tipificaciones que pueden dar lugar a un concurso de delitos. Un caso común sería aquel en el que si en un actuar delictivo además de obstaculizar o acceder abusivamente se borra o destruye la información. Por lo mismo muchos delitos informáticos son considerados de naturaleza intermedia, puesto que no solo se afecta el bien jurídico de protección de sistema informático y protección de datos sino otros bienes jurídicos, en otras palabras, la violación de datos y sistemas informáticos tiene como fin en muchas ocasiones afectar bienes jurídicos de personas naturales o jurídicas. Es en dicho aspecto que los delitos informáticos concuerdan con los delitos vinculados al Internet.

Los delitos vinculados al internet en general se diferencian de los delitos vinculados propiamente a los sistemas informáticos y de protección de datos, en cuanto que los primeros protegen los bienes jurídicos constitucionales como el patrimonio, la intimidad, el buen nombre, mientras que los segundos tratan sobre la calidad o buen funcionamiento de los sistemas informáticos y de la información en sí misma (Guarnizo, 2020). No obstante, como se mencionó en el párrafo anterior, lo que sucede es que los delitos vinculados a sistemas informáticos suelen ser delitos de naturaleza intermedia o delitos derivados que terminan afectando un derecho mientras que en los delitos vinculados al Internet la afectación de un derecho constitucional es más directa y patente, razón por la cual en este texto se presenta la idea de que ambos tipos de delitos no deberían estar tan tajantemente separados, pues en últimas hacen alusión a la defensa de los derechos constitucionales.

Cabe recordar que la figura jurídica de concurso se halla contenida en el Artículo 31 del Código Penal, el cual plasma que el que con una sola acción u omisión o con varias acciones u omisiones se pueden infringir varias disposiciones de la ley penal o varias veces la misma disposición, por lo que quien en ello concurra quedará sometido a la que establezca la pena más grave y que ésta a su vez, se puede aumentar en otro tanto. En otras palabras, la importancia de contemplar el mayor

daño hecho estriba en la importancia de salvaguardar y dimensionar apropiadamente la protección de la dignidad humana.

Sobre el concurso efectivo, este se presenta, de acuerdo con la Sentencia C-464 de 2014 de la Corte Constitucional, cuando uno o varios comportamientos de la misma persona coetáneamente, encuadran en varios tipos penales que sin excluirse el uno del otro, deben aplicarse simultáneamente. Es decir que la Obstaculización ilegítima de sistema informático o red de telecomunicación (269B), puede presentarse junto a: Uso de software malicioso (artículo 269E), Violación de datos personales (269F), Acceso abusivo a un sistema informático (art 269 A), Interceptación de datos informáticos (art 269 C), Daño Informático (art 269 D). En lo que respecta al concurso aparente, de acuerdo con la Sentencia C-464 de 2014 de la Corte Constitucional, se configura cuando ilusoriamente existe una concurrencia de tipos penales sobre una conducta. Esto es, cuando una misma conducta punible se subsume en varios tipos penales diversos y excluyentes, razón por el cual, el juez deberá decidir o resolver sobre cuál de ellos basa el comportamiento en estudio.

En el caso de la Obstaculización ilegítima de sistema informático o red de telecomunicación o el Acceso abusivo a sistema informático, al ser un tipo penal de naturaleza subordinada y compuesta en cuanto es un tipo de naturaleza intermedia, dicho delito suele tener lugar a razón de afectar otros bienes jurídicos o derechos fundamentales, por lo cual el juez, como se verá en el apartado jurisprudencia, no solo asocia sino que deja subordinado con otros delitos más grandes como el de hurto por medios informáticos y otros delitos semejantes.

4. Nuevas problemáticas en torno a la protección de sistemas informáticos y de datos personales

En el apartado anterior se sentaron las bases para diferenciar entre sistema de datos y sistema informático. En el presente apartado se profundizará en las nuevas problemáticas que resultan de dichos dos sistemas, teniendo en cuenta el contexto más inmediato. Dicho contexto, parte de tener en cuenta las medidas de reclusión a modo de cuarentenas al inicio de la pandemia de Covid 19 propiciaron que muchas personas se volcaran hacia los medios digitales y las tecnologías de la información para cumplir a distancia con sus labores, estudios y trabajos. Dicho fenómeno, por tanto, también propició que los medios digitales fueran mucho más usados para compras o intercambios de todo tipo por Internet. Por otra parte, la pandemia de Covid 19 también incrementó las desigualdades en la región latinoamericana agravando fenómenos como el desempleo (OECD et al., 2020b). La escasez de recursos ha agudizado, asimismo, y aun cuando haya muchos otros

factores en juego como la cultura, las distintas formas de estigmatización, xenofobia, discriminación y exclusión social.

