Estudio del marco normativo de protección de datos personales con objeto de prevenir la materialización de delitos informáticos que vulneran la dignidad humana. Análisis comparado entre Colombia y España

Trabajo final de grado para optar al título de abogadas

Aura María Pozo Chávez, Ingrid Tatiana Pallares Arévalo

Director

Rafael Eduardo Carrillo Marquez

Maestría en Derecho

División de Ciencias Jurídicas y Políticas

Facultad de Derecho

Universidad Santo Tomás, Bucaramanga

2022

Dedicatoria

Dedicamos el resultado de este trabajo principlamente a Dios, por darnos la fuerza necesaria para culminar esta meta.

A nuestras familias; nuestros padres que siempre nos brindaron apoyo incondicional, nuestras hermanas que siempre nos brindaron palabras de ánimo, y nuestros abuelos por enseñarnos a afrontar las dificultades. Nos han enseñado a ser personas con valores, constancia, firmeza y perseverancia, y por esto, mil gracias.

Contenido

Lista de Tablas

Lista de Figuras

Resumen

El objetivo general de esta investigación es analizar, mediante un estudio comparado entre Colombia y España, el marco normativo de protección de datos personales como medio para prevenir la materialización de delitos informáticos que vulneran la dignidad humana. Este estudio se efectuó bajo un enfoque cualitativo, pues persigue la cualificación de un fenómeno. La investigación es documental, debido a que la principal fuente de información es secundaria, pues se apoya en documentos que han sido generados por terceras personas como lo son libros, artículos científicos, trabajos de grado, reportajes periodísticos, instrumentos legales, sentencias y jurisprudencia. El nivel es descriptivo, pues busca caracterizar los principales elementos involucrados en los delitos informáticos que vulneran la dignidad humana de los colombianos. Los resultados de la investigación arrojaron que aun cuando Colombia ha hecho progresos importantes en cuanto a la tipificación de los delitos informáticos y la emisión de nuevos instrumentos jurídicos orientados a proteger los datos de índole personales y, por consiguiente, la dignidad humana, sus esfuerzos no han sido suficientes para frenar el impacto de los delitos informáticos. Finalmente, se concluye que si se incorporan algunos elementos del marco legal español a la legislación colombiana es posible mejorar el sistema legal de protección de datos y, a su vez, propiciar la disminución de los delitos informáticos contra la dignidad humana.

Palabras clave: Delitos informáticos, protección de datos personales, análisis de derecho comparado, Colombia y España.

Abstract

The main purpose of this research is to analyze, through a comparative study between Colombia and Spain, the regulatory framework for the protection of personal data as a means to prevent the materialization of cybercrimes that violate human dignity. This study was carried out under a qualitative approach, since it pursues the qualification of a phenomenon. This is a documentary research, because the main source of information is secondary, since it is based on documents that have been generated by third parties such as books, scientific articles, degree projects, journalistic reports, legal instruments, sentences and jurisprudence. The level is descriptive, since it seeks to characterize the main elements involved in cybercrimes that violate the human dignity of Colombians. The results of the investigation showed that even though Colombia has made important progress in terms of the classification of cybercrimes and the issuance of new legal instruments aimed at protecting personal data and, consequently, human dignity, its efforts have not been enough to curb the impact of cybercrime. Finally, it is concluded that if some elements of the Spanish legal framework are incorporated into Colombian legislation, it is possible to improve the legal system of data protection and, as a consequence, promote the reduction of cybercrimes against human dignity.

Keywords: Cybercrimes, personal data protection, comparative law analysis, Colombia and Spain.

Introducción

El acelerado desarrollo de las tecnologías de la información y la comunicación (TIC) ha propiciado el uso masivo del internet, lo cual ha beneficiado significativamente a la humanidad, pues ha facilitado la ejecución de una gran cantidad de actividades que antes tomaban más tiempo y no eran tan eficaces como lo son en la actualidad. Sin embargo, el uso casi irrestricto de las TIC ha dado lugar a otro tipo de actividades: las delictivas conocidas como lo son los delitos informáticos.

Colombia, ha realizado importantes avances en la tipificación de los delitos informáticos, así como en la emisión de normas jurídicas orientadas a proteger los datos de índole personal. La vulneración de los derechos fundamentales por medio de las TIC, sobre todo aquellos asociados a la dignidad humana, se ha convertido en una situación alarmante que ha sido difícil de enfrentar, ya que, actualmente, hay quienes consideran que la información de carácter personal es el petróleo moderno, lo cual no está muy lejos de la realidad, pues muchas personas han tenido que pagar grandes sumas de dinero para recuperar sus datos personales o en el caso de los responsables del tratamiento de la información, los bancos de datos.

Teniendo en cuenta esta conflictividad, se planteó la pregunta problema de investigación que este trabajo documental resuelve, a saber: ¿De qué manera puede contribuir la adecuación del marco normativo de protección de datos personales en la prevención de la materialización de delitos informáticos que vulneran la dignidad humana?

El objetivo general de esta investigación es analizar, mediante un estudio comparado entre Colombia y España, el marco normativo de protección de datos personales como medio

para prevenir la materialización de delitos informáticos que vulneran la dignidad humana. Para dar respuesta al objetivo general se plantearon tres objetivos específicos, a saber:

- Describir los delitos informáticos que repercuten de forma directa, en la vulneración de la dignidad humana en Colombia.

- Identificar el marco normativo de protección de datos personales en la legislación colombiana, debilidades y fortalezas.

- Estudiar el sistema legal español de protección de datos personales en el marco de la Comunidad Europea con el fin de describir los elementos potencialmente incorporables a la legislación colombiana.

Este estudio se efectúa bajo un enfoque cualitativo, pues persigue la cualificación de un fenómeno. La investigación es documental, debido a que la principal fuente de información es secundaria, pues se apoya en documentos que han sido generados por terceras personas como lo son libros, artículos científicos, trabajos de grado, reportajes periodísticos, instrumentos legales, sentencias y jurisprudencia. El nivel es descriptivo, pues busca caracterizar los principales elementos involucrados en los delitos informáticos que vulneran la dignidad humana de los colombianos.

Entre las principales conclusiones que arroja esta investigación es que si se incorporan algunos elementos del marco legal español a la legislación colombiana es posible mejorar el sistema legal de protección de datos y, a su vez, propiciar la disminución de los delitos informáticos contra la dignidad humana.

1. Generalidades de la Investigación

1.1 Descripción del problema

El desarrollo del ser humano en sociedad ha propiciado un creciente uso y consumo de las herramientas tecnológicas; que, a su vez, ha promovido el veloz desarrollo de la ciencia, la información y la tecnología misma. Esto ha cambiado los hábitos de las personas, pues la generalidad de las interacciones cotidianas, son efectuadas a través de medios electrónicos. En consecuencia, la ejecución de actividades cotidianas se realiza de manera más fácil, rápida, eficiente y eficaz.

En este sentido, Polo-Roca (2020) considera que los avances de las nuevas tecnologías son la base de la sociedad actual, especialmente, en lo relacionado al manejo de la información y la comunicación, lo cual ha dado origen a un nuevo fenómeno que el autor, denomina *big data,* para referirse a la recolección y almacenamiento de los millones de datos personales que se encuentran disponibles en la red. “Ya se calculó que para el 2018 habría más de 3.330 millones de dispositivos conectados en las ciudades inteligentes compartiendo millones y millones de datos entre ellos cada segundo” (Polo-Roca, 2020, p. 51).

Lo expuesto significa, que la *big data* se ha convertido en un recurso indispensable para la vida moderna, donde todos y cada uno de los miembros de la sociedad, son productores y consumidores de información de forma simultánea; todo ello, permea a todos los ámbitos del ser humano y ha conllevado al advenimiento de la sociedad de la información, la cual, como es de suponer, se ha cimentado mediate la captación, procesamiento, almacenamiento y difusión de la información (datos).

Por otra parte, el avance y democratización del uso de la tecnología, ha favorecido la globalización, pues en cuestión de segundos las personas pueden movilizar fondos

monetarios, adquirir bienes y/o servicios y acceder a multiplicidad de datos e información de todo tipo, permitiendo el establecimiento de relaciones e intercambios a nivel global. Sin embargo, esta situación viene acompañada de una serie de desventajas, ya que el fácil acceso que se puede tener a la información personal, ha fomentado la transgresión de ciertos bienes jurídicos, a través del uso y abuso de esta clase de instrumentos (Cano et al., 2014).

En este sentido, se puede afirmar que el acceso casi irrestricto a la información que ofrecen las nuevas tecnologías, les confiere una alta vulnerabilidad a los usuarios de internet y a quienes hacen uso de servicios digitales o presenciales con registros o archivos digitales, pues en cualquier momento, personas con fines deshonestos, delictivos o simplemente, maliciosos, pueden irrumpir y hacer uso indebido de la información, dando lugar al surgimiento de un nuevo tipo de ilícitos.

Estas conductas al margen de la ley, son conocidos por diversos nombres, tales como: delitos informáticos, delitos cibernéticos, delitos telemáticos, crímenes virtuales, cibercrímenes, entre otros. Este tipo de ilícitos se definen como actuaciones ilegales perpetradas por medio de la utilización inapropiada de la tecnología, con el propósito de arremeter contra la privacidad y/o bienes de otras personas, perjudicando o sustrayendo toda clase de información que está almacenada en servidores, nubes de datos o *gadgets* (Acosta, Benavides, & García, 2020).

Lo expuesto, genera un conflicto a nivel personal, social, económico, pero sobre todo jurídico, puesto que el uso del Internet ha facilitado que cada vez sea mayor la frecuencia y el impacto con el que los dispositivos tecnológicos de almacenamiento y procesamiento de datos, sean vulnerados en sus componentes más sensibles. Lo que ocasiona que se exponga gran cantidad de información de diferentes niveles de valor personal, administrativo, financiero, crediticio, económico y trascendental, lo cual coloca en un estado de indefensión

el patrimonio de las personas naturales y jurídicas, así como la dignidad, la honra y la integridad física, moral, emocional y mental de los seres humanos (Bechara et al., 2020).

