Estudio jurídico frente a los obstáculos para la judicialización del delito de violación de datos personales en la ciudad de Medellín

Carolina Peña[1]

Resumen

Este artículo de reflexión tiene como objetivo analizar los obstáculos por los cuáles atraviesa la normatividad penal colombiana para judicializar las conductas punibles derivadas de la comisión del delito de violación de datos personales en la ciudad de Medellín. Se aborda una metodología cualitativa con un tipo de estudio descriptivo jurídico y un enfoque histórico – hermenéutico, en tanto se identifican las modificaciones introducidas en la Ley 1273 de 2009, sobre el tratamiento de los datos personales y se analiza en espacio temporal acotado desde la entrada en vigencia de la ley en mención hasta la fecha. Los resultados permitieron evidenciar que en la actualidad no se judicializa el delito de violación de datos personales en todos los casos denunciados; cuyas razones están direccionadas a la subjetividad de los especialistas judiciales, a la apelación de la Corte Constitucional mediante la revisión de los casos interpuestos a través de tutelas y el desconocimiento de las formas que tienen los delincuentes para cometer sus ilícitos y de esta forma poder asociarlos dentro del marco de la legislación penal planteada para tal fin. Se concluye que uno de los principales obstáculos por los que atraviesa la normatividad penal colombiana para la judicialización del delito de violación de datos personales en la ciudad de Medellín**,** es la dificultad para buscar que cada hecho jurídicamente relevante en cause a todos los responsables que participen o faciliten la comisión de los mismos, pues a veces el ente acusador se queda corto al pedir la judicialización de un eslabón, permitiendo que este sea reemplazado fácilmente para que la cadena estructural que comete el delito se afiance y pueda seguir creciendo en la consecución de víctimas de este flagelo.

Palabras clave. Obstáculos, judicialización, delitos, violación de datos personales Ley 1273 de 2009, Habeas data, ciberdelitos.

Abstract

This article of reflection aims to analyze the obstacles that Colombian criminal regulations go through to prosecute punishable behaviors derived from the commission of the crime of violation of personal data in the city of Medellín. A qualitative methodology is approached with a type of legal descriptive study and a historical-hermeneutical approach, while the modifications introduced in Law 1273 of 2009 are identified, on the treatment of personal data and it is analyzed in a limited time space from the entry in force of the law in question to date. The results showed that at present the crime of violation of personal data is not prosecuted in all the cases reported; whose reasons are addressed to the subjectivity of judicial specialists, to the appeal of the Constitutional Court through the review of the cases filed through guardianships and the ignorance of the ways that criminals have to commit their crimes and, in this way, to be able to associate them within the framework of the criminal legislation proposed for this purpose. It is concluded that one of the main obstacles that the Colombian criminal regulations go through for the prosecution of the crime of violation of personal data in the city of Medellín, is the difficulty in finding that each legally relevant fact causes all those responsible who participate or facilitate the commission of the same, because sometimes the accusing entity falls short when requesting the judicialization of a link, allowing it to be easily replaced so that the structural chain that commits the crime is strengthened and can continue to grow in the achievement of victims of this scourge.

Keywords. Obstacles, prosecution, crimes, violation of personal data Law 1273 of 2009, Habeas data, cybercrimes.

[1] *Posgrado en Derecho Penal y Criminología, Abogada, abogadaantioquia@gmail.com, Universidad Católica Luis Amigó*

Introducción

La globalización apoyada en las nuevas tecnologías y las redes de comunicación e información en la última década, han derivado un nuevo paradigma sociológico denominado la sociedad de la información, la cual ha sido fundamental para procesar, almacenar y comunicar la información de forma ilimitada e independiente; así mismo para la interacción en los distintos sistemas sociales en cualquiera de sus disciplinas: económica, política, antropología; entre otras, como el derecho en donde ha sido determinante para la creación de nuevos tipos penales que rompan con los "modos operandi" de los delitos; no solo los clásicos (hurto, lesiones personales, homicidio, entre otros), sino, los delitos informáticos que exigen nuevas valoraciones jurídicas para la identificación de los autores, la imputación, su intencionalidad, dentro de la comisión de los mismos (Silva, 2008)

En concordancia con lo anterior, cabe señalar, que, si bien es cierto que Colombia ha estado a la vanguardia en el tratamiento de los datos personales a partir de la mencionada Ley 1273 de 2009, además de la Ley Estatutaria de Habeas Data (ley 1266 de 2008); también es cierto que, no han sido suficientes esta herramientas legales para la judicialización del delito de violación de datos personales, toda vez que cada vez se visualiza el aumento de los casos en las distintas modalidades de este delito.

Según informe de la fiscalía general de la Nación, cada vez son más los casos de delito de violación de datos personales perpetrados tanto por personas de la comunidad en general, como de funcionarios públicos que violan información reservadas de las instituciones del Gobierno (Fiscalía, Registraduría, entre otras) (Fiscalía General del Nación, 2021), (Tendencias del Cibercrimen en Colombia 2019-2020).

Las diversas modalidades actuales que se presentan van desde la publicación intima de información, interceptación de datos informativos, hurto por medios informativos, extracción de claves secretas (entidades financieras), entre otras modalidades. Es evidente, de acuerdo a las conductas de algunos ciudadanos frente a la comisión de delitos relacionados con la

violación de los datos personales, que se requiere de leyes más estrictas y concretas; además, de penas y sanciones más altas para que estos puedan tomar conciencia del respeto por los derechos del otro en relación con la protección de la información y de los datos.