En otras palabras, vivimos en una época en la cual han aumentado los niveles de pobreza e inequidad e incluso los problemas y trastornos psicológicos a la par que la vida cotidiana se ha volcado de golpe a los espacios digitales. En otras palabras, el espacio digital se ha convertido en un espacio propicio para violentar a las personas de múltiples formas, no solo por delitos vinculados a robos de datos y capital financiero, sino delitos de crimen de odio y exclusión con la particularidad de que en la red muchas interconexiones no tienen un emplazamiento geográfico claramente identificable, sino que por el contrario trazan una red de interconexiones trasnacionales. De hecho, el mismo crimen contra delitos informáticos suele tener una dimensión trasnacional. Se hace necesario ante dicho panorama que los parámetros constitucionales también alcancen de forma contundente los espacios digitales, razón por la cual se hace necesario que las distintas legislaciones traten el tema de cómo deben operar las empresas de sistemas informáticos y de aplicaciones en su respectivo territorio, razón por la cual la dimensión corporativa trasnacional también debería tener un apartado importante en la parte del código penal en la cual se tutela el bien jurídico de sistema informático y de datos personales.

Otro reto o nueva problemática ligado a los sistemas informáticos tiene que ver con el hecho de que nuevas técnicas para impedir el acceso o para obstaculizar o para acceder abusivamente o dañar un sistema informático aparecen y se actualizan cada día en virtud de la misma cualidad de las tecnologías de la información las cuales son dinámicas y cambiantes en el tiempo. La técnica más común es la generación de virus, que son programas de computadora que tienen la facultad para reproducirse y transmitirse automáticamente y que generan afectaciones en el rendimiento de un sistema computacional. El delincuente informático instala dicho programa para generar el algún tipo de falla en el software de la máquina, con lo que espera como resultado la afectación de la integridad o disponibilidad de la información, como por ejemplo el no poder acceder al sistema.

Otra técnica para obstaculizar e impedir es la denominada Bomba Lógica, la cual es generada por algún actor que tenga acceso y privilegios de usuario que le permita instalar software malicioso (es decir, virus) el cual es configurado para ejecutarse con alguna condición preestablecida, afectando la integridad, confidencialidad o disponibilidad de la información (Guarnizo, 2020). Cabe decir que dichas técnicas también se actualizan y cambian a la par con los cambios de tecnologías. De esa forma, los actos delictivos en el mundo actual tienen entre sus muchas problemáticas tres que destacan por sobre muchas otras que son el uso recién y casi de golpe de los entornos digitales para un gran número de tareas de compras e intercambios y ocio, la dimensión trasnacional de los entornos y redes digitales y

la continua actualización de técnicas de acceso abusivo, obstaculización y robo de información, entre otras acciones delictivas.

Cabe decir que las medidas que toman personas y organizaciones para protegerse de ciberataques y violaciones a sus sistemas informáticos, también se actualizan continuamente e incluso han dado lugar principalmente en la esfera empresarial a que se adopten protocolos y una serie de normas y medidas preventivas. Protocolos y normativas que, de acuerdo con Guarnizo (2020), suelen recomendar el evitar realizar tareas sensibles para la empresa desde el teléfono celular, la importancia de implementar una apropiada política de almacenamiento de información en la nube, el uso del correo corporativo para tareas estrictamente empresariales, la implementación de antivirus, antimalware y antifishing e incluso la importancia de la ciberresiliencia para aquellos casos en los que personas naturales o jurídicas han sido víctimas de un delito informático.

Otra problemática tiene que ver con el hecho de que muchas veces no es posible identificar qué tipo de violación a un sistema informático se ha llevado a cabo, más aún teniendo en cuenta que dichos actos delictivos pueden ser llevados a cabo por personas que se hallan tranquilamente en su casa con un equipo de computo con alguna seguridad para evitar su detención o dirección de IP (dirección del protocolo de Internet). Una razón más para evitar que haya una separación excesiva o demasiado contundente entre delitos informáticos y delitos vinculados al Internet. Cabe tener en cuenta que en ese sentido la reglamentación específica sobre la protección de datos ayuda a solventar los casos en los que no es posible identificar el daño al sistema informático puesto que finalmente la afectación es hacia ciertos datos.