Los delitos informáticos más difundidos son aquellos que afectan los bienes tangibles (financieros) por el impacto que este tipo de ilícitos tiene en la estabilidad empresarial y en la economía en su conjunto. No obstante, hay un tipo de transgresiones, que cada vez ocurren con mayor frecuencia, pero que reciben menor atención, aun cuando son graves, se hace referencia en este punto, a aquellos que se comenten contra la dignidad humana. Entendida esta última como: "el elemento axiológico por excelencia del ordenamiento jurídico" por lo que "el derecho se erige …como instrumento rigurosamente orientado, …a la consecución de la justicia y al respeto de la dignidad de la persona" (Jimena, 2020, p. 364)

En vista de lo expuesto, en el año 2009, el Congreso de Colombia modificó el Código Penal, al crear un nuevo bien jurídico tutelado denominado "protección de la información y de los datos"; asimismo, preservó integralmente los sistemas que utilizan las Tecnologías de la Información y las Comunicaciones (TIC), a través de la Ley 1273 de 2009. Es decir, que el legislador incorporó, en el ordenamiento jurídico, elementos relacionados a las nuevas TIC, así como, con las nuevas figuras delictivas, con la intención de responder eficazmente a la criminalidad informática. Asimismo, mediante la Ley Estatutaria 1581 de 2012 reglamentada por los Decretos 1377 de 2013 y 1081 de 2015 se pretendió regular de forma integral la protección y tratamiento de datos personales.

Lo anterior, permite reflexionar sobre la importancia que tiene el desarrollo legislativo con respecto a este tema, pues es necesario que existan mecanismos jurídicos y punitivos que garanticen la protección de la información personal de los colombianos que, por diversas razones, está en manos de terceros, pues su vulneración facilita la comisión de faltas a la dignidad de quienes son víctimas de la violación a la privacidad. Es menester

entender, que los delitos informáticos no solo afectan a los bienes de los particulares, sino que atacan directamente la dignidad de las personas, con lo cual se sacuden las bases mismas de la democracia y el estado de derecho, por lo que resulta fundamental, garantizar, primeramente, la protección y respeto por la dignidad humana.

Sin embargo, el rápido y vertiginoso avance de las nuevas tecnologías, implica reforzar las normas de protección de datos personales, pues la legislación es más reactiva que proactiva, en el sentido que no se adapta conforme como se modifican las herramientas tecnológicas para ser medio para la comisión de los delitos. En la actualidad, el sistema legal de protección de datos personales, no es eficiente al proteger de manera integral la dignidad humana de quienes son víctimas de delitos informáticos.

En este sentido, conviene realizar el estudio del marco normativo de protección de datos personales con objeto de prevenir la materialización de delitos informáticos que vulneran la dignidad humana mediante un análisis comparativo entre la legislación colombiana y española, habida cuenta que, el referido país dispone de un marco jurídico bastante más robusto que el colombiano, en cuanto a la materia.

1.2 Formulación de pregunta de investigación

En virtud de lo señalado, ¿De qué manera puede contribuir la adecuación del marco normativo de protección de datos personales en la prevención de la materialización de delitos informáticos que vulneran la dignidad humana?

1.3 Justificación

Los delitos informáticos han evolucionado a la misma velocidad que lo ha hecho la tecnología, variando en su modalidad, frecuencia e impacto; razón por la cual, las disposiciones jurídicas relacionadas a este tipo de acciones deben ser actualizadas de manera constante, para que sea posible una regulación idónea. No obstante, la dinámica del proceso legislativo, hace imposible que la velocidad de adecuación legislativa se equipare a la velocidad de los cambios tecnológicos, por ello, las leyes que regulan la materia, deben adelantarse a los posibles cursos de acción de la tecnología, por lo que el fortalecimiento de sistemas de protección de datos personales puede ser un medio efectivo para prevenir los delitos informáticos contra la dignidad humana (Bolañoz & Narváez, 2014).

En la actualidad, los delitos informáticos han aumentado de forma considerable, tal como señala Acosta-Argote (2021), para el primer trimestre de 2020 este tipo de delitos había crecido en un 37 % con respecto al mismo periodo de 2019. Cabe mencionar, que, dentro de los delitos informáticos reportados durante el periodo referido, aquellos relacionados con la vulneración de los datos personales y, consecuentemente, con la dignidad humana, representan aproximadamente el 78 %. Para el cierre de 2020, se habían denunciado 6.159 violaciones a los datos personales.

Sobre este particular, Acosta (2021) señala que para 2021, los delitos informáticos crecieron en Colombia en un 17 % con respecto al 2020. Esto significa que, la vulneración de la dignidad humana sigue siendo flagrante, sin que el marco legal vigente en materia de protección de datos personales pueda garantizar el resguardo de la información, ergo la salvaguarda de la dignidad humana de quienes son objeto de algún tipo de violación de seguridad.

Ahora bien, considerando las posibilidades que ofrecen las TIC, así como el surgimiento de nuevos escenarios para la perpetración de crímenes (el ciberespacio), el entorno es propicio para la vulneración de los derechos de terceros, de forma rápida, segura y anónima para los delincuentes. Entonces la protección se constituye en la mejor forma de regular esta clase de ilícitos que cada vez evoluciona y perjudica a mayor cantidad de usuarios. Es decir, que, a través del reforzamiento del marco normativo de protección de los datos personales, se puede evitar la comisión de los delitos, mientras que mediante el fortalecimiento de los tipos penales se ataca la conducta delictiva, pero no se resguarda a las víctimas, cuyas dignidades ya habrían sido vulneradas.

La Ley 1273 de 2009, mediante la cual se enmienda el Código Penal de Colombia y se incorporan artículos para sancionar los cibercrímenes, es considerada como un progreso que posibilita hacer frente a las amenazas relacionadas a la seguridad informática. Con relación a esto, Serrano (2014) expone que:

> Durante sus ponencias Kevin Mitnick, experto en seguridad informática quien participó en el evento tecnológico Campus Party celebrado en Bogotá desde hace algunos años. Considera la normatividad positiva, debe evolucionar y adaptarse al compás de la tecnología, día a día las tendencias y sistemas cambian, mejoran y evolucionan, entonces las leyes se van quedando obsoletas. (p. 11)

Sin embargo, tal como se ha señalado, la mejor forma de evitar la materialización de delitos informáticos que vulneren la dignidad humana es mediante el fortalecimiento del marco normativo de protección de datos personales. Pues, aunque en Colombia existen normas como la Ley Estatutaria de Protección de Datos Personales y, como se ha mencionado se han incorporado los delitos informáticos al código penal, la ocurrencia de estos ilícitos no ha dejado de aumentar, por lo que se propone realizar un estudio comparativo de la

legislación colombiana y la española, con miras a prevenir la materialización de delitos informáticos que vulneran la dignidad humana, a través de la adecuación del marco normativo de protección de datos personales .

Es de hacer nota que, la legislación española se ha nutrido de las regulaciones de la Comunidad Europea, la cual ha sido particularmente innovadora y exigente en materia de protección de datos, pero, además, los españoles han generado su propia normatividad interna orientada hacia el fortalecimiento de la protección de datos personales.

Hoy en día, es bastante común observar en los distintos medios de comunicación, noticias que expresan cómo se arremete contra la intimidad de las personas, el acceso desmesurado a las redes sociales, perjuicios a información digitalizada, difusión ilícita de contenidos, pornografía infantil, comercialización ilegal de datos confidenciales, vulneración de la seguridad de cuentas bancarias, entre otros delitos informáticos que colocan en un estado de indefensión a personas naturales y jurídicas.

1.4 Objetivos

1.4.1 Objetivo General

Analizar, mediante un estudio comparado entre Colombia y España, el marco normativo de protección de datos personales como medio para prevenir la materialización de delitos informáticos que vulneran la dignidad humana.

1.4.2 Objetivos Específicos

- Describir los delitos informáticos que repercuten de forma directa, en la vulneración de la dignidad humana en Colombia.

- Identificar el marco normativo de protección de datos personales en la legislación colombiana, debilidades y fortalezas.

- Estudiar el sistema legal español de protección de datos personales en el marco de la Comunidad Europea con el fin de describir los elementos potencialmente incorporables a la legislación colombiana.

2. Diseño metodológico

2.1 Enfoque y tipo de investigación

Este estudio se efectúa bajo un enfoque cualitativo, pues persigue la cualificación de un fenómeno. Las investigaciones cualitativas, fundamentalmente, se sostienen en la fenomenología y parten de una realidad que hay que crear, documentar y comprender, visto que las manifestaciones sociales cambian en función a las impresiones de sus intérpretes (Hernández, Fernandez, & Baptista, 2006).

La investigación es documental, debido a que la principal fuente de información es secundaria, pues se apoya en documentos que han sido generados por terceras personas como lo son libros, artículos científicos, trabajos de grado, reportajes periodísticos, instrumentos legales, sentencias y jurisprudencia. El nivel es descriptivo, pues busca caracterizar los principales elementos involucrados en los delitos informáticos que vulneran la dignidad humana de los colombianos.

2.2 Fuentes de información

Como se indicó, anteriormente, la principal fuente de información es secundaria, pues se apoya en documentos que han sido generados por terceras personas como lo son libros,

artículos científicos y de investigación, trabajos de grado, reportajes periodísticos, instrumentos legales, sentencias y jurisprudencia.

2.3 Procedimientos

En este apartado, se esboza el procedimiento que se va a llevar a cabo para dar respuesta a los objetivos de esta investigación. Para ello, se han identificado dos fases de investigación, a saber:

2.3.1 Fase I: Componentes preparatorios

Esta es la fase del estudio, se identifica el fenómeno de estudio y se efectúa el planteamiento del problema, en función a la revisión bibliográfica documental, que orienta a la propuesta de los objetivos de investigación, así como la justificación de la misma. Sucesivamente, abarca los siguientes pasos:

- Determinar el fenómeno de estudio,
- Recopilar información y datos bibliográficos sobre el fenómeno,
- Presentar el anteproyecto de investigación (redacción del planteamiento del problema, objetivos, justificación, marco teórico y metodológico).

2.3.2 Fase II: Resultados y Conclusiones

Una vez que se ha concluido la primera fase, se procede a culminar el procedimiento de estudio, siguiendo los pasos que se describen a continuación:

- Cruzar la información obtenida de la revisión documental con los modelos teóricos revisados y compararlo con los resultados obtenidos por otros investigadores (Discusión).

- Se establecen conclusiones en función a los resultados alcanzados.
- Se elabora y presenta el informe de investigación conforme a los criterios establecidos por la Universidad.