Lo anterior, sustentado en algunas Sentencias que la Corte Constitucional ha proferido como en el caso de la Sentencia T-020/14, a través de la cual se presenta acción de tutela en busca de la protección de los derechos fundamentales al *Habeas Data*, la dignidad humana y la igualdad, los cuales fueron vulnerados por el hecho de que la Corte Suprema mantuvo información en la página web sobre una condena impuesta en su contra, lo cual, además de considerarse actos de discriminación, ha impedido el ejercicio laboral y comercial como consecuencia de dichos registros. Ante esta situación, la Corte resuelve revocar la sentencia proferida y conceder el amparo del derecho fundamental al *Habeas Data* en relación a la protección de los principios de finalidad y circulación restringida (Corte Constitucional, 2014)

En consideración con lo anterior, y partiendo del interés académico y profesional, resulta importante realizar esta investigación con el fin de analizar los obstáculos por los cuáles atraviesa la normatividad penal colombiana para judicializar las conductas punibles derivadas de la comisión del delito de violación de datos personales en la ciudad de Medellín. Para desarrollar el tema de investigación se plantean tres objetivos específicos: en primer lugar se indaga si la judicialización en el delito de violación de datos personales se lleva a cabo en todos los casos denunciados; en segundo lugar, se determinan las razones por las cuáles no se penalizan todos los casos del delito de violación de datos personales; y, en tercer lugar, se analizan las estadísticas delictivas de violación de datos personales en la ciudad de Medellín desde la entrada en vigencia de la Ley 273 de 2009 hasta la fecha.

El método empleado al abordar esta investigación es cualitativo con un tipo de estudio descriptivo jurídico, en tanto se identifican las modificaciones introducidas en la Ley 1273 de 2009, sobre el tratamiento de los datos personales. El estudio también posee un enfoque histórico – hermenéutico, toda vez que posee un espacio temporal acotado desde la entrada en vigencia de la ley 273 de 2009 hasta la fecha, principalmente ahondando en analizar las

dificultades que se tienen al momento de judicializar a los sujetos activos que infringen los bienes jurídicos protegidos por el artículo 269F del Código Penal; Así mismo, esta investigación es de carácter espacial por estar delimitado en el municipio de Medellín, escogido por ser el lugar donde se desarrolla la presente investigación y por el incremento que ha tenido el delito en los últimos años. Las fuentes empleadas son de carácter primario, ya que se recolecta la información legislativa vigente en materia de tratamiento de los datos personales; además de tener en cuenta sentencias resueltas por la Corte Constitucional; además, para la recolección de la información se utilizan técnicas de visión documental y la entrevista a un experto en delitos relacionados con la violación de datos personales. La información se extrae de bases de datos como Google académico, Scielo, Redalyc y Dialnet; además de la Jurisprudencia Europea y Colombiana en termino de protección de datos.

Este articulo consta de dos capítulos. Después de exponer la introducción, se aborda el primer capítulo con el desarrollo del estado del arte y los antecedentes normativos; el segundo capítulo expone los resultados y análisis de los mismos y se finaliza con las conclusiones y referencias bibliográficas.

Capítulo 1. Análisis de la literatura

Algunos autores se han interesado en investigar sobre el delito de violación de datos personales para conocer sobre las normas sustanciales y procesales en virtud de las cuales el Estado es garante de la protección de la información y de los datos y la judicialización de aquellos delitos cibernéticos que atentan contra los derechos de las personas a salvaguardar la información. A continuación, se exponen algunos estudios relacionados con la Ley 1273 de 2009 (modificación del código penal sobre la protección de la información y de los datos), la Ley Estatutaria 1266 de 2008 (Congreso de la Repùblica, 2008) sobre el Habeas Data, la ley sobre la protección, la seguridad y la veracidad de los datos personales; la ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales, dentro otros temas relacionados con el estudio.

Un estudio realizado por Rivera (2019), sobre la realidad y sobre la Privacidad de los Datos Personales en Costa Rica, tuvo como finalidad abordar la jurisprudencia aplicada por la Sala Constitucional con el objetivo de que todas las personas conozcan la legislación existente sobre la información que se puede compartir y en el caso de ser expuestos como datos no autorizados tener claro el amparo de acuerdo con la ley 8968 relacionada con la protección de las personas frente al tratamiento de sus datos personales.

Los resultados permitieron conocer los pronunciamientos de la Sala Constitucional en referencia al tema de la privacidad de los datos personales extrayendo sentencias importantes para abarcar los conceptos de protección de datos como: Sentencia 5802-99 la cual afirma que "la recolección de los datos debe darse con base en el consentimiento del sujeto o con la autorización de la ley"; Sentencia 2018 – 01391 (acoso telefónico), Sentencia 2015-007357 (correos y documentos electrónicos), Sentencia 2015-005320 (violación al derecho de la intimidad); además de leyes como la Ley 8968 (consentimiento informado), La Ley 9048, de los delitos informáticos, entre otros (Rivera, 2019). Se pudo concluir que, a la población costarricense de acuerdo con la sala Constitucional, tienen derecho a la protección de sus datos personales, a tener el control de su información y decidir al respecto como bien lo consideren.

Otro aporte fue el realizado por Garzón et al (2020), sobre la protección de datos, una visión comparada desde la legislación española y colombiana. El objetivo principal fue realizar un recorrido cronológico relacionado con los avances en la protección de datos en `países como España y Colombia tomando como base la historia clínica electrónica, la cual contiene información constitucionalmente sensible sobre el estado de salud de los pacientes, por tanto, al haber un intercambio, el Estado debe asegurar que el método y transferencia cumpla con los estándares de protección de acuerdo a la legislación gubernamental vigente.

Los resultados permitieron evidenciar que tanto el Colombia como en España existe legislación vigente de protección de datos; no obstante, en términos de historias clínicas electrónicas, Españas se encuentra más evolucionada y cuenta con el control de la información que se maneja de los pacientes y vigila que se cumpla las leyes a cabalidad;

mientras que en Colombia aún no se encuentra implementada, toda vez, que de acuerdo con la ley 2015 de 2020 el Ministerio de Salud debe determinar los aspectos técnicos que deben cumplir las EPS para dicha implementación Historia Cínica Electrónica. Se tiene máximo cinco años a partir de la ley para que todo en el país optimice la herramienta sistemática que permita la interacción de datos.