5. El régimen general de protección de datos en Colombia ante las nuevas demandas de seguridad informática

Cabe empezar por mencionar la Ley 1581 de 2012 mediante la cual se expidió el Régimen General de Protección de Datos Personales, el cual tiene por objeto proteger el derecho a la comunicación y desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos. Es decir, una ley con una base constitucional en derechos.

A modo de ejemplo, el Artículo 4 del Decreto 1317 de 2013 que regula la mencionada Ley 1581 de 2012, plasma lo siguiente sobre la recolección de datos personales:

> Artículo 4. Recolección de los datos personales. En desarrollo de los principios de finalidad y libertad, la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a ~a normatividad vigente. Salvo en los casos expresamente previstos en la Ley, no se podrán recolectar datos personales sin autorización del Titular.

También se expresa, además de los fines con los que debe operar una recolección de datos, el hecho de que no se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar el tratamiento de datos personales. En el artículo 5 del Decreto 1317 de 2013 se habla de la importancia de la autorización lo cual entraña a su vez la importancia de que quien brinde el consentimiento para el tratamiento de sus datos personales, esté debidamente informado sobre para qué serán aquellos utilizados. Se menciona asimismo que de haber cambio en las políticas del tratamiento de datos se deberá contar con una nueva autorización.

En otras palabras, regular la protección de datos en base a la protección de derechos fundamentales compensa problemáticas como la de no poder identificar de qué forma se ha accedido a un sistema informático y el hecho de que las técnicas de obstaculización, acceso o daño abusivo se actualicen continuamente. Es importante que la regulación cuente además con una serie de principios básicos. En la legislación colombiana los principios rectores del tratamiento y protección de datos están contemplados en la Ley 1581 de 2012 en el artículo 4.

El primero en mención es el Principio de legalidad en materia de Tratamiento de datos, el cual hace alusión a la importancia de ajustarse a la ley. El segundo es el Principio de finalidad que atañe a que el tratamiento de datos debe obedecer a una finalidad legítima. El tercero es el Principio de libertad el cual expresa que el tratamiento de datos solo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. El cuarto es el Principio de veracidad o calidad que dice que la información debe ser veraz, completa, exacta, actualizada, comprobable y comprensible, por lo cual se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error. El quinto es el Principio de transparencia. El sexto es el Principio de acceso y circulación restringida en el cual se contempla que la información tratada no pude hacerse publica sin autorización o acción legal y que el tratamiento sólo podrá hacerse por personas autorizadas por el Titular yo por las personas previstas en la ley. El séptimo es el Principio de seguridad que atañe a que la información debe ser tratada con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros. Finalmente, el octavo principio es el Principio de confidencialidad el cual menciona que todas las personas que intervengan en el tratamiento de datos personales que

no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información.

Los principios mencionados en el párrafo anterior permiten ligar la esfera de datos personales con la esfera de la ética en derechos humanos, en cuanto que los espacios digitales e Internet son entornos dinámicos y complejos que requieren de una normatividad con unos estándares o vectores integrales sustentados con contenidos valorativos que reconozcan la importancia de lo humano. En ese sentido, otro acierto de la Ley 1581 de 2012, es el reconocimiento y diferenciación de los llamados datos sensibles, los cuales aparecen en el artículo 5 de la siguiente forma:

> Artículo 5°. Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Sin embargo, pese al reconocimiento respecto a la importancia de los datos sensibles en la práctica se presentan situaciones en las que resulta difícil delimitar ciertas fronteras y en los que quienes comparten ciertos datos se escudan en el derecho de libre expresión, razón por la cual por medio de fenómenos como el “voz a voz”, por ejemplo, muchas personas pueden poner a circular datos sensibles de otra persona (González, 2012). En todo caso, la ley ofrece un marco jurídico de protección en el cual se prohíbe el tratamiento de datos sensibles excepto cuando el titular dé una autorización explícita, en los casos en los que la ley demande dicho tratamiento o en aquellos casos en los que el tratamiento de datos sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. También es importante considerar el tratamiento de datos de niños, niñas y adolescentes, cuyos datos también pueden considerarse en la categoría de datos sensibles (González, 2012). Por otra parte, no se debe olvidar que, al momento de juzgar, existen figuras como la del concurso aparente que se mencionaba en el apartado anterior.