3. Resultados y Discusión

3.1 La dignidad humana como base de la constitucionalidad colombiana

En este capítulo se efectúa un breve resumen del origen y evolución histórica de la dignidad humana, así como de la transformación del concepto con el transcurrir del tiempo y el devenir de la humanidad. De igual forma, se exponen las implicaciones que conlleva la transgresión a la dignidad humana. Adicionalmente, se abordan los delitos informáticos como fuente de vulneración a la dignidad humana; asimismo, se presentan las características de las víctimas y victimarios de la dignidad humana a través de los delitos informáticos en Colombia.

El propósito de esta sección es exponer las ideas principales asociadas al tema propuesto, a los efectos de establecer un contexto histórico y conceptual con respecto a la dignidad humana desde la perspectiva del derecho, enfatizando, en aquellos aspectos que pueden contribuir a su violación, en el marco del uso de las nuevas tecnologías, como lo son los delitos informáticos.

3.1.1 Origen y evolución de la dignidad humana

En la era antigua, los griegos ahondaron en la realidad de la naturaleza y en la realidad humana, concibiéndose como una noción de igualdad esencial en todas las personas. Aristóteles, expresó en cuanto a la dominación del hombre sobre el hombre que ésta es artificial, pues esclavitud y libertad ocurren por convenio. Naturalmente no existen

diferencias entre unos y otros, por lo tanto, tales distinciones resultan injustas. Platón, por su parte, percibe al ser humano como el enlace de dos realidades: el alma (divina e inmortal) y el cuerpo (físico y perecedero). Esta dualidad en la percepción del ser humano fue una de las cualidades que definió la dignidad humana. En este sentido, el referido autor plantea que la dignidad humana se expresa en un doble proceso; por una parte, la individualización de la persona y, por la otra, la divinización del hombre (Gallardo, 2020).

En oposición al pensamiento griego, Cicerón plantea una fundamentación de una igualdad natural de todos los seres humanos, al señalar que es infinita y universal. A partir de ahí, hay un nivel más íntimo dentro de *la polis* del propio individuo, que aun cuando es imperfecto, tiene la capacidad para razonar. Por lo que en cuanto se apegue a los dictámenes de la naturaleza, alcanzará la virtud (Pelé, 2010).

Séneca propone el valor propio del ser humano no solo desde la moralidad, sino en defensa de este mismo valor. El reconocimiento de la dignidad humana es paralelo a su protección. Para concientizar sobre el deber que tienen las personas de proteger su dignidad, este filosofo recurre a la conciencia individual y plantea que cada persona debe defender el espacio de su individualidad, pues, según él, es el único bien realmente valioso que con seguridad posee. Séneca planteó la dignidad humana desde la comprensión de la alteridad y la consciencia de la vulnerabilidad ajena (Gil, 2015).

Posteriormente, con la influencia de la fe de las religiones protestantes, se avanza hacia la santidad de la dignidad humana, que se explica, para ese momento, por el carácter de la persona creada a imagen de Dios. A partir de ahí, se instaura un parentesco especial en el ser humano. Desde el punto de vista de estas religiones, en virtud de los atributos que le fueron concedidos al ser humano como el pensamiento, el lenguaje, la bondad, entre otras

cualidades, éste podía expresar su grandeza y superioridad sobre el resto de los seres vivos que están en la naturaleza (Peces-Barba, 2005).

Al respecto, Leibniz (2001, referenciado por Gallardo, 2020), sostiene que la dignidad humana es una idea preexistente, innata en las personas, la cual emana de la naturaleza humana del hombre, pero progresivamente se desconecta de cualquier origen divino. En la actualidad, la dignidad humana se percibe como una noción preexistente, innata en el ser humano.

El concepto de la dignidad humana tiene gran relevancia para el derecho y sus diversas ramas justifican esa importancia. La filosofía del derecho realiza importantes aportes, pues se enfoca en el origen del conflicto que coloca a la dignidad humana como sustento de la ética pública de la modernidad, es decir como un antecedente de los valores políticos y jurídicos, así como los principios y derechos que emanan de esos valores (Restrepo, 2011). En este sentido, es acertado expresar que la dignidad humana es la base de una ética pública laica que se ha venido instituyendo con el pasar del tiempo.

A partir del siglo XV, Kant a través de su modelo de la Ilustración conglomeró ese doble aspecto de la dignidad humana al intentar explicar el concepto de ilustración, donde relaciona al ser humano, "que para él es un fin en sí mismo y que no tiene precio, con la idea de su autonomía, en el sentido que no necesita andaderas y puede caminar por sí mismo" (Peces-Barba, 2005, p. 17).

Desde esta perspectiva, la dignidad se tiene por el hecho de nacer e involucra un ámbito negativo de protección individual que interviene como límite a la conducta de los otros y de cada uno frente a sí mismo. De esta manera, define una esfera de respeto merecida que atañe a cada persona digna y que, luego, posibilitará cimentar la noción de los derechos

humanos propios prepositivos, que se conforman en presuposición de legitimidad del poder del Estado (Restrepo, 2011).

Durante el siglo pasado, como materialización de las nociones liberales, la democracia se impuso, en la teoría y en la praxis, como el único régimen posible para las sociedades modernas. Todo lo cual, dio inicio con la revolución francesa, que, representó un hito para el reconocimiento de lo que se denominó como *dignidad de hombre*. En virtud de los atropellos que las clases más altas propinaban al pueblo francés, dando lugar a la Declaración Universal de los Derechos del Hombre. Fue un hecho trascendental en la historia de la humanidad, pues gracias a esto el *populacho* conoció que tenían garantías básicas que cualquier organización social tiene la obligación de respetar y hacer respetar (Montero, 2005).

Posteriormente, con la revolución industrial, las pugnas sociales se realzaron por el apogeo de la automatización de los procesos productivos, quitándole al ser humano, aparentemente su capacidad para trabajar. En esta época, Marx cimenta la dignidad humana en la capacidad laboral y sostiene que el trabajo es medio a través del cual las personas logran su perfección. La primera guerra mundial, pero sobre todo la segunda guerra mundial, ponen en la palestra el conflicto de la dignidad humana y la imperiosidad de repensar el respeto por los derechos fundamentales de las personas (Comisión Económica para América Latina y el Caribe, 2015).

Los horrores que se materializaron en la Segunda Guerra Mundial condujeron a la constitución de la Organización de las Naciones Unidas (ONU), entre otras organizaciones internacionales, que posibilitaron la creación de una serie de instrumentos jurídicos que protegían la dignidad y los derechos fundamentales de las personas por medio de las disposiciones contenidas en estos convenios entre naciones. Asimismo, representó un cambio

trascendental para las constituciones políticas de los Estados miembros y un gran progreso para los gobiernos que no tenían regímenes democráticos, pues progresivamente han ido modificando sus ordenamientos jurídicos y estructuras políticas para establecer modelos democráticos.

A partir de la creación de la ONU, el término *dignidad humana* fue incorporado de forma predominante en el preámbulo y/o en el texto de una serie de instrumentos jurídicos de rango internacional como la Carta de la ONU (1945), la Declaración Universal de los Derechos del Hombre (1948), la Convención Internacional para la Eliminación de Todas las Formas de Discriminación Racial (1965), el Pacto Internacional de Derechos Civiles y Políticos (1966), el Pacto Internacional de Derechos Económicos, Sociales y Culturales (1966), la Convención Americana sobre Derechos Humanos (1978), la Convención sobre la Eliminación de Todas las Formas de Discriminación contra las Mujeres (1979), la Carta Africana de Derechos Humanos y de los Pueblos (1981), la Convención contra la Tortura y Otros Tratamientos Crueles, Deshumanos o Degradantes (1984), la Convención de Derechos del Niño (1989), la Carta de los Derechos Fundamentales de la Unión Europea (2000), y la Carta Árabe de Derechos Humanos (2004), entre otros.

En esta misma línea, es acertado señalar que el concepto de dignidad humana es fundamental para el constitucionalismo contemporáneo, ya que gracias a los sucesos históricos que se derivaron de la Segunda Guerra Mundial, esta noción se presenta como un núcleo axiológico constitucional que ha dado lógica y significado a todo tipo de democracia (Mendieta & Tobón, 2018).

Ahora bien, históricamente, la noción de dignidad humana ha estado asociada a dos campos adicionales de conceptualización: la persona y los derechos. En cuanto a la persona, al ser el soporte sobre el cual recae lo digno, da respuesta a la cuestión del quien de la

dignidad "y remite a la necesidad o no de diferenciar al ser humano en su naturalidad biológica y al sujeto moral, como algo que le pertenece y lo distingue de lo animal" (Restrepo, 2011, p. 11). Con respecto a los derechos, es complemento de la calidad de digno, si la dignidad se erige en un especial merecimiento social, individual o político, los derechos serán el contexto de definición de lo merecido por aquellos que poseen esa naturaleza. Los derechos humanos resultan ser su máxima expresión y realización histórica.

Desde la constitución de la ONU, los derechos humanos pasaron de ser un tema de interés exclusivo e interno de las naciones, a transformarse en un tema central del derecho y las relaciones internacionales. En los últimos tiempos, las actividades de la comunidad internacional en el contexto de la protección y tutela de los derechos humanos se han incrementado significativamente; de igual modo, se han elaborado y mejorado los instrumentos que consagran estos derechos, así como las instituciones dedicadas a su patrocinio y salvaguarda (Meléndez, 2012).

Martínez (2013), plantea que la democracia y los derechos humanos comparten su estrecha relación e incluso en un grado de cimiento con la noción de la dignidad humana. Continúa explicando, que los derechos fundamentales son una manifestación jurídica de la dignidad de los seres humanos, cuya función radica en permitir y asegurar su respeto, "y la democracia es el ámbito en el que pueden desarrollarse las relaciones políticas de la comunidad en un marco de respeto a la dignidad" (p. 41). En esta misma línea, Restrepo (2011) plantea que el concepto de dignidad humana:

> Opera como principio fundamentador, autónomo y último de los derechos humanos, en tanto se constituye en raíz fundante de los mismos, razón que determina unos límites, una serie de potestades y exigencias inalienables del individuo frente a la organización social, que el Estado está en obligación de reconocer. Y mediante este

> recorrido, se convierte en la condición de surgimiento y justificación de los demás derechos positivos, incluso del derecho mismo, entendido como regulación de la convivencia humana (p. 12).