Antecedentes normativos.

En la actualidad, uno de estos delitos informáticos de mayor promulgación es la violación de los datos personales, la cual es una infracción penalizada en Colombia. Con el articulo 269F del Código Penal, se promulgó la sanción o pena privativa de la libertad de "cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, a aquella persona que sin estar facultada obtenga, intercambie, compre, divulgue, modifique o emplee datos personales" (Diaz, 2013, p. 1); no obstante, con la entrada en vigencia de la Ley 1273 de 2009, denominada también "ley de delitos informáticos", se obtuvo un gran avance legislativo en materia de tratamiento de datos personales; esta ley modificó el Código Penal y creó el "bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones" (Alcaldía de Bogotá , 2009, 1).

Ante esto, Colombia promulgó la Ley 1273 de 2009, modificando así, al Código penal y creando el bien jurídico tutelado: de la información y de los daños, compuesto por importantes tipos penales, entre ellos el que se encuentra en el artículo 269F denominado violación de datos personales. Esta tipificación se crea para proteger derechos fundamentales que se encuentran en la constitución política como la intimidad, el buen nombre y la honra. Ahora bien, al ser derechos fundamentales se hace necesario analizar si la conducta punible se está judicializando en todos los casos, puesto que en los delitos cibernéticos se requiere del apoyo internacional para lograr rastrear a los ciberdelincuentes y lograr una fructífera judicialización.

De la misma manera en la Sentencia T-444/14, mediante la cual se presenta acción de tutela en contra de la Procuraduría General de la Nación por considerar que dicha entidad ha violado los derechos a la privacidad y a la protección de los datos personales al valerse de sus facultades constitucionales y legales para solicitar de 'forma arbitraria información' acerca de las demandantes sobre datos sensibles que no pueden considerarse públicos. Ante esta situación la Corte Constitucional resuelve revocar la sentencia y tutelar los derechos de las demandantes a la intimidad, al *Habeas Data*, a la no discriminación y al acceso a la justicia; a su vez hacer un llamado a la Procuraduría General de la Nación para que tome medidas adecuadas que permitan garantizar la confidencialidad y la seguridad de los nombres de la accionantes y se abstenga de imponer por vía general lecturas que los jueces y notarios debe cumplir a fin de evitar que se coarte el margen de autonomía que la constitución les atribuye (Rama Judicial, 2014)

Por otra parte, al hablar de delitos informático hace referencia a todas aquellas conductas típicas, antijurídicas y culpables realizadas en el espacio cibernético, conductas sancionadas por la Ley 273 de 2009 en los artículos 269I a 269J debido a la necesidad de regular el incremento considerable en los últimos años.

Uno de los delitos más comunes es el de la violación de datos personales, art 269F , "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" (Congreso de la República de Colombia, 2012).

No obstante, en el Convenio sobre la Ciberdelincuencia, se acordó trabajar por la prevención y judicialización de la cibercriminalidad. Delitos que están en constante crecimiento dado a los avances tecnológicos a nivel mundial, por lo cual, se pacta que los estados parten tendrán como uno de sus objetivos mejorar las capacidades de las investigaciones de los delitos y la

colaboración de todas las autoridades para la judicialización de las conductas punibles (Organización de los Estados Americanos, 2019)

De esta manera puede afirmarse que su importancia radica en la necesidad de judicializar conductas que antes de la entrada en vigencia de la Ley 273 de 2009 (Congreso de la República, 2009) no se penalizaban con la rigurosidad que se detalla con la modificación de la norma y la importancia de proteger datos de carácter privado con información detallada sobre el sexo, raza, religión, estado civil, entre otros.

En este orden de ideas, el derecho a la Intimidad, al buen nombre, a la dignidad humana y a la honra, en su categorización de derechos fundamentales de índole constitucional. Art 15 derecho a la intimidad y al buen nombre art 20 Informar y recibir información veraz e imparcial y la de fundar medios masivos de comunicación. Art 21 derecho a la honra (Sistema Único de Información Normativa, 1991).

Ahora bien, otro concepto relevante de mencionar es el Habeas data, el cual es definido como un derecho que tiene las todas las personas de conocer, actualizar y rectificar las informaciones que se halla recogida en bancos de datos. Este es un derecho constitucional en relación al tratamiento de los datos de información personal de acuerdo con el artículo 15 de la constitución Política Nacional y según artículo 20 de esta misma, la protección de la información relacionada actividades financieras, comerciales, de crédito, o proveniente de otros países (Pérez, 2016)

Según el mismo autor, todas las entidades tienen el deber de mantener la información actualizada para llevar a cabo los procedimientos en forma efectiva en el momento de la rectificación de la información; todas las personas tienen el derecho de conocer dicha información sobre ella en los registros, actualizar dichos datos registrados si se encuentran atrasados y corregirlos en caso de que a información se encuentre desacertada y eliminar aquella que la persona encuentre sensible aunque sea cierta.

El habeas data en Colombia se creó desde la constitución política de 1991 misma, la cual a través del tiempo se ha ido regulando en favor de la protección de los datos de las personas. Fue la ley 1266 de 2008 la cual mostró un avance significativo en términos de Habeas data, de la protección, la seguridad y la veracidad de los datos personales aportados en especial a entidades financieras y de telecomunicaciones, entre otras entidades comerciales y de servicios. En términos generales, el Habeas data supone una garantía sobre la gestión adecuada de la información personal (Pérez (2016)

Capitulo II. Resultados

La judicialización en el delito de violación de datos personales no se ha llevado a cabo en todos los casos denunciados.