Hasta este punto se puede afirmar que el estado colombiano cuenta con un marco general bastante apropiado para penalizar delitos informáticos y un marco también apropiado para entender el tratamiento e datos personales, no obstante la crítica ante el hecho de que en ocasiones los delitos informáticos no son penalizados de forma contundente está sobre la mesa en cuanto que los clásicos delitos físicos y directos son mucho más fáciles de detectar y probar y el hecho de que al ser los

delitos informáticos delitos derivados, muchas veces al ser detectados si estos no se conectan con los derechos fundamentales y tipificaciones penales más generales, pueden derivar en penas pequeñas y poco contundentes. Es importante en ese sentido que desde los entes investigativos y judiciales se refuerce el presupuesto en el área delitos y seguridad informática. Por otra parte, hay que tener en cuenta que tanto las víctimas como los victimarios no solo son personas naturales sino también jurídicas, de ahí la importancia de hablar de compliance y responsabilidad corporativa (Galán, 2021). Un tema que será ampliado en el apartado de este artículo.

Hay que tener en cuenta que leyes que regulan el derecho informático en Colombia son relativamente recientes, sin embargo, por ello ismo deben examinarse y aprobarse con cierta prioridad, puesto que el avance de la tecnología no da espera. Cabe recordar que en materia probatoria destaca el artículo 8° de la Ley 527 de 1999, según el cual todo documento almacenado electrónicamente que se aporte al proceso judicial debe corresponder al contenido en el medio electrónico original (por ejemplo, un celular o un computador). Es decir, desde 1999 se habla de originalidad del material probatorio digital. En dicha ley se define además el mensaje de datos como “la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos o similares, como, el intercambio electrónico de datos, internet, el correo electrónico, el telegrama, el telefax, entre otros”.

En la Ley Estatutaria 270 de 1996 de la Administración de Justicia, se reguló el ejercicio de la justicia en el país, facultando a jueces y magistrados para valorar los medios de prueba que acarree consigo la innovación de la tecnología. Se puede mencionar de igual forma en el espectro del derecho informático, la Ley 527 de 1999, "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones" y en la cual se define y presenta el concepto de mensaje de datos.

De esa forma, hasta el año 2009 no se hablaba de obstaculización de sistema informático, pero se trataba la criminalidad informática por medio de los delitos cibernéticos del Código penal y los procesos se llevaban a cabo siguiendo lo dispuesto en el Código de Procedimiento Penal. Una vez creado el tipo penal de Obstaculización o de Acceso abusivo o de Daño a sistema informático, se puede observar en la jurisprudencia examinada que lo común es que dicho tipo penal no se juzgue por sí solo sino en conjunto con otros delitos. En general delitos cuya finalidad es el hurto y dentro de los cuales se encuentra el fraude con tarjetas de crédito y débito, o el robo en cajeros automáticos (es decir, delitos de tipo penal de naturaleza subordinada y compuesta). Finalmente, y a fin de poner un ejemplo de cómo interviene el delito de hurto junto a los delitos informáticos como derivados y cuáles son las consecuencias penales, se tomará el Auto Interlocutorio de la Corte

Suprema de Justicia, e cual tuvo lugar en la Sala de Casación Penal nº 56591 del 08-09-2021. En dicho auto la Sala resuelve:

> Si es procedente admitir la demanda de casación presentada por el apoderado de Yury A.G. Núñez, en calidad de propietaria o poseedora de buena fe del automóvil marca Chevrolet Aveo de placas AUU 815, sobre el cual pesa una medida de suspensión del poder dispositivo, contra la sentencia dictada el 8 de octubre de 2019 por el Tribunal Superior de Buga, que confirmó, con algunas modificaciones, el fallo proferido por el Juzgado Segundo Promiscuo Municipal con funciones de conocimiento de Florida, V., y condenó a Roy Emir Guevara González, J.G. y Edwin Torres Castro como cómplices de los delitos de obstaculización ilegítima de sistema informático o red de telecomunicación, violación de datos personales y hurto por medios informáticos y semejantes, este último en grado de tentativa, todos agravados.