De la concepción que se tenga acerca de la naturaleza humana emana el tratamiento que debe otorgársele a todo individuo que tenga la referida esencia, a lo que se conoce como dignidad. Debido a las complejidades que se presentan para definir la dignidad humana en las esferas del derecho y la filosofía, el concepto de dignidad más implementado tiene una cualidad simplemente instrumental, a partir de la cual se asocia esta noción al trato o respeto adecuado a los individuos, únicamente, por su esencia de seres humanos, sin justificar por qué se le otorga ese trato (Martínez V. , 2013).

3.1.2 Implicaciones de las transgresiones a la dignidad humana

Al hablar sobre la transgresión de la dignidad humana, se plantea una vulneración a los derechos fundamentales de las personas. En virtud de lo expuesto en la sección anterior, las Cortes Internacionales, actualmente, utilizan el concepto de la dignidad humana para sustentar sus decisiones; una de ellas, es la Corte Europea de Derechos Humanos, que ha implementado la dignidad humana como un componente relevante para interpretar la Convención Europea sobre los Derechos Humanos, aun cuando el referido término no aparezca de forma expresa en su texto. Por su parte, la Corte Interamericana de Derechos Humanos, ha manifestado que la dignidad desempeña un rol importante no solo en clasificación del perjuicio ocasionado por las vulneraciones a los derechos humanos, sino también en la responsabilidad que tiene el Estado en lo inherente a la reparación del agravio (González, 2016).

La Ley Fundamental de la República Federal de Alemania, inicia con un capítulo acerca de los derechos fundamentales y éste, a su vez, empieza con el enunciado "La dignidad humana es inviolable", en su artículo 1, el cual propició que, actualmente, en Alemania, la dignidad humana tenga un rol preponderante en el discurso de los derechos humanos y en la jurisprudencia (Habermas J. , 2010). En el año 2006, la inviolabilidad de la dignidad humana fue un tema que tuvo un gran auge cuando el Tribunal Constitucional de Alemania declaró inconstitucional la *Ley de Seguridad Aérea,* aprobada por el Parlamento alemán en el contexto del ataque terrorista a las torres gemelas del *World Trade Center*. Dicha norma jurídica buscaba "autorizar a las fuerzas armadas a derribar el avión de pasajeros que, en semejante situación, se hubiese convertido en una bomba humana. Y ello con el objetivo de proteger a un número elevado e indeterminado de personas situadas en tierra" (Habermas, 2010, p. 106).

Ante esta propuesta, el Tribunal Constitucional indicó que la muerte de esos pasajeros por parte de instituciones del Estado sería inconstitucional, pues el deber de salvaguardar la vida de potenciales víctimas de un ataque terrorista tiene que ser postergado ante el deber que tiene el Estado de respetar la dignidad de los referidos tripulantes. "…al disponer el Estado unilateralmente de sus vidas, se… les niega a los pasajeros el valor que le corresponde al hombre per se" (Tribunal Constitucional, 2008, citado por Habermas, 2010, pp. 106-107).

Ahora bien, algunos autores plantean que la dignidad implica el rechazo a cualquier noción inherente a la cosificación de la persona, por ende, el ser humano merece un trato digno. En este sentido, el respeto a la dignidad radica en poner límites racionales a cualquier cosa o situación que pueda afectar al ser humano de forma deliberada o accidental (Domínguez M. , 2019).

Según la Corte Constitucional de Colombia, la dignidad es un atributo que le es inherente al ser humano, el cual emana de las características de las personas, como la voluntad y la razón; que son elementos que hacen que la dignidad sea connatural, una condición ontológica de la cual nacen expectativas sociales y, por ende, establece los parámetros de la convivencia social (Restrepo, 2011).

En esta misma línea, la Corte Constitucional colombiana señaló en su sentencia T335 de 2019 que:

> La dignidad humana, el libre desarrollo de la personalidad y la intimidad personal, configuran los elementos básicos para que una persona pueda desenvolverse en sociedad, ya que son los baluartes que garantizan el ejercicio de la libertad y la autonomía individual, sin la intervención de terceros ajenos al fuero íntimo de cada ser humano, siempre que se respeten los derechos de los demás y el orden jurídico. (Sentencia T-335, 2019, párr. 31)

La dignidad de los seres humanos es un valor metajurídico que el derecho tiene el deber de reconocer; cabe acotar que la dignidad no es un derecho, sino que es el basamento de todo derecho. El respeto a la dignidad se instituye como un valor superior, lo opuesto implicaría la autodestrucción de la sociedad, si se menosprecia y desprecia la condición humana de cada individuo, significaría la nulidad de la condición de todas las personas. En síntesis, la dignidad implica el respeto por la condición humana. “La dignidad humana entraña no solo la garantía negativa de que la persona no va a ser objeto de ofensas y humillaciones, sino que supone también afirmación positiva del pleno desarrollo de la personalidad de cada individuo” (Domínguez, 2019, pp. 83-84).

En este sentido, se puede afirmar que la relevancia que se le ha otorgado al desarrollo de los derechos humanos y la democracia no puede visualizarse en el enlace con la noción

que lo sustenta, como lo es la dignidad humana. Debido a esto, se pueden observar criterios que, soportados en la defensa de la dignidad, justifican guerras, intervenciones militares en otros países, trayendo como consecuencia vulneraciones a la dignidad (Bohórquez & Aguirre, 2009).

Adicionalmente, se puede visualizar que en defensa de la dignidad, se sustentan posturas radicalmente opuestas en temas centrales de la vida cotidiana como el aborto, la eutanasia, la investigación científica con embriones humanos, la gestación por sustitución, la atención de personas con enfermedades terminales, entre otros, colocando el desarrollo del conocimiento, la ciencia y la tecnología en la palestra de la opinión pública de toda la humanidad (Martínez V. , 2013).

Otra de las funciones de la dignidad humana es la neutralización de las diferencias irreconciliables en el proceso de distinción y expansión de los derechos humanos. La vulneración de la dignidad humana ha resultado ser esclarecedora, pues permite visualizar las condiciones de vida insoportables y de marginación que padecen las clases sociales pobres, el trato desigual de mujeres y hombres en el lugar de trabajo, la discriminación de los extranjeros, así como de las minorías culturales, lingüísticas, religiosas, étnicas, raciales y de todo aquel que se considere diferente (Bohórquez & Aguirre, 2009).

En este sentido, la Corte Constitucional colombiana, mediante sentencia T-007 de 2020, manifestó que:

> Particularmente, sobre los derechos a la imagen y la intimidad, la Corte ha sostenido que…en la medida en que están íntimamente relacionadas con la dignidad humana "se extiende más allá de la muerte y, por ende, el juez de tutela tiene competencia para establecer [su] vulneración y tomar las medidas de protección correspondientes a pesar del fallecimiento del titular del derecho (Sentencia T-007, 2020, párr. 79).

Estas situaciones de transgresión de la dignidad humana pueden orientar, tanto a la extracción prolongada de las disposiciones normativas de los derechos fundamentales protegidos y garantizados, como el descubrimiento y la institución de nuevos derechos humanos. “Así, la intuición de la dignidad humana, siempre presente en el trasfondo, logra penetrar, en primer lugar, en la conciencia de los afectados y, después, en los textos jurídicos, donde será conceptualmente articulada” (Habermas, 2011, p. 109).

La incorporación de la dignidad humana en el ámbito jurídico sucede de forma global con el desarrollo de la modernidad y las doctrinas liberales e individualistas, adjuntándose en las constituciones políticas de las naciones de forma paralela al proceso de internacionalización de los derechos humanos. Gracias a esto, los derechos humanos se transformaron en un arquetipo ético de las sociedades actuales y en perspectiva de estimación del desarrollo moral de los Estados.

3.1.3 Los delitos informáticos y la vulneración a la dignidad humana

Como se ha venido señalando, la dignidad humana, es percibida con una doble dimensión. En principio, es un valor, un concepto asociado al bien, a la buena conducta, a la moralidad y a la buena vida de cada persona, que es la interna; por otra parte, están los derechos de los individuos, sus responsabilidades y aspiraciones, así como los progresivos deberes de terceros, que es la externa. Debido a la importancia que tiene para la sociedad, así como la necesidad de protegerla, el derecho tiene el deber de tutelar la dignidad humana por medio de sus diferentes especialidades, obteniendo trascendencia en el contexto constitucional como guardián de las disposiciones normativas supremas de la cual se derivan los basamentos del resto de las normas jurídicas, incluso las de naturaleza penal, pues

corresponde a la rama punitiva del derecho tipificar y sancionar las conductas ilícitas y custodiar el respeto de los derechos de las personas (Molina & Lamas, 2018).

Uno de esos derechos es la intimidad de las personas, que además de ser un derecho fundamental protegido por diversos tratados internacionales sobre derechos humanos, es esencial para salvaguardar la dignidad humana y conforma los cimientos de cualquier sociedad democrática. Aunado a esto, se tiene que la dignidad humana consolida y ampara otros derechos como la libertad de expresión, información y asociación, así como el derecho a la propia imagen y al honor.

En este sentido, la Corte Constitucional colombiana señaló en la sentencia C 640 de 2010 que:

> En 1995, se reiteró esta visión del derecho a la intimidad, cuando se afirmó que "…este derecho, que se deduce de la dignidad humana y de la natural tendencia de toda persona a la libertad, a la autonomía y a la autoconservación, protege el ámbito privado del individuo y de su familia como el núcleo humano más próximo". (Sentencia C 640, 2010, p. 1)

La evolución de la ciencia, así como el desarrollo y la masificación de la tecnología ha irrumpido en la vida moderna del ser humano, alterando el funcionamiento de las sociedades contemporáneas y abriendo espacio a nuevas formas de comunicación, así como la aparición de noveles modos de almacenamiento de datos. La globalización de las tecnologías de la información y la comunicación ha sido acelerada y, aun cuando ha traído importantes beneficios para la humanidad, en distintos ámbitos, también se ha propiciado un uso irrestricto de estas herramientas, por lo que han surgido nuevos tipos de delitos que atentan contra la dignidad humana de los individuos, como lo es el ataque a sistemas de almacenamiento de datos.

Un ataque cibernético a un sistema de almacenamiento y procesamiento de datos puede generar impactos negativos importantes; entre las consecuencias que se derivan de un atentado de esta naturaleza es la vulneración de la dignidad humana. Un ejemplo de lo que se comentan puede ser: el ataque contra Apple iCloud en 2014, conocido como *Celebrity Photo Leak*, el cual expuso imágenes íntimas de algunos personajes de la farándula. También está el ataque que se produjo contra la compañía Anthem en 2015, que permitió a los atacantes el acceso a datos de salud de millones de sus clientes norteamericanos (Evaluando Cloud.com, 2016).