La violación de datos personales se ha convertido en un flagelo que está afectando a la población en su seguridad y ha conllevado a perjuicio tanto físicos como inmateriales; y, estos van desde la usurpación de identidad, el daño reputacional a empresas o el deterioro económico o social para las personas en general.

Colombia antes esta situación ha sancionado la ley 1581 de 2012 por la cual se expide el Régimen General de Protección de Datos Personales, y se prohíbe la transferencia de información sin que se proporcione el nivel adecuado de protección; y, el Decreto 1377 de 2013 (presidencia, 2013), el cual reglamenta esta ley y dicta otras disposiciones para la protección de datos personales. Cabe señalar, que anterior a la citada Ley 1581 de 2012 y el Decreto 1377 de 2013, Colombia mediante la Constitución política de 1991 (artículo 15, inciso 2º) reglamentó en relación a los derechos fundamentales que:

> todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. 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. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (Corte Constitucional, 2017. p.1)

Así mismo, a partir de la Ley 1273 de 2009 se modificó el Código Penal y "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 de la información y las comunicaciones, entre otras disposiciones (Secretaría del Senado, 2009)

No obstante, la sanción por violación de los datos personales (Habeas data) en Colombia regulada por la ley 1581 de 2012 y el Decreto 1377 de 2013 no va más allá de sanciones con multas económicas y cierre temporal o definitivo de los establecimientos. Sin embargo, cuando se trata de delitos informáticos, dichas conductas son sancionadas por la Ley 273 de 2009 en los artículos 269I a 269J (Ministerio de Eduicaciòn , 2020)

Según Daccach (2020),

> La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes

De acuerdo con un estudio realizado por Escobar et al. (2018) sobre la eficacia de las normas penales colombiana para prevenir y sancionar los ciberdelitos, se pudo conocer sobre la judicialización de algunos casos de delitos informáticos cometidos en contra de la nación.

El primer caso hace referencia al señor "Andrés Fernando Sepúlveda Ardila conocido como "el hacker", señalado de pertenecer y liderar una oficina de interceptaciones ilegales en el país" (Escobar et al. 2018); señalado este de monitorear de forma ilegal el proceso de negociación de la Habana a través de correos y extracción de documentos por medio de técnicas de HACKIN, en una oficina ubicada en Bogotá. Se realizó audiencia y mediante sentencia condenatoria fue enviado a prisión por 10 años acusado "por los delitos de Espionaje, Concierto para delinquir agravado, Acceso abusivo a un sistema informático, Uso de software malicioso y Violación de datos personales agravado, en calidad de coautor material" (Escobar et al. 2018.p. 47).

El segundo caso se trata del señor Solano Moreno, conocido como el "Rey millas" por la realización de maniobras ilícitas que a través del ingreso de forma fraudulenta a las páginas web de las aerolíneas, con la finalidad de obtener tiquetes aéreos. Se le imputaron delitos de violación de datos personales (ART 269F) y hurto informático (ART 269I) y por encontrarse en condiciones de condena domiciliaria por los mismos delitos, se le imputó, además, el delito de Fuga de presos (Art. 448 C.P) en calidad de reincidente (Escobar et al. 2018.p. 47).

En relación con lo anterior, es importante resaltar que en colombia si se llevan a cabo a la judicialización en el delito de violación de datos personales, aunque no en todos los casos denunciados. En primer lugar, cuando se trata de violación de datos personales (Habeas datas) se llega a sanciones económicas y cierre de establecimientos; sin embargo, muchos de los casos no son judicializados porque falta fortalecimiento de la legislación en el país; además por la falta de pruebas contundentes que permitan llevar los casos hasta la judicialización.

De acuerdo con una entrevista con la finalidad de recabar información y analizar los obstáculos por los cuáles atraviesa la normatividad penal colombiana para judicializar las conductas punibles derivadas de la comisión del delito de violación de datos personales en la ciudad de Medellín, un experto en el tema manifestó de acuerdo con la pregunta:

La Ley 273 de 2009 modifica el código penal y crea un nuevo bien jurídico para la protección de la de la información y los datos; ¿usted considera que esta ha sido suficiente? ¿Por qué?

> Por lo menos es un buen acercamiento para sentar precedentes y así reducir a su mínima expresión la comisión de estos hechos punibles, pues el legislador puso dentro de esta norma las nuevas modalidades de delitos que estaban siendo utilizados para la época, sin embargo, hoy después de más de 12 años de vigencia, hay que apoyarse en la jurisprudencia para hacer un buen análisis de cada tipo penal y encausar cada conducta buscando una pena ejemplarizante, pues a medida que avanza el mundo, la tecnología es pionera y por ende salen a la luz mil y una nueva forma de

> cometer fraudes a través de la manipulación de los datos personales. Es importante que cada jurista que quiera o se vea en la necesidad de navegar en este espinoso mundo de la protección de la información y los datos, hilvane la ley penal citada en la pregunta con la Ley estatutaria 1581 de 2012, para que se vea inmiscuido en una visión holística de la situación que se le presente en particular.

¿Cuáles considera sean las razones por las cuáles no se penalizan todos los casos de delito de violación de datos personales en Colombia?

> Desconocimiento de las formas que tienen los delincuentes para cometer sus ilícitos y de esta forma poder asociarlos dentro del marco de la legislación penal planteada para tal fin. De otra parte, se debe buscar que cada hecho jurídicamente relevante en cause a todos los responsables que participen o faciliten la comisión de los mismos, pues a veces el ente acusador se queda corto al pedir la judicialización de un eslabón, permitiendo que este sea reemplazado fácilmente para que la cadena estructural que comete el delito se afiance y pueda seguir creciendo en la consecución de víctimas de este flagelo.