Como se puede apreciar, la apoderada del vehículo deseaba recuperarlo en cuanto que dicho medio de transporte era utilizado por quienes cometieron actos delictivos con tarjetas de crédito y cajeros informáticos. Se puede observar, por tanto, que la obstaculización de sistema informático como tipo penal puede hacer parte de un concurso de delitos y en cuanto tal tener efectos de penalidad incluso sobre objetos distintos a los objetos informáticos como en el caso del automóvil Chevrolet Aveo. Por otra parte, dejando un poco de lado la visión que proporciona el derecho penal, desde el ámbito administrativo, también se debe tener en cuenta que una pequeña equivocación en un sistema informático pude derivar en consecuencias bastante negativas para los usuarios de un sistema, de ahí la necesidad de que la ley de protección de datos se actualice especificando la importancia de que las empresas cuenten con rígidos protocolos de acción en sistemas informáticos. De hecho, a partir de lo expuesto también se infiere que no debe hablarse únicamente de protección de datos sino de “protección de datos y de sistemas informáticos”.

6. Perspectiva de derechos fundamentales y las responsabilidades corporativas e individuales del delito informático

Los delitos informáticos que se presentan en la Ley 1274 de 2009 surgieron debido a la creciente criminalidad en materia informática y a la necesidad que en el plano internacional demandaba la misma repercusión que tuvo el Convenio sobre la ciberdelincuencia de Budapest (2001), adoptado por el Consejo de Europa. Por lo que hubo la necesidad de comenzar a diseñar iniciativas como el Proyecto de Ley No. 042 de 2007, con el fin de modificar y adicionar algunos tipos penales del capítulo VII del Código Penal relativos a la «Violación a la intimidad, reserva e interceptación de comunicaciones”. Partiendo de ahí, la seguridad informática no fue directamente entendida en materia de derechos fundamentales sino como un

avance necesario del derecho respecto al derecho internacional en el cual dicho bien figuraba y se comprendía como un bien jurídico intermedio.

En otras palabras, a través de la afectación de datos y sistemas informáticos se pueden afectar derechos individuales, pero la misma información y la dimensión comunicativa del ser humano no son vistos como derechos en sí mismos. El énfasis, por tanto, se puso sobre la computadora o los sistemas de procesamiento de datos involucrados en un delito. Finalmente, se optó el sistema legislativo para los delitos informáticos que estriba en diseñar un título adicional para ser incluido en el Código penal, porque si bien, era más técnica la expedición de una ley especial, aquella podría perderse en el entramado del ordenamiento jurídico, sin merecer la atención requerida por parte de administradores de Justicia. Un paso importante para la administración de justicia, no obstante, el énfasis recayó en los sistemas informáticos y no tanto en el tratamiento de datos la cual hoy día opera con una ley especial (Ley 1581 de 2012) y no en el entramado estrictamente penal, el cual puede ser visto como necesario para la defensa de los derechos fundamentales.

Cabe añadir que, desde el punto de vista jurídico, no hay mayor problema con que los delitos informáticos se entiendan como de naturaleza intermedia, en cuanto que la obstaculización, manipulación, o suplantación informática, tiene como fines, por ejemplo, el apoderamiento del dinero de otra persona, sino que el problema estriba cuando en juico no se asocia debidamente el delito informático con aquellos otros fines o cuando las violaciones al tratamiento de datos solo conducen a la posibilidad de que los usuarios de distintos sistemas presenten quejas ante la Superintendencia de Industria y Comercio por infracciones a la Ley 1581 de 2012. Un aspecto sumamente importante puesto que con los datos de una persona hoy día se puede afectar sus finanzas y negocios, imagen, proyecto de vida, entre otros aspectos de la vida social.

Si bien existe la posibilidad de que se pueda acceder de forma gratuita a lo datos objeto de tratamiento o a que se pueda revocar la autorización o de solicitar la supresión de ciertos datos, se requiere una penalidad mucho más fuerte que equipare los delitos de tratamiento de datos a los delitos de sistemas informáticos, es decir, que los delitos de tratamiento de datos sean penalizados con mayor rigor aun cuando sean considerados al igual que los delitos de sistemas informáticos como delitos de naturaleza intermedia y no solo que sean tratados por la Superintendencia de Industria y Comercio.