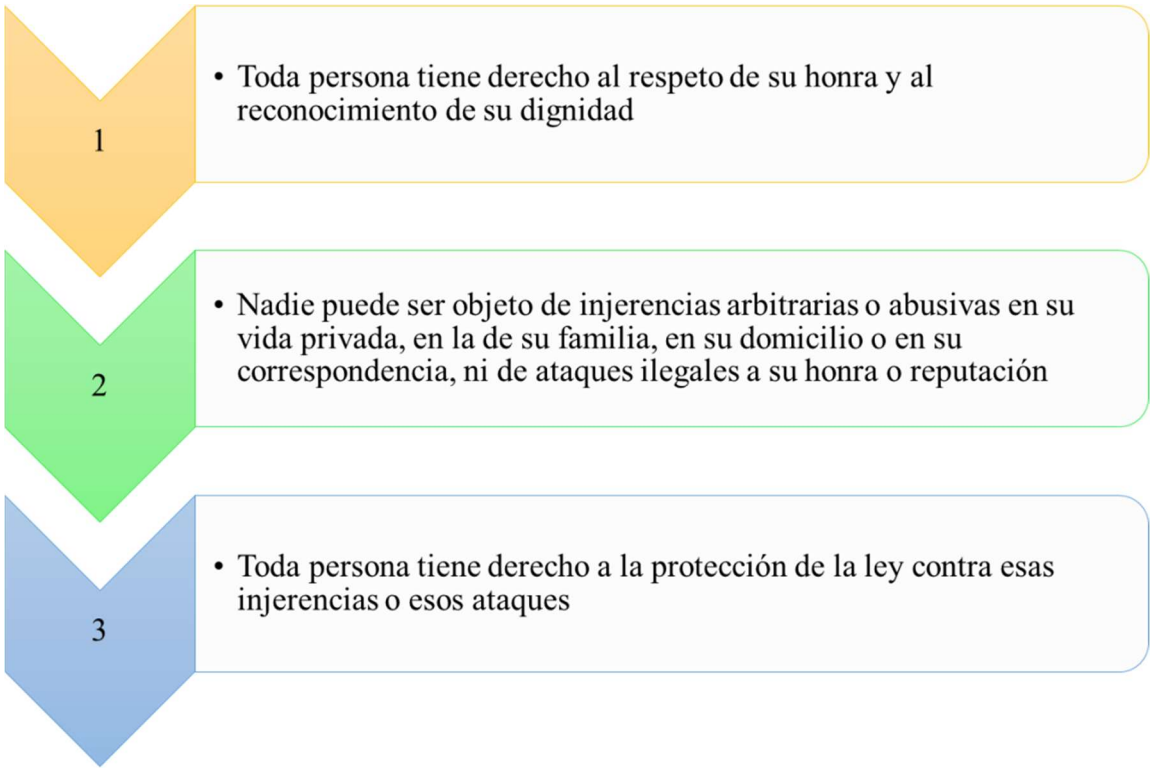
El rápido desarrollo de la tecnología y, la influencia que ésta tiene en el ámbito social y empresarial, ha promovido la materialización de conductas ilegales conocidas como "delitos informáticos", los cuales han abierto un escenario de riesgos muy amplio, así como el estudio de este tema en áreas técnicas y jurídicas, especialmente en aquellos campos asociados con la auditoría informática.

Actualmente, puede visualizarse que cada vez es mayor el impacto y la reiteración de la vulneración de los dispositivos de almacenamiento y procesamiento de información, en sus componentes más sensibles, exponiendo diversos e importantes datos de valor, así como los patrimonios reales de organizaciones y personas, aunado a su dignidad, su vida y honra. En virtud de lo expuesto, se tiene que la evolución desmedida de las posibilidades de interrelación mundial por el empleo de la comunicación satelital ha generado que las personas naturales y jurídicas (públicas y privadas) queden expuestas, debido a la vulnerabilidad de los sistemas de intercomunicación y manejo de los datos, así como la falta de preparación para manipular y cuidar la información (Arias et al., 2010).

Esa transgresión contra los referidos dispositivos de almacenamiento y procesamiento de datos atenta contra los derechos fundamentales que conforman la dignidad

humana, ya que tales dispositivos actúan como una prolongación de la persona, por cuanto contienen parte de sí mismos. Por ejemplo, la intimidad, entendida como el derecho que poseen las personas para aislar al resto de los individuos del conocimiento de su vida privada, controlando quién y cuándo tiene acceso a los diversos aspectos de su vida, consistiendo en un límite que defiende la autonomía de un ser humano frente a los demás y frente a posibles intromisiones indebidas por parte de los poderes públicos. Cabe acotar que la intimidad forma parte de los elementos que componen la dignidad humana (Posso, 2014). En este sentido, la Convención Americana sobre los Derechos Humanos, en su artículo 11 (1969), dispone una protección a la honra y la dignidad, tal como se puede visualizar en la figura 1.

Figura 1. *Protección a la honra y la dignidad por parte la Convención Americana sobre los Derechos Humanos*



Según De Sousa Santos (2014, citado por Chiluisa, 2021), la intimidad personal se transforma en un eje la dignidad humana, “es el lenguaje hegemónico del respeto a los

derechos humanos" (p. 10). En síntesis, la intimidad personal es un derecho que se deriva de la dignidad humana y está jurídicamente protegido por diversas normas nacionales e internacionales. No obstante, el desarrollo acelerado y el uso irrestricto de las TIC ha traído como consecuencia el nacimiento de los delitos informáticos, los cuales son diversos, pero afectan los derechos fundamentales de las personas.

La vulneración de datos personales, atenta directamente contra la dignidad de las personas y por más esfuerzos que se han realizado, los ordenamientos jurídicos en general no han podido estar a la par del avance tecnológio contemporáneo. A continuación, la figura 2, muestra los delitos que atentan contra la intimidad de las personas, según lo establecido en el Código Penal colombiano.

Figura 2. *Delitos que atentan contra la intimidad de las personas*

En síntesis, aquellas conductas que atentan contra el derecho a la intimidad, a la honra, al buen nombre y a la imagen de las personas, vulneran de forma directa e indirecta el derecho a la dignidad humana que tienen las personas en Colombia. De conformidad con lo

dispuesto en el Código Penal colombiano vigente, los delitos que atentan contra el buen nombre y la imagen de las personas, son las que se mencionan en la figura 3.

Figura 3. *Delitos que atentan contra el buen nombre y la imagen de las personas*

3.1.4 Características de víctimas y victimarios a de la dignidad humana mediante delitos informáticos en Colombia.

Los instrumentos que utilizan las personas que perpetran delitos informáticos han evolucionado con el pasar de los años, desde el disquete, pasando por memorias portátiles con puertos USB, hasta correos electrónicos y salas de conversación virtual de internet, con el fin de vulnerar los derechos de las personas. No obstante, actualmente, además de los delincuentes informáticos propiamente, otro tipo de criminales ha encontrado los espacios digitales ideales para materializar sus delitos, un ejemplo de ello son los pedófilos que se dedican a generar confianza online con niños para, posteriormente, aprovecharse de ellos, violarlos, secuestrarlos e incluso asesinarlos (Arias, et al, 2010). Además, se pueden

encontrar falsificadores, estafadores, Didefraudadores, proxenetas, secuestradores, traficantes de drogas, armas, pornografía e información, así como sicarios, terroristas, entre otro tipo de delincuentes que se valen de las TIC para perpetrar o concretar sus actos ilícitos. En este sentido, se hace referencia hacia la evolución tecnológica de los delitos clásicos. Sin embargo, los delitos informáticos sobre la dignidad humana, en sí mismos, constituyen no solo la evolución cibernética de los delitos convencionales, sino una forma nueva de atacar o de irrespetar al otro, al amparo de la invisibilidad que ofrece la red y las herramientas tecnológicas.

Es importante aclarar que los delitos informáticos además de estar asociados a la materialización de un hecho ilícito por medio de instrumentos informáticos también están relacionados con la afectación de la información per se, como bien jurídico protegido, distinto a los intereses jurídicos tradicionales (Suárez-Sánchez, 2009, referenciado por Arias et al., 2010).

En el año 2019, la TicTac concluyó que en el contexto colombiano:

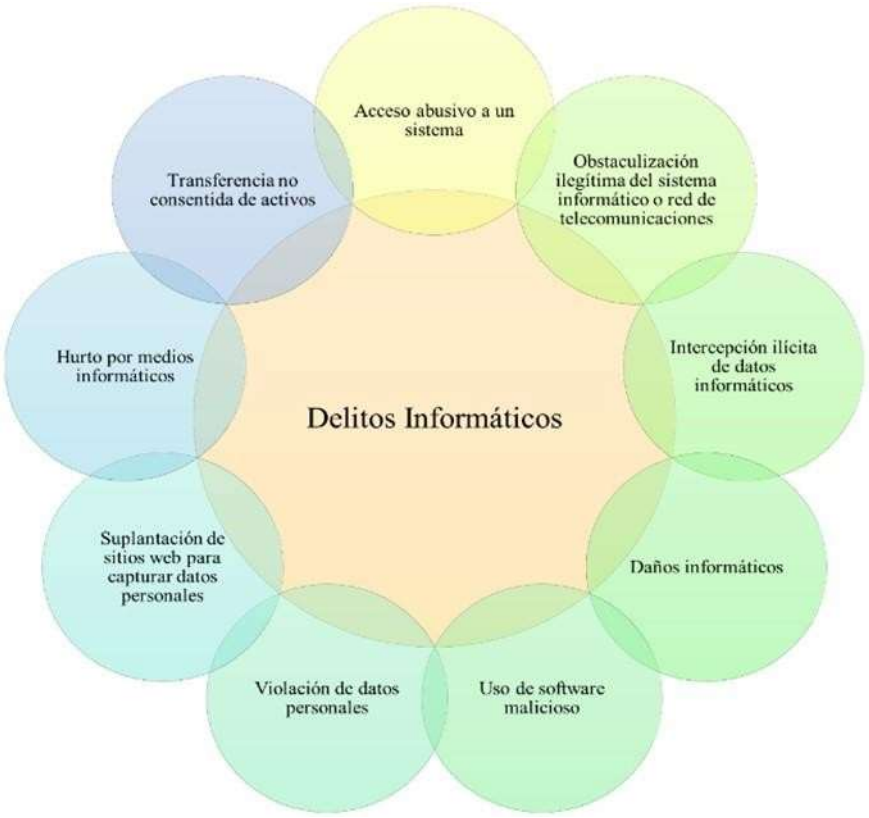
> El hurto a través de medios informáticos es el que ocupa el primer puesto de denuncias en Colombia (31058 casos); seguido por infracción a información personal (8037) y el acceso inapropiado y sin previo consentimiento (7994 acusaciones). Asimismo, último, dentro de esta lista, cabe mencionar las transferencias involuntarias de activos (3425). Por último, el uso de virus o software malicioso (2387) (TicTac, 2019, referenciado por Ramírez et al., 2020, p. 5).