Y en relación con la pregunta sobre ¿Cuáles considera deberían ser las tácticas utilizadas para la persecución de estos delincuentes y lograr la judicialización de estos delitos?, respondió:

> Sin lugar a duda, la principal táctica que debe buscar el gobierno colombiano, en cabeza del ente acusador, Fiscalía General de la Nación, para combatir los delitos informáticos es que sus representantes se apoyen en expertos en el tema, quienes puedan ir más allá del resultado del delito, y así buscar desarticular todos los medios, tanto humanos como técnicos que son utilizados por el delincuente final, pues detrás de un delito cibernético siempre abran otros actores que se tornan imperceptibles, por esto sólo una persona experta, adiestrada y destacada podrá encontrar todos los elementos que se requieren para cometer el delito cibernético. Tratando de colocar en términos más coloquiales la respuesta, pensaría que un hacker debe ser atacado y desenmascarado por otro hacker u otro gurú en el tema que tenga las mismas o

mejores capacidades para descifrar y sacar a la luz pública desde lo técnico cada movimiento que realiza el malhechor. Otro aspecto importante a tener en cuenta es la vigilancia que cada interesado le haga a las redes de comunicación que son utilizadas y creando programas de prevención.

Razones por las cuáles no se penalizan todos los casos de delito de violación de datos personales

Con la ley 1273 de 2009, se crea un nuevo bien jurídico denominado "de la protección de la información y de los datos" y de acuerdo con los artículo 269 (A - J), tipifica los distintos delitos relacionados con el acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, violación de datos personales, la suplantación de sitios web para capturar datos personales, modificación del sistema de resolución de nombres de dominio, circunstancias de agravación punitiva y transferencia no consentida de activos (Policia Nacional, 2009).

El Artículo 269 en su literal A, denota el delito de acceso abusivo, el cual hacia parte del Código penal del 2000 bajo el bien jurídico tutelado de la intimidad y las reserva en las comunicaciones y a partir de la ley ley 1273 de 2009 se reforma parcialmente y se crea intitulado de los delitos contra la información y los datos trasponiendo el articulo 195 al 269. Sin embargo, algunos juristas lo interpretaron como derogación de la ley, y creado nuevamente bajo el nuevo bien jurídico protegido. También se aplica este tipo penal de acuerdo con la norma 1266 de 2008 o también llamada Ley de Habeas Data la cual hace referencia a la ley de datos personales (datos públicos, privados, semiprivado, usuario, datos económicos) (Riascos, 2012).

Cabe resaltar que aunque la Ley 1273 de 2009, crea la protección de la información y de los datos; algunos casos no se entran dentro de esta ley, por tanto, no son penalizados; considerando esta como una de las principales causas por las cuales no se penalizan todos los casos de delito de violación de datos personales, aunada esta a la falta de cultura que ha

tenido Colombia para el tratamiento de los datos personales, lo que se convierte en un largo proceso de concientización de los especialistas judiciales, los operadores que almacenan datos y a la población en general sobre como tratar dicho datos personales y como darles el tratamiento tanto personal como jurídico que corresponde (García, 2009).

por otra parte, el Código Penal parte de los distintos bienes jurídicos en cada uno de los delitos o faltas cometidas en contra de la vida, la integridad física, la libertad sexual y de la propiedad; recogiendo así las faltas por las cuales se puede vulnerar el bien jurídico que afecte la integridad personal, económica y /o la dignidad humana sin embargo, cumple un rol fundamental la interpretación del especialista judicial ya que puede excluir el tipo de conductas que considere que no lesionen el bien jurídico que se protege; por tanto, dentro del margen de arbitrio judicial que al ley concede, este puede concretar y determinar la pena que algunas veces no conlleva a ningún tipo de sanción o pena; es decir, esto lo determina el juzgador al momento de emitir o no la sentencia condenatoria (Grisales, 2014).

En concordancia, algunos de los casos de delitos de violación de datos personales no son penalizados, toda vez que el especialista judicial lo resuelve mediante la revisión de los casos interpuestos a través de tutelas en la Corte Constitucional. Un ejemplo de ello es la Sentencia T-490/18, por medio de la cual se interpone un derecho de petición ante particulares por concepto de derecho a la honra, buen nombre y habeas data; en donde la Corte Constitucional resuelve amparar el derecho fundamental de la petición señalada en dicha sentencia (Corte Constitucional, 2018).

Las estadísticas delictivas de violación de datos personales en la ciudad de Medellín desde la entrada en vigencia de la ley 273 de 2009 hasta la fecha.

En la actualidad existen casos concretos de la violación de los datos personales y uno de estos fue el vinculado al expresidente Juan Manual Santos en donde el Hacker Andrés Sepúlveda, delincuente informático logró interceptar las comunicaciones y correos electrónicos en donde este adelantaba los acuerdos entre el Gobierno nacional y los jefes de Las Fuerzas Armadas Revolucionarias de Colombia FARC en relación con los diálogos en

la Habana (Cuba). El Hacker fue acusado de espionaje, concierto para delinquir y acceso abusivo a un sistema informático; además de uso de software malicioso y violación de datos personales. Es importante resaltar que, por dicho caso, la Fiscalía llamo a interrogatorio a los implicados en el caso (Óscar Iván Zuluaga e hijo David) por nexos y pagos realizados para tal fin. En la actualidad el Hacker Andrés Sepúlveda está detenido desde el año 2015 pagando una pena privativa de la libertad de 120 meses y al pago de 120 salarios mínimos mensuales legales como multa (Sánchez, 2016).