En ese sentido la penalidad también debe reforzarse y caer sobre las organizaciones o las personas jurídicas, en cuanto que muchas veces son las mismas organizaciones que poseen los datos las que hacen un uso indebido o irresponsable o muchas veces las organizaciones dejan de adoptar las medidas

necesarias para asegurar la trasparencia y al mismo tiempo el cuidado de los datos personales. Por otra parte, hay ocasiones en las que organizaciones o personas jurídicas se encuentran dentro de esquemas de corrupción o de lavado de activos en los cuales se valen de un uso indebido de sistemas informáticos y de tratamiento de datos para llevar a cabo sus operaciones criminales.

Cabe recordar que el crimen corporativo incluye una amplia variedad de conductas punibles como la evasión tributaria o la manipulación de estados financieros, entre otros delitos que implican en el mediano y largo plazo un detrimento patrimonial y fiscal del Estado fiscal que se refleja en la disminución de la capacidad de inversión de los países y en el incremento de la inequidad social (De La Torre, 2018). El soborno y el lavado de activos son dos delitos bastante representativos los cuales muchas veces pueden llegar a adoptar una dimensión trasnacional en la cual el uso indebido de sistemas informáticos y de datos personales se hace a través de varios países. Si bien el crimen corporativo puede ser juzgado por el derecho interno de los distintos Estados de acuerdo con la incidencia en estos es importante reforzar la cooperación internacional respecto a la seguridad informática y de datos personales y los tratados que permitan aplicar la extraterritorialidad de la ley penal.

En muchos Estados muchos delitos corporativos se remiten al derecho económico y se inscriben, por tanto, en el espectro de las sanciones administrativas. La lucha contra los dineros ilegales y la corrupción también contribuye a la lucha contra delitos como la trata de personas o el tráfico de drogas, por lo cual, y por muchas otras razones como el detrimento fiscal, la responsabilidad corporativa debería ser penal cuando tenga que ver con delitos como la manipulación o el fraude de datos con fines corruptivos o de hurto a usuarios, el soborno o el lavado de activos, y deberá ser administrativa cuando los temas a tratar sean temas administrativos (Costa, 2015). En otras palabras, hay que contemplar la necesidad de juicios puros para personas jurídicas y que dichos juicios contemplen los delitos informáticos y los delitos en el tratamiento de datos como delitos derivados con los cuales se afecta a los derechos fundamentales de las personas.

Cabe tener en cuenta que la responsabilidad penal corporativa tiene que ver con las penas impuestas no a una persona en particular sino a corporaciones, firmas o empresas por delitos cometidos en su contexto, en cuanto que las personas jurídicas no solo se pueden instrumentalizar, sino que ellas mismas pueden ser instrumentos para ciertos fines antijurídicos o contrarios a los derechos fundamentales y al ordenamiento legal (Bacigalupo, 2011). También se debe tener en cuenta que una vez probado un crimen corporativo una empresa puede llegar a recibir una multa, en cuanto que la mayoría de los delitos que se inscriben en el derecho penal económico y en la responsabilidad de las corporaciones, colindan con sanciones administrativas, hasta ser incluso disuelta en los casos más graves, no obstante, para delitos que afectan los derechos fundamentales deben hallarse

responsabilidades individuales claras dentro del sistema corporativo de acuerdo con los parámetros de antijuridicidad, tipificación e intencionalidad. De forma que haya una responsabilidad penal compartida entre la persona natural y la persona jurídica en vía de proteger los derechos de los demás miembros de la sociedad (Costa, 2015).

Hay que tener en cuenta que la responsabilidad penal corporativa se remite o se circunscribe a delitos cometidos en su contexto, es decir, que se derivan del desarrollo del objeto social de las empresas, razón por la cual “la responsabilidad penal de la empresa” se debe diferenciar de” la responsabilidad penal en la empresa” que es aquella en la cual la responsabilidad recae sobre los trabajadores de la corporación dentro de la corporación, como lo es por ejemplo el acoso sexual u otras conductas que pueden hacer uso de sistemas informáticos y de uso indebido de datos personales. Por lo general el carácter trasnacional de grandes delitos como el lavado de delito recae en la responsabilidad penal de la empresa mientras que conductas individuales concretas son objeto de la responsabilidad en la empresa. Un adecuado esquema de regulación penal debe proporcionar herramientas para realizar dicha distinción entre responsabilidad individual y corporativa.