Es menester aclarar que, en el contexto de los delitos informáticos, los victimarios gozan del anonimato que le brindan las TIC, por lo que es difícil tener un perfil exacto de estos criminales. No obstante, cuando se trata de las víctimas cuya dignidad humana se ve transgredida por esta clase de ilícitos, cualquier persona que tenga sus datos almacenados en

una base datos, haga uso del Internet y sistemas informáticos está expuesta a la lesión de su dignidad, sobre todo los adolescentes que no tienen reparos en compartir cada detalle de su vida en las redes sociales.

El Código Penal colombiano vigente clasifica y tipifica los delitos informáticos, tal como se muestra en la figura 4

Figura 4 *Clasificación de los delitos informáticos, según el Código Penal colombiano vigente*



Bechara *et al.*, (2020), explica que estos delitos tipificados por el Código Penal colombiano, consisten en lo siguiente:

- Acceso abusivo a un sistema informático: Tipificado en el artículo 269A. Se materializa cuando el hacker se vale de la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad

informática instaurados por las organizaciones con el propósito de obtener beneficios económicos, para investigar o, en algunos casos, para evidenciar la capacidad y los recursos que brindan las TIC.

- Obstaculización ilegítima del sistema informático o red de telecomunicación. Tipificado en artículo 269B. Se perfecciona cuando el hacker bloquea ilícitamente un sistema o imposibilita su acceso de forma temporal. Asimismo, este delito encuadra el ingreso a cuentas de correos electrónicos sin el conocimiento ni el consentimiento de sus propietarios, así como la disposición o bloqueo de las claves obtenidas de diversas maneras.
- Intercepción ilícita de datos informáticos. Tipificado en el artículo 269C del Código Penal colombiano y en el artículo 3 de la Convención de Budapest. Consiste en la obstrucción de datos sin autorización legal, en su lugar de origen, en el destino o en el interior de un sistema informático o de emisiones electromagnéticas de un sistema electromagnético que los transporte.
- Daños informáticos. Tipificado en el artículo 269D. Se presenta cuando un individuo, sin autorización, cambia, altera, perjudica, elimina, borra o destruye datos del programa o de documentos electrónicos.
- Uso de software malicioso. Tipificado en el artículo 269E. Se materializa cuando se generan, obtienen, venden, distribuyen, envían, incorporan o extraen del país programas informáticos que ocasionan detrimento en los recursos de las TIC.
- Violación de datos personales. Tipificado en el artículo 269F. Se perfecciona cuando una persona, sin estar autorizada, extrae, vende, compra, envía, publica o implementa información personal almacenada en ficheros, archivos, bases de

datos o sistemas parecidos con el propósito de darle uso personal o para terceros. La legislación penal colombiana, tipifica este acto, con la finalidad de proteger los derechos fundamentales de los conciudadanos, como la libertad ideológica y la dignidad humana.

- Suplantación de sitios web para capturar datos personales. Tipificado en el artículo 269G. Consiste en el acceso a sistemas informáticos con el fin de estafar y obtener información confidencial, fraudulentamente, a través de una página web o un dominio parecido al de la entidad a la cual se quiere abordar. Cuando la víctima no diferencia la original de la falsa, suministra datos personales, claves bancarias, entre otras informaciones privadas que, posteriormente, el suplantador guarda en una base de datos y, luego, utiliza para beneficio propio y/o de terceros.
- Hurto por medios informáticos o semejantes. Tipificado en el artículo 269I. En este escenario, se perpetra el delito de hurto a través la manipulación de sistemas informáticos, red sistema electrónico, telemático o cualquier otro medio parecido; también se materializa por medio de la suplantación de un usuario ante los sistemas de autenticación y de autorización establecidos.
- Transferencia no consentida de activos. Tipificado en el artículo 269J. Consiste en la transferencia no consentida de cualquier activo en perjuicio de un tercero, valiéndose de alguna manipulación informática o artificio semejante.

En este sentido, se puede observar que el Código Penal colombiano (1995) prevé la protección de la intimidad de las personas, de hecho, dedica un título completo a esto, como lo es el Título X “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad

del domicilio", en el cual brinda especial atención a la transgresión de la intimidad de las personas a través de medios informáticos, electrónicos y telemáticos.

Como se ha venido señalando, la intimidad consiste en la facultad jurídica que tienen las personas para excluir a terceros de ciertos ámbitos que se extienden a la vida privada de los individuos. Por consiguiente, las presunciones inherentes al acceso a los secretos documentales, control ilegal de sonido o imagen de las personas, intercepción de telecomunicaciones y/o allanamiento de morada son concebidas como transgresiones de esas facultades de aislar a terceros en algunos ámbitos jurídicos de naturaleza limitada (Mata, 2003).

3.2 El sistema legal colombiano de protección de datos.

En esta parte de los resultados se abordan los aspectos más relevantes del sistema legal colombiano en lo que a protección de datos personales se refiere. Para ello, se esboza el marco legal que rige el desarrollo de nuevas tecnologías en el territorio colombiano, así como la seguridad cibernética desde la perspectiva legal. Por último, se presentan las debilidades y fortalezas del ordenamiento jurídico colombiano en relación a la protección de datos de índole personal.

El desarrollo de esta sección amplía la visión de la legislación nacional en materia de protección de datos de carácter personal, así como de seguridad cibernética, a fines de comprender mejor cuáles son esas debilidades que pueden fortalecerse con la adición de elementos potencialmente incorporables al marco legal colombiano que rige la protección de datos, que promuevan la disminución de delitos informáticos que atentan contra la dignidad humana.

3.2.1 Nuevas tecnologías y legalidad en Colombia

Con la evolución acelerada de las tecnologías a nivel global, se vio la necesidad de regular el desarrollo de este campo, con el fin de promover el avance de Colombia en esta área y, a su vez, proteger y garantizar el cumplimiento de los derechos que tiene cada una de las personas que habitan en el territorio colombiano.

En este sentido, el en el año 1991, se promulgó el Decreto 393 por medio del cual "se dictan normas sobre asociación para actividades científicas y tecnológicas, proyectos de investigación y creación de tecnologías" (Decreto 393, 1991, p. 1). Esta norma busca que personas jurídicas sin ánimos de lucro se asocien con entidades del Estado con los propósitos que se indican en la figura 5.

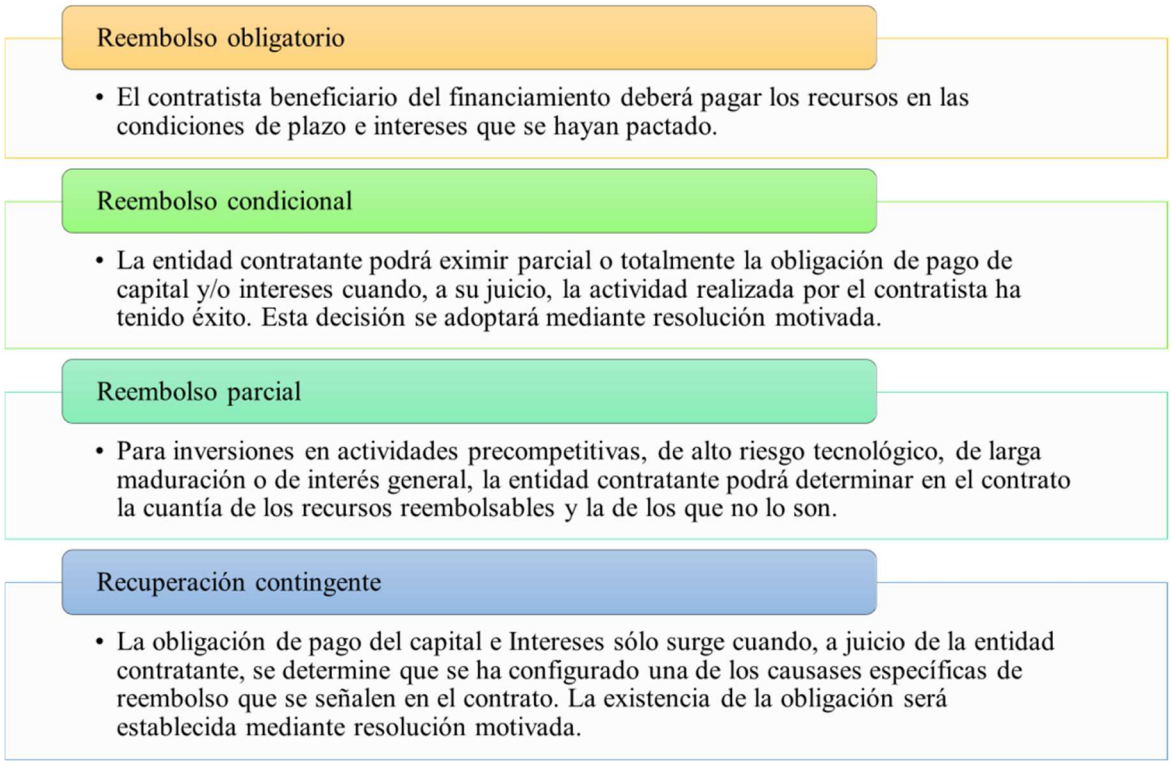
Figura 5 *Propósitos de la asociación para el desarrollo de actividades científicas y tecnológicas*

Ahora bien, para comprender que entiende la legislación colombiana por actividades científicas y tecnológicas, se recurre al artículo 2 del Decreto 591 de 1991, las cuales se enlistan en la figura 6.