Las llamadas millonarias ha sido otro tipo de caso de violación de datos personales, toda vez que mediante el teléfono realizan estafas poniendo en contacto al delincuente con la víctima. A través de este sistema, los delincuentes utilizan la ingeniería social que no es otra cosa que la manipulación psicológica con falsas premisas con la finalidad que la víctima divulgue información personal a través de la manipulación de la autonomía de la voluntad. Esta modalidad busca generar pánico en la victima para que esta realice todo lo que se le pide, sugestionándolo de que si no lo hace perderá algo o, por el contrario, que ganará un premio millonario. Aunado a esto se encuentran la utilización de medios tecnológicos, la instalación se software malicioso, el robo de datos esponsales; lo que se conoce como *phishing y hacking* (Sánchez, 2016).

Por otra parte, el caso llevado a cabo en el tribunal Superior de Medellin, en contra del señor Juan Diego Daza Ocampo, llamo altamente la atención dada la magnitud de delito.

> El señor Daza aceptó haber cometido los delitos enrostrados cuando fungía como Gestor de Operaciones en una de las filiales del banco de Occidente de la ciudad de Medellín, apoderándose de $383.672.678, luego de realizar un total de 232 transacciones de crédito por canales de consignación de caja rápida, durante un lapso de ocho años, del año 2006 al 2014 (Sala Penal tribuna de Medellin, 2014)

En consecuencia, el magistrado a cargo resuelve declarar penalmente responsable al señor daza como “como autor de la conducta punible en forma continuada de Hurto calificado agravado específica y genéricamente, previsto en los artículos 239, 240.4, 241.2, 267.1 y parágrafo del 31 del C. Penal” (Sala Penal tribuna de Medellin, 2014.p.21); y en consecuencia

se condena a 96 meses de prisión, inhabilidad en el ejercicio de derechos y funciones públicas por el término de la pena privativa de la libertad.

Otro de los casos, fue el hostigamiento realizado a través de las redes sociales a un menor de 12 años, afectando directamente su entorno social, familiar, la intimidad y la honra. Se presenta el ciberacoso, trascendiendo el espacio virtual y afectando la vida cotidiana de este menor y de toda su familia, perturbado la tranquilidad y normalidad de las vidas de estos.

En general y de acuerdo con cifras estadísticas en la última década se han impuesto multas por $6.793 millones y dentro de las actuaciones más relevantes se encuentra multa impuesta a la sociedad American System Service S.A.S. por $163 millones por el reporte de información de sus titulares si previa autorización de estos; de la misma forma, la Cooperativa Multiactiva Universitaria Nacional fue sancionada con multa por valor de $129 millones al no implementar medidas técnicas de seguridad permitiendo que terceros tuvieran acceso a la red sin ningún tipo de restricción a los datos crediticios de los titulares de las cuentas. Así mismo, la compañía Récord de Colombia S.A. fue sancionada por multa de $123 millones por el tratamiento datos personales de salud sin previa autorización y con fines comerciales para el ofrecimiento de su servicio. Por otra parte, fue impartida una "orden a la Corte Suprema de Justicia por un asunto de denominación de datos sensibles de un menor de edad contenidos en una sentencia publicada en la página web, al advertir que la información estaba desactualizada e inducía al error" (Prado, 2015).

Ahora bien, al indagar sobre otros datos estadísticos delictivos de violación de datos personales, se ha encontrado que en los últimos dos años la irrupción informática, los delitos de suplantación tanto de personas como de entidades y el hurto por medios electrónicos son unas de las acciones más ejecutadas por los ciberdelincuentes, aumentando las cifras con la llegada del a contingencia de Covid – 19. De acuerdo con el informe de la Dijín para el año 2020 en el segundo semestre fueron registrados 18.255 delitos realizados a través de canales informáticos, cifra esta, que fue duplicada en relación con el año 2019 en donde los casos llegaron a 9.300, aumentando en un 409% las modalidades de estafas y fraudes a través de

las redes y en donde los más afectados además de las personas, han sido los micro y macro empresarios (Acosta, 2021).

En este sentido, es importan resaltar que las penas por fraude en línea y las distintas redes informáticas van desde multas económicas hasta prisión de la libertad. A continuación, en la tabla 1, se describen los delitos ejecutados y sus respectivas penas.

Tabla 1. Penas por fraude en línea

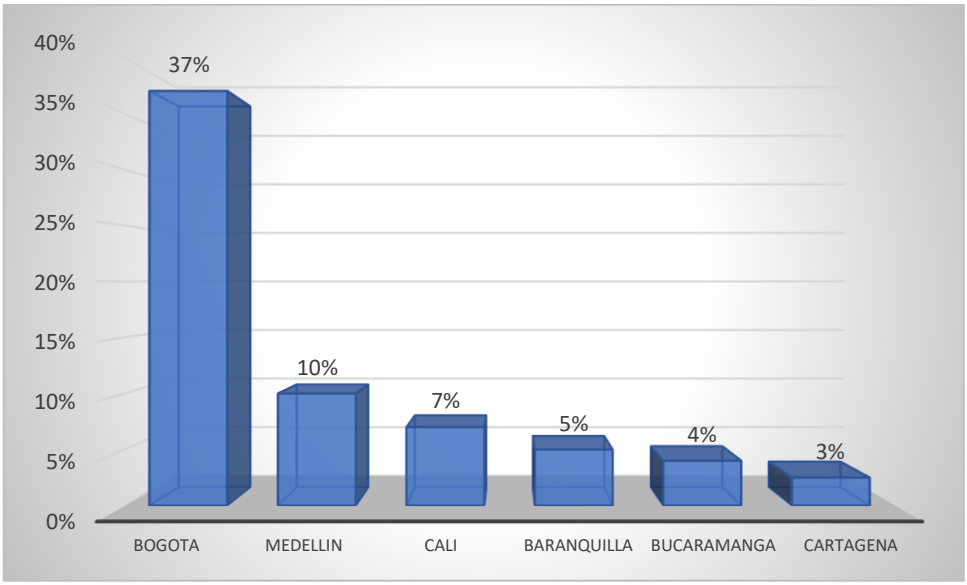
Delito	**Código Penal artículo 269 – 246**		
Suplantación de identidad a través de correos electrónicos para obtener información	Acceso abusivo a sistema informático $: 100 a 1000 (smlmv) Prisión: 48 – 96 meses	Daño informático $: 100 a 1000 (smlmv) Prisión: 48 – 96 meses	Violación datos personales $: 100 a 1000 (smlmv) Prisión: 48 – 96 meses
Paginas falsas de empresas que buscan captar información de ID y contraseña de los usuarios	Acceso abusivo a sistema informático $: 100 a 1000 (smlmv) Prisión: 48 – 96 meses	Daño informático $: 100 a 1000 (smlmv) Prisión: 48 – 96 meses	Violación datos personales $: 100 a 1000 (smlmv) Prisión: 48 – 96 meses
Fraude por redes sociales a través de prestamos ilegales o por fuera de entidades financieras	Suplantación de sitios web para capturar datos personales $: 110 a 1000 (smlmv) Prisión: 48 – 96 meses	Transferencia no concedida de activos $: 200 a 1500 (smlmv) Prisión: 48 – 120 meses	Estafa $: 66.66 a 1500 (smlmv) Prisión: 36 – 144 meses
Robo de cedulas para solicitar préstamos en entidades bancarias			
Landing page flake Por medio de las cuales se recolectan datos haciéndose pasar por empresas conocidas, los usuarios piden un prestamos y deben pagar derechos de desembolso, lo cual es una estafa			$: 110 a 1000 (smlmv) Prisión: 48 – 96 meses