En suma, los delitos en el tratamiento de datos requieren un esquema penal más rigurosos y tanto dichos delitos como los delitos informáticos requieren un esquema que permita distinguir responsabilidades individuales y corporativas y un esquema de sanciones para cada responsabilidad y nivel de responsabilidad que contemple multas, cierre de empresas, restricciones para contratar con el Estado, y penas intramurales según corresponda. También se requieren programas que trabajen en la transparencia informativa de las corporaciones por medio de las TICs, en la cooperación internacional y la alienación de órganos de control fiscal estatales, entre otros.

Conclusiones

En lo que atañe al tema de la seguridad informática, en Colombia suele hacerse una diferenciación o separación demasiado tajante entre protección de datos y protección de sistemas informáticos, siendo el primer aspecto apropiado por el derecho administrativo y el segundo por el penal, no obstante, en la realidad actual se encuentra que es a través de complejos sistemas digitales e informáticos en donde transitan muchos de los datos más importantes de las personas o de los usuarios de distintas empresas o corporaciones. En otras palabras, no se puede perder de vista que los datos personales, la comunicación y los medios que se emplean para la misma en el ámbito digital, se hayan relacionados con el ámbito de los Derechos Fundamentales y que tienen una relación estrecha e inseparable en virtud de las actuales tecnologías de la información.

El énfasis excesivo en el punto de vista penal si bien permite sancionar ciertas irregularidades en lo que atañe a la seguridad informática, desvía la atención del hecho que desde el punto de vista administrativo las empresas y entidades deben contar con rígidos protocolos de acción a fin de que los datos de las personas estén resguardados. Respecto al tema delitos informáticos se encontró que estos empiezan a ser contemplados en la Ley 1273 de 2009, aunque dicha ley no una ley especial sino un título y un bien jurídico añadido al Código Penal. No obstante, el tratamiento de datos sí aparece como una ley especial, en concreto, la Ley 1581 de 2012, por lo cual dicha dimensión requiere de mayor rigurosidad sancionatoria en cuanto que vivimos en una época en la cual los datos son vitales para finanzas y los negocios, para los proyectos de vida y para el trascurrir de la vida cotidiana, por lo que su uso indebido afecta drásticamente los derechos de las personas.

Por otra parte, en lo que tiene que ver con la naturaleza penal de los delitos informáticos, estos son considerados de naturaleza subordinada y compuesta en un bien intermedio, en cuanto que no solo suelen aparecer en concurso junto a otros delitos, sino que las finalidades son otras afectaciones a otros bienes bajo tipo delictivos como el hurto.

Por ello mismo la culpabilidad de obstaculizar un sistema o acceder abusivamente a un sistema no basta con la obstaculización o el acceso en sí mismos, sino que es necesario contemplar el dolo con el cual se quería afectar a una persona. Dolo que también está presente en los delitos vinculados al internet como el ciberbullyng. De ahí el hecho de que, si bien los delitos informáticos y los delitos en el tratamiento de tratamiento de datos pueden considerarse como delitos subordinados, al igual que los delitos vinculados al Internet, deben contemplarse dentro de un esquema de derechos fundamentales por los cuales se proteja no directamente al sistema informático sino a la persona o a las personas que son víctima de tales delitos.

Cabe tener en cuenta que hay muchos aspectos que hacen complejos los temas que se han tocado en este artículo como el hecho de que hay personas naturales o jurídicas que sí pueden acceder u obstaculizar un sistema informático en sus labores cotidianas. De forma que al momento de tipificar se hace necesario realizar una serie de diferenciaciones contextuales. También se hace sumamente necesario para el tipo de delitos de los que se han tratado, distinguir entre responsabilidades individuales y responsabilidades corporativas.

En suma, en esta investigación se llega a la conclusión de que las leyes de protección de datos deberían estar mucho más integradas con el tema de los sistemas informáticos. Dicho aspecto de la integración resulta necesaria a fin de

tratar la seguridad informática de forma amplia y de contemplar a futuro formas adecuadas de actualización de leyes, más aún teniendo en cuenta la actual tendencia desenfrenada por la vida digital, lo cual se incrementó con la pandemia de Covid 19 en la cual muchas personas y empresas comenzaron a hacer un uso mucho más extensivo de lo digital y de sistemas informáticos para sus distintas operaciones.