Figura 6 *Actividades científicas y tecnológicas, según el Decreto 591 de 1991*

De igual modo, se prevé que la Nación, a través de sus entidades descentralizadas puedan celebrar contratos de financiamiento con el propósito de desarrollar las actividades científicas y tecnológicas, cuyo objeto sea suministrar recursos al particular contratista o a otra entidad pública, en cualquiera de las formas que dispone el artículo 8 del Decreto 591 de 1991, tal y como se muestra en la figura 7.

Figura 7 *Formas de contratos de financiamiento destinados a actividades científicas y tecnológicas*



Cabe acotar que, de conformidad con lo indicado en el artículo 9 del referido Decreto, la Nación y sus entidades públicas descentralizadas pueden celebrar contratos de administración de proyectos, tanto con personas jurídicas públicas como privadas, para el desarrollo de las actividades científicas y tecnológicas.

En esta misma línea, con el progreso de la tecnología se presenta la imperiosidad de acondicionar el ámbito de las tecnologías de la información y la comunicación en Colombia para enfrentar los retos que implica el progreso de la confluencia tecnológica, institucional y de mercados, suponía esbozar una nueva simetría entre el fomento del avance competitivo del sector, así como la ejecución de los propósitos de mayor revestimiento y acceso de los colombianos, instituciones públicas y empresas a las TIC, procedente del carácter de servicio público que presumen las telecomunicaciones (Guerra & Oviedo, 2011).

En virtud de lo expuesto, en el año 2009, se sanciona la Ley 1341 o Ley de Tecnologías de la Información y las Comunicaciones (TIC). Esta norma jurídica, configura el reconocimiento por parte del Estado colombiano a que el impulso del acceso, empleo y apropiación de las TIC, la evolución y la implementación eficiente de la infraestructura, la creación y evolución de contenidos y aplicaciones, protección a los usuarios, formación del talento humano en cuanto a estas tecnologías y su índole transversal representan cimientos esenciales para la materialización de las sociedades de la información del conocimiento y repercuten en la perfección de la inclusión social y de la competitividad de la nación. La referida legislación proporciona una percepción unificada aplicable a las TIC fundamentado en cuatro ejes elementales:

- Principios claros, que definen el horizonte de mediano y largo plazo tanto para el Gobierno como para la industria en un sector sujeto a permanentes innovaciones tecnológicas y de mercado.
- Unificación del marco institucional, consistente con la convergencia tecnológica y de mercado que genera nuevas oportunidades de negocio para los proveedores de redes y servicios de telecomunicaciones, así como la expansión de las posibilidades de nuevos servicios de calidad para los usuarios.
- Reglas claras para la solución de conflictos que se puedan presentar en el acceso y uso de la infraestructura de telecomunicaciones.
- Régimen de transición, que permite la adopción gradual de los principios de habilitación general por parte de los proveedores de redes y servicios, consecuente con los incentivos adecuados a la inversión que debe proveer el Estado para generar confianza en la inversión privada, tanto doméstica como extranjera. (Guerra y Oviedo, 2011, p. 8)

Es imperioso manifestar que las tecnologías informáticas son cada vez más necesarias para la ejecución de tareas en la mayoría de los escenarios que tiene la sociedad, esto despierta e incrementa la inquietud sobre el empleo de la información y los niveles de seguridad sobre los datos personas y la intimidad de las personas que contienen estos.

3.2.2 Seguridad cibernética desde la perspectiva legal

La seguridad cibernética adquiere mayor relevancia, cada vez, sobre todo en el escenario empresarial, esferas que implican los ámbitos de protección, entre sus preocupaciones. La creciente necesidad e importancia de proteger la información obedece a las frecuentes irregularidades electrónicas, tecnologías de protección que cada día son más limitadas e ineficientes, mayor dependencia de la tecnología para la elaboración de actividades, así como maneras de hacer negocios (Pereira, 2015).

La ciberseguridad o seguridad cibernética es definida por la Asociación de Auditoría y Control sobre Sistemas de Información (citado por Martínez, 2017), como la "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (p. 104).

En los últimos tiempos, Colombia, así como muchos otros países, se han implementado normas jurídicas que buscan proteger los datos desde su confidencialidad, integridad y disponibilidad, con la finalidad de eludir conflictos en el campo de la autenticación; dicho de otra manera, el obstáculo de actos usurpadores, y que se ofrezca verdaderamente una garantía con respecto a que el individuo que envía el contenido de un mensaje es el propietario de la cuenta de correo electrónico (Candelario & Rodríguez, 2015).

En virtud de lo expuesto, resulta imperioso que, tanto la parte jurídica como por la técnica, se integren, pues el volumen de información que, a diario, se procesa garantiza un desarrollo de dimensionamiento soportado en la clase de datos, a partir de lo cual se derivan los conceptos de privacidad, intimidad y seguridad de la información.

En Colombia, debido a las complejidades que tuvo el ámbito jurídico para conceptualizar algunos términos, fue a partir de 1999 que se comenzó a legislar lo inherente a la seguridad cibernética de la información, de forma específica, las regulaciones que cualquier individuo o empresa debe cumplir con el fin de mantener segura la información, además de cumplir con los requisitos que la ley exige (Fuquene, 2019). En sentido, la tabla 1, señala las normas jurídicas vigentes, en Colombia, en materia de seguridad cibernética.

Tabla 1

Normas jurídicas colombianas vigentes, en materia de seguridad cibernética

Norma Jurídica	Finalidad de la Norma Jurídica
Ley 527 de 1999	Definir y reglamentar el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, así como establecer las entidades de certificación y dictar otras disposiciones.
Ley 599 de 2000	Expedir el Código Penal Colombiano. Cabe acotar que, en esta ley se preservó la estructura del tipo penal de "violación ilícita de comunicaciones". Además, se creó el bien jurídico de los derechos de autor y se incluyeron algunas conductas vinculadas indirectamente con el delito informático, como: ofrecer, vender o comprar dispositivos para interceptar la comunicación privada entre personas. Adicionalmente, se tipificó el "acceso abusivo a un sistema informático".
Decreto 1524 de 2002	Reglamentar el artículo 5 de la Ley 679 de 2001, inherente a Pornografía en menores de edad.
Ley 1266 de 2008	Dictar disposiciones generales del hábeas data y regular el manejo de la información contenida en bases de datos personales, especialmente información financiera, crediticia, comercial de servicios y aquella que proviene de terceros países. Asimismo, se dictan otras disposiciones.

Norma Jurídica	Finalidad de la Norma Jurídica
Ley 1341 de 2009	Definir principios y conceptos acerca de la sociedad de la información y la organización de las TIC; crear la Agencia Nacional del Espectro y dictar otras disposiciones.
Ley 1336 de 2009	Adicionar y robustecer la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.
Ley 1273 de 2009	Modificar el Código Penal; crear un nuevo bien jurídico tutelado denominado "protección de la información y de los datos"; preservar integralmente los sistemas que utilicen las TIC; dictar otras disposiciones.
Resolución 2563 de 2010	Regular la administración de bases de datos del sistema de portabilidad numérica.
Ley 1581 de 2012	Dictar disposiciones generales para la protección de datos personales.
Decreto 1377 de 2013	Reglamentar parcialmente la Ley 1581 de 2012.
Resolución 5111 de 2017	Establecer el régimen de protección de los derechos de los usuarios de servicios de comunicaciones; modificar el capítulo 1 del Título I de la Resolución CRC 5050 de 2016; dictar otras disposiciones.
Decreto 255 de 2022	Adicionar la Sección 7 al Capítulo 25 de la Parte 2 del Libro 2 del Decreto 1074 de 2015. Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.

En este sentido, es importante aclarar que, las normas jurídicas deben tener en cuenta los desarrollos tecnológicos, pues, generalmente, están más adelantados que las legislaciones que aplicables. Debido a esto, es importante que el Estado colombiano tenga la posibilidad de incorporarse a estándares internacionales que le permitan acoplarse a un marco jurídico que, quizás, no se esté implementando en la esfera nacional e incluso regional.

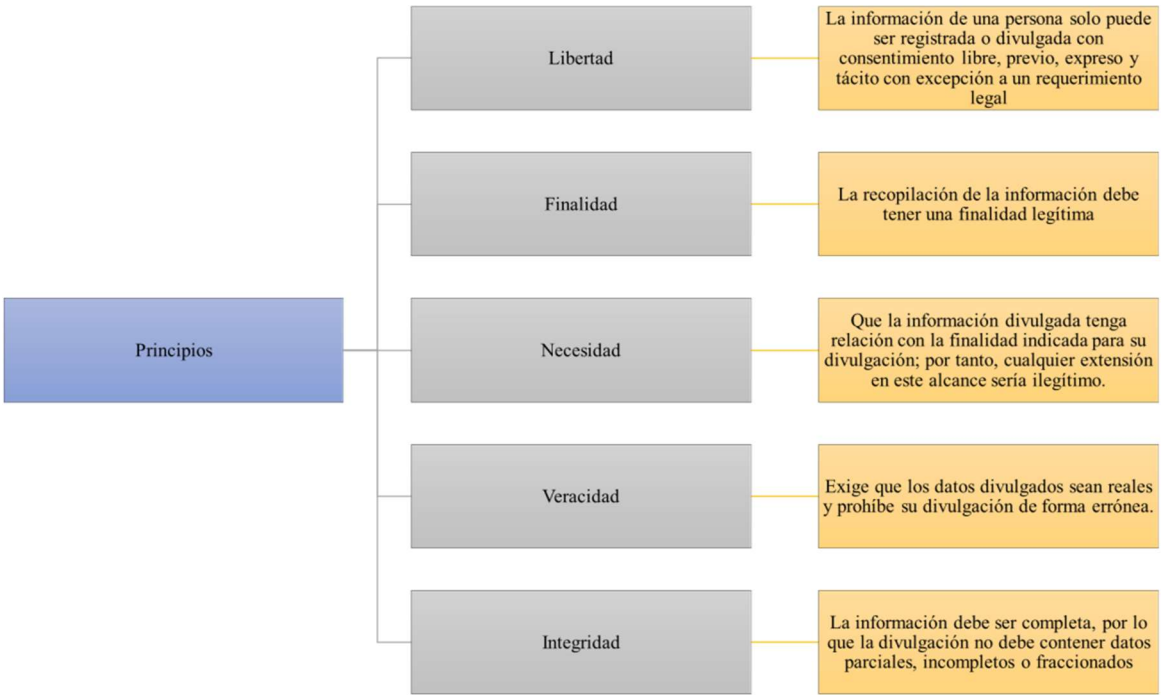
Cabe acotar que, la legislación sobre seguridad cibernética, en Colombia, además de proteger los sistemas en general, está orientado a salvaguardar la información que está

guardada en los sistemas de almacenamiento y procesamiento de datos. Según Ducuara y Soto (2018), existen cuatro (4) tipos de información, tal y como se explica en la figura 8.