Fuente: adaptado de Acosta (2021).

Por otra parte, en relación a la suplantación de identidad se obtiene que en el año 2020 se alcanzó un total de 1.527 casos en relación con el año 2019 que se evidenciaron 333, representando como se mencionó en párrafos anteriores un porcentaje del 409%; siendo el correo electrónico una de las modalidades más utilizadas; por otro lado, la suplantación en sitios web tuvo 4.776 casos en 2020 frente a 892 en el año 2019 con una variación de 435%. Es importante resaltar que las ciudades con mayores actos delictivos de cibercrimen han sido: Bogotá con 12.981 casos representados por el 37%, Medellín con 3.442 casos con un 10%, Bucaramanga con 1.256 casos correspondiente al 4%, Cali 2.363 casos con el 7%,

Barranquilla con 1.809 casos con el 5% y Cartagena con 887 casos representados por el 2.50%, ver grafica 2.

Gráfica 1. Ciudades con mayores casos



Fuente elaboración propia con datos de Acosta (2021).

Como se puede observar en la gráfica 1. Las ciudades con mayores numeros de casos en ciberdelitos y violación de datos personales son Bogotá con el 37%, seguido de Medellin con el 10% y Cali con el 7%; las otras ciudades tienen algunos casos con menor porcentaje de participación.

Conclusiones

La violación de datos es un delito que es penalizado en Colombia, siendo este uno de los pocos países que lo realiza y para ello se crea la ley de delitos informativos Ley 1273 de 2009 que modifica el Código Penal Colombiano y crea un bien jurídico tutelado como la protección de la información y los datos; además, se preservan los sistemas de tecnología y las comunicaciones.

Al indagar sobre si la judicialización en el delito de violación de datos personales se lleva a cabo en todos los casos denunciados, se ha encontrado que no siempre se judicializan estos delitos, en primer lugar, porque muchos de estos son resueltos a partir de acciones de tutelas en la Corte Constitucional que obliga el restablecimiento de los derechos en materia de protección de datos esponsales de acuerdo con la ley Ley 1273 de 2009; en segundo lugar por el desconocimiento de las formas que tienen los delincuentes para cometer sus ilícitos y de esta forma poder asociarlos dentro del marco de la legislación penal planteada para tal fin y en tercer lugar por la subjetividad como los juristas interpretan la ley y los casos delictivos.

Al analizar las estadísticas delictivas en colombia y en la ciudad de Medellin, que este tipo de delitos de violación de datos personales son hechos que se han venido realizando constantemente por los delincuentes y más aun con la facilidad que ofrece la tecnología para los ciberdelitos. Durante el periodo 2019 – 2020 este tipo de delitos se han duplicado y las principales ciudades son Bogotá, Medellin y Cali.

Con la Ley 1273 de 2009, se crea un nuevo bien jurídico denominado "de la protección de la información y de los datos" y en sus artículos 269 (A - J), tipifica los distintos delitos relacionados con el acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, violación de datos personales, la suplantación de sitios web para capturar datos personales, entre otros.

Para dar respuesta al objetivo general sobre el análisis de los obstáculos por los cuáles atraviesa la normatividad penal colombiana para judicializar las conductas punibles derivadas de la comisión del delito de violación de datos personales en la ciudad de Medellín, se concluye que uno de los principales obstáculos por los que atraviesa la normatividad penal colombiana para la judicialización del delito de violación de datos personales en la ciudad de Medellín**,** es la dificultad para buscar que cada hecho jurídicamente relevante en cause a todos los responsables que participen o faciliten la comisión de los mismos, pues a veces el ente acusador se queda corto al pedir la judicialización de un eslabón, permitiendo que este

sea reemplazado fácilmente para que la cadena estructural que comete el delito se afiance y pueda seguir creciendo en la consecución de víctimas de este flagelo.

Referencias

Alcaldía de Bogotá . (2009). Ley 273 de 2009. *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado*, https://www.habitatbogota.gov.co/transparencia/normatividad/normatividad/ley-1273-2009.