Finalmente, otras formas de actualización de leyes relacionadas con la seguridad informática y la protección de datos, tiene que ver con el hecho de que las empresas y entidades cuenten con protocolos de acción no solo para la protección de los datos en sí mismos sino para la protección de los mismos sistemas informáticos, razón por la cual es importante que dichos protocolos mencionen los sistemas de protección antivirus, por ejemplo, y la necesidad de que dichos sistema se vayan actualizando periódicamente. También se requiere que los protocolos mencionen formas de acción y de reporte ante las posibles equivocaciones en un sistema informático, pues a partir de una equivocación esta puede convertirse en un hecho derivado que un delincuente podría aprovechar para cometer actos ilícitos en sistemas digitales.

Referencias:

Atarama Rojas, T. (2013). Una propuesta para la formulación del derecho a la comunicación. Derecom, ISSN-e 1988-2629, Nº. 12 (dic-febr), 2013.

Bacigalupo, S. (2011). Ética empresarial y Responsabilidad penal de las empresas. Encuentros multidisciplinares, ISSN-e 1139-9325, Vol. 13, Nº 39, 2011 (Ejemplar dedicado a: ética, corrupción y transparencia en clave multidisciplinar), págs. 2-9.

Cabero Almenara, J. y Ruiz Palmero, J. (2018). Las Tecnologías de la Información y Comunicación para la inclusión: reformulando la brecha digital. IJERI: International journal of Educational Research and Innovation, ISSN-e 2386-4303, n. 9, 2018, págs. 16-30.

Conde González, F. J. (2016). El uso de redes sociales por parte de autoridades: consideraciones desde los derechos humanos. Defensor, Número 6, año XI v, junio 2016 Revista mensual de la Comisión de Derechos Humanos del Distrito Federal, p 16-21.

Costa Sanjurjo, P. (2015). Organización de empresas y responsabilidad penal corporativa. Tesis doctoral dirigida por Juan Soriano Llobera (dir. tes.), Jaume Guixà Mora (dir. tes.). Universitat Politècnica de Catalunya (UPC) (2015).

Davara Rodríguez. M. A. (2016). Los delitos informáticos. Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal, ISSN 0210-2161, Nº. 15-16, 2016, págs. 1825-1830.

De La Torre Lascano, M. (2018). Lavado de activos: estudio sobre la prevención (en especial referencia al caso ecuatoriano). Tesis doctoral dirigida por Eduardo A. Fabián Caparrós (dir. tes.). Universidad de Salamanca (2018).

España Boquera. M. C. (2003). Servicios Avanzados de Telecomunicaciones. 1ª ed. España. Ediciones Díaz de Santos, S.A. 2003. 816 p.

Estévez, J. F. (2020). El Derecho Digital, una rama del Derecho imprescindible para afrontar la sociedad de la información. Actualidad jurídica Aranzadi, ISSN 1132-0257, Nº 959, 2020, pág. 12.

Galán Muñoz, A. (2021). Compliance frente a delitos informáticos. Estudios penales en homenaje al profesor José Manuel Lorenzo Salgado / coord. por Miguel Abel Souto, Santiago B. Brage Cendán, Carlos Martínez-Buján Pérez, Fernando Vázquez-Portomeñe Seijas, Gumersindo Guinarte Cabada, 2021, ISBN 9788413971995, págs. 553-572.

Gamboa, R. H. (2005). Validez procesal de la información digital. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, ISSN-e 1909-7786, Nº. 1, 2005.

González Padilla, R. (2012). Protección de datos personales en posesión de particulares. Derecho Comparado de la Información, ISSN-e 1870-0594, Nº. 20, 2012, págs. 3-49.

Guarnizo Portela, M- P. (2020). La naturaleza jurídica de los delitos informáticos en Colombia. Universidad Nacional Abierta y a distancia. Escuela de ciencias básicas, tecnología e ingeniería. Especialización en seguridad informática.

Huete Nogueras, J. (2010). La reforma de los delitos informáticos. Diario La Ley, ISSN 1989-6913, Nº 7534.

Loreti, D. (2005). América Latina y la libertad de expresión. Bogotá, Colombia; Grupo Editorial Norma.

Montañez Párraga, A. C. (2017). Análisis de los delitos informáticos en el actual sistema penal colombiano. Tesis: Universidad Libre de Colombia.

Nobles Pérez, E. J., Narváez Chala, E. y Rúgeles Montoya, A. F. (2020). Ámbito de validez de la prueba electrónica en los delitos informáticos. Politécnico Grancolombiano.

Toro, N. (2019). el mensaje de datos y la prueba electrónica. Bogotá: Leyer.