Acosta Argote, C. (2021). ¿Qué castigos estipula el Código Penal para los delitos informáticos como la estafa? Recuperado de https://www.asuntoslegales.com.co/actualidad/que-castigos-estipula-el-codigo-penal-para-los-delitos-informaticos-como-la-estafa-3180022

Bonilla Rodríguez, E. (2000). *Más allá de los dilemas de los métodos. La investigación en las ciencias sociales.* Recuperado de https://es.scribd.com/doc/106220258/ELSSY-BONILLA-Mas-Alla-Del-Dilema-de-Los-Metodos-Introduccion-y-Cap-1

Corte Constitucional (Sentencia T-695 de 2017). Recuperado de: https://www.alcaldiabogota.gov.co/sisjur/listados/tematica2.jsp?subtema=25266&cadena=

Corte Constitucional,. (Sentencia T-020/2014). Habeas data como derecho autónomo y como garantía de otros derechos fundamentales. Recuperado de: https://www.corteconstitucional.gov.co/relatoria/2014/T-020-14.htm.

Corte Constitucional (Sentencia T-490/18). Principios y garantías constitucionales. Recuperado de: https://www.corteconstitucional.gov.co/relatoria/2018/t-490-18.htm

Dacccht, T15. J.C. (2020). Ley de Delitos Informáticos en Colombia. Recuperado de: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Diaz, G. A. (2013). El delito de la violación de datos en Colombia. *Observatorio Iberoamericano de protección de datos*, http://oiprodat.com/2013/04/25/el-delito-de-violacion-de-datos-personales-en-colombia/.

Escobar roa, D.A y Jiménez Moreno, L.D (2018). Eficacia de las normas penales colombiana para prevenir y sancionar los ciberdelitos. Repositorio Institucional. https://repositorio.unibague.edu.co/bitstream/20.500.12313/1925/1/Trabajo%20de%20grado.pdf

Fiscalía General del Nación. (2021). Violación de datos personales. https://www.fiscalia.gov.co/colombia/tag/violacion-de-datos-personales/.

Garzón Forero, H.S., Arias Moreno, M., y Castro Herrera, B. N (2020). Protección de datos una visión comparada desde la legislación española y colombiana. https://alejandria.poligran.edu.co/handle/10823/2134

García Rambla J.L (2009). Legalidad informática. Tratamiento y delitos de violación de datos personales en Colombia (I de III). Recuperado de http://legalidadinformatica.blogspot.com/2009/12/tratamiento-y-delitos-de-violacion-de.html

Grisales Pérez, G. (2014). Hurto por medios informáticos y transferencia no consentida de activos en Colombia. Revista Derecho Penal N°:48, 121-189. https://xperta.legis.co/visor/rpenal/rpenal_0501bdaa7778007ee0530a010151007e/revista-de-derecho-penal-contemporaneo/hurto-por-medios-informaticos-y-transferencia-no-consentida-de-activos-en-colombia

Hernández, SR., Méndez., MA., y Cuevas, C. y. (2017). *Fundamentos de investigación.* México: McGraw-Hill. Un proceso transformación digital percibidos por un grupo de altos directivos de una empresa de servicios de tecnologías de la información. Bogotá, Colombia.

Hernández Sampieri, R., Fernández Collado, C. y Baptista Lucio, P. (2014), Metodología de la investigación. Enfoque cualitativo y cuantitativo. 6a ed. Editorial McGraw Hill. México D.F. pp 634

Ministerio de Educación, (2020). Protección de Datos Personales. https://www.mineducacion.gov.co/1759/w3-article-387771.html?_noredirect=1#:~:text=A%20trav%C3%A9s%20de%20la%20Ley,las%20entidades%20del%20p%C3%BAblicas%20y

Organización de los Estados Americanos. (2019). Convenio de Budapest. R. *Convenio Budapest*, https://www.oas.org/juridico/english/cyb_pry_convenio.pdfconvenio de Budapest.

Pérez Fernández OE. (2016), habeas data en Colombia: su desarrollo y conexidad con los derechos fundamentales. https://repository.ucatolica.edu.co/bitstream/10983/14745/1/HABEAS%20DATA%20CON%20%20LICENCIA.pdf

Rama Judicial. (2014). Sentencia T-444/14. *Derecho a la privacidad/derecho a la protección de datos personales/derecho a la no discriminación.*, https://www.ramajudicial.gov.co/documents/2302615/0/SENTENCIA+T-444-14+M.P+MAR%C3%8DA+VICTORIA+CALLE.pdf/cf87c449-2913-.

Ramírez Prado, J. (2015). La violación de Habeas Data dejó multas por $1.892 millones durante el año pasado. Recuperado de: https://www.asuntoslegales.com.co/actualidad/la-violacion-de-habeas-data-dejo-multas-por-1892-millones-durante-el-ano-pasado-2228696

Rivera Barrantes, V. (2019). Realidad sobre la Privacidad de los Datos Personales en Costa Rica. e-Ciencias de la Información, 9(2), 1- 13. https://www.scielo.sa.cr/pdf/eci/v9n2/1659-4142-eci-9-02-68.pdf

Riascos Gómez, L.O (2012). Los delitos contra los datos personales y el habeas data en la Ley 1273 de 2009. Derecho y Realidad Núm. 20, 336 - 429

Sala Poenal tribuna Medellin (2014). Sentencia de Segunda Instancia Nro. 011. Delitos: Hurto calificado agravado y otros. Recuperado de: https://salapenaltribunalmedellin.com/images/pdf/providenciaspenal/008/05001600020620142638.pdf

Secretarìa del Senado (Ley 1273 de 2009). Por 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 de la información y las comunicaciones, entre otras disposiciones. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Silva, A. D. (2008). La imputación objetiva del nexo lógico en el tipo penal de violación de datos personales.

https://repository.unab.edu.co/bitstream/handle/20.500.12749/11897/200812_Revista_Estrado_Vol_7_no-12_29-37.pdf?sequence=1&isAllowed=y

Sistema Único de Información Normativa, (1991). Recuperado de: https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Constitucion/1687988nstitución Política 1991.