Figura 8 *Tipos de información de acuerdo con la Constitución colombiana*

En este sentido, el artículo 15 de la Constitución colombiana señala tres derechos fundamentales como lo son el derecho a la intimidad, al buen nombre y al habeas data. Ahora bien, el derecho a la intimidad cuenta con cinco principios que lo fundamentan, tal como se muestra en la figura 9.

Figura 9 *Principios que fundamentan el derecho a la intimidad*



En esta misma línea, el referido autor plantea que, con base en los principios señalados en la figura 9, y como un derecho individual está el derecho al buen nombre que hace referencia a la reputación de las personas, por lo que la vulneración de cualquiera de los principios ut supra, puede transgredir este derecho, debido a que no cumple con los criterios que establecen las normas jurídicas para garantizar la confidencialidad y la integridad de la información. Por otra parte, el derecho al habeas data contempla tres facultades, como lo son el derecho a conocer la información que refiere a una persona, derecho a actualizar la información y el derecho a la rectificación; este derecho puede ser vulnerado si al momento de recolectar los datos no se cuenta con el consentimiento libre, previo y expreso del titular, si estos son erróneos o está categorizada como información personal reservada (Fuquene, 2019).

Aun cuando en Colombia, existe un marco regulatorio para garantizar la seguridad cibernética y proteger los datos personales, las denuncias por la vulneración de sistemas informáticos va en aumento, sin contar aquellos casos en los que los individuos no denuncian

o no desconocen que están siendo víctimas de conductas que constituyen delitos informáticos. Cada vez, el número de delitos informáticos aumenta en cantidad y frecuencia; asimismo, a diario se descubren nuevas formas de vulnerar los sistemas de almacenamiento y procesamiento de datos, por lo que resulta complejo que las legislaciones estén a la par de la tecnología, sobre todo en lo inherente a la seguridad cibernética.

3.2.3 Debilidades y fortalezas del sistema legal colombiano de protección de datos.

El desarrollo acelerado de la tecnología, el auge del internet y la implementación cada vez más frecuente de las transacciones financieras virtuales, ha propiciado el crecimiento desmedido de los delitos informáticos, los cuales amenazan la integridad, intimidad, disponibilidad, seguridad y confiabilidad de la información y los activos que las personas naturales y jurídicas poseen.

La obtención de información por medio de la vulneración de los dispositivos de almacenamiento y procesamiento de datos, afecta tanto a personas naturales como al Estado, poniendo en una situación de riesgo a la infraestructura de las entidades públicas y privadas. Con la finalidad de generar gobernabilidad en el ámbito de ciberseguridad y la protección de datos personales, el Estado colombiano ha planteado estrategias, planes, proyectos, políticas públicas e iniciativas que suministren los parámetros necesarios para lograr este propósito (Osorio, 2018).

Hoy en día, la mayoría de los procesos se encuentran automatizados, por lo que es seguro señalar que la información fluye en volúmenes incalculables por diversos medios como redes privadas de información, redes sociales, redes públicas servidores de almacenamiento de datos en la nube, lo cual ocasiona que la interconectividad de distintos

sistemas exhorte al cuidado, custodia, protección, garantía y seguridad de la información (Osorio, 2018).

El tratamiento de los datos personales se convirtió en un negocio multimillonario; sin embargo, los derechos fundamentales de las personas, así como los intereses del Estado no deben ser afectados; razón por la cual, Colombia, debe sancionar una legislación adecuada y eficiente, en el corto plazo, que garantice la protección de los derechos constitucionales de los individuos, los intereses del Estado colombiano y que, a su vez, permita la fluidez de la información, como una praxis natural de la cual la sociedad de la información, en la cual los seres humanos conviven.

Como se indicó anteriormente, la Constitución Nacional prevé en su artículo 15 el derecho fundamental a la intimidad y al habeas data.

> **Artículo 15.** 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.
>
> La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

> Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

En este sentido, es acertado señalar que el habeas data es un derecho fundamental autónomo que, asimismo, representa un medio de protección de derechos fundamentales. Cabe acotar que, este derecho fue ideado con el propósito de hacer frente a los abusos que pueden derivarse del poder que tiene la informática y el desarrollo de la tecnología, los cuales facilitan la transmisión ilimitada de los datos personales de los individuos. Este derecho posibilita que las personas que habitan en el territorio colombiano tengan la facultad de controlar y acceder a los datos que se utilizan ellas, por parte de terceros (Rueda, 2012).

De conformidad con lo dispuesto en los artículos 15, 16 y 20 de la Constitución Política de Colombia, existe una estrecha relación entre el derecho a la intimidad de las personas, el derecho al libre desarrollo de la personalidad y el derecho a rectificar la información errónea que una persona autorizó para la implementación en bases de datos o sistemas de información, lo cual da lugar al habeas data.

Con respecto a este derecho la Corte Constitucional de Colombia ha emitido diversos criterios. En la sentencia T 729 de 2002, se reitera el carácter autónomo del habeas data, por considerar que este es un derecho autónomo del derecho a la intimidad. Por su parte, en sentencia C 748 de 2011, la Corte Constitucional define y reitera el núcleo fundamental del derecho al habeas data.

> El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos,

> así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales (Sentencia C 748, 2011, p. 229).

En virtud de lo expuesto por la Corte Constitucional, en el año 2012 se emitió la Ley 1581, "por la cual se dictan disposiciones generales para la protección de datos personales". La referida ley nace en razón de la imperiosidad de establecer normas "obligatorias, generales e integrales para el tratamiento de datos personales que respondan a la reglamentación integral de un derecho fundamental" (Ruiz, 2017, pp. 12-13).

En este sentido, se puede visualizar que en Colombia se han hecho esfuerzos importantes, para legislar sobre la protección de datos personales; sin embargo, las normas jurídicas vigentes poseen algunas inconsistencias que terminan representando una debilidad del marco jurídico colombiano en el ámbito de protección de datos personales. Un ejemplo de lo indicado es el artículo 2 de la Ley 1581 de 2012.

> **Artículo 2.** La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales

El referido artículo refiere al ordenamiento jurídico colombiano, el cual es aplicable dentro del territorio nacional, de acuerdo a sus límites fronterizos. Ahora bien, es importante tener en cuenta que, en la mayoría de los casos, los responsables o encargados del tratamiento de los datos personales están fuera del territorio colombiano, como lo es el caso de Google, Facebook, Twitter, Instagram, Gmail, Hotmail, Yahoo!, Microsoft, entre otros, razón por la cual de haber una vulneración en esos sistemas que afecte los derechos fundamentales de un

colombiano sería imposible aplicar la legislación colombiana, pues al estar ubicados en Estados Unidos de América, el régimen legal aplicable es el de ese país.

Dicho de otra manera, el marco legal colombiana en materia de protección de datos personales adolece de fuerza de cumplimiento frente a otras jurisdicciones, sobre todo si no existen convenios internacionales firmados entre las partes involucradas, es decir, entre Colombia y el país donde se encuentren almacenados los datos personales de los individuos.

En el contexto de Estados Unidos, tal como lo explican Ducuara y Soto (2018), la Ley Patriota, sancionada luego de los ataques terroristas del 11 de septiembre de 2001, tiene como finalidad proteger los intereses de los Estados Unidos de América y fortalecer los temas de seguridad nacional, tal como lo dicta el artículo 215 de la mencionada ley, el cual indica que el FBI puede, en cualquier momento, acceder a los registros de las bases de datos de los operadores de servicios de internet, en pro de la seguridad nacional. En ese escenario, se estarían vulnerando los derechos a la intimidad de los colombianos y las personas que habitan en el territorio nacional, el cual pretende ser normado por la Ley de Protección de Datos de Colombia.

Aun cuando el legislador ha hecho grandes esfuerzos para garantizar la protección de los datos personales, las normas jurídicas vigentes que regulan la materia en Colombia no gozan de fundamento para dar respuesta a las necesidades que emanan del uso del internet y de sistemas de almacenamiento y procesamiento de datos, ya que estos se encuentran encuadrados en una dinámica globalizada que requiere de una regulación más amplia y estricta que abarque varios ámbitos de aplicación extraterritoriales acorde con la realidad que se tiene a nivel mundial (Duacuara & Soto, 2018).

En virtud de lo señalado hasta ahora, las normas jurídicas que regulan la protección de datos personales, no responden a las demandas que existen en la actualidad. Además de

contar con una legislación adecuada orientada a proteger los derechos fundamentales de los colombianos, especialmente el derecho a la intimidad, es importante educar a los miembros de la sociedad colombiana, que sean usuarios del internet a fines que tomen acciones conscientes para optimizar la confidencialidad, integridad y disponibilidad de sus datos en la red.

3.3 Sistema legal español de protección de datos en el marco de Comunidad Europea

En esta sección de los resultados se esboza el sistema legal español en materia de protección de datos, en el marco de la Comunidad Europea a los fines de conocer las novedades que presenta esta legislación y cuáles pueden incorporarse en el ordenamiento jurídico colombiano, con el propósito de fortalecerlo y disminuir la perpetración de los delitos informáticos en Colombia.

Para ello, se procedió a presentar las debilidades y fortalezas del sistema legal español en relación a la protección de datos; asimismo, se indican las lecciones de la Comunidad Europea en materia de delitos informáticos que afectan la dignidad humana. De igual modo, se efectuó una comparación entre el marco legal de protección de datos colombiano frente al español para, posteriormente, proceder a señalar cuáles serían esos elementos potencialmente incorporables a la legislación colombiana para mejorar el ordenamiento jurídico colombiano que regula la protección de datos, con el propósito de promover la disminución de los delitos informáticos que atentan contra la dignidad humana.

3.3.1 Sistema legal español de protección de datos (debilidades y fortalezas)

En la legislación española, la protección de datos personales tiene líneas bien delimitadas; por una parte, dispone que la noción del derecho fundamental a la protección de

datos personales determina al dato personal como la información vinculada a una persona identificable independientemente de su naturaleza (pública o privada, natural o jurídica). Por otra parte, desde el punto de vista de la implementación de normas de la protección de datos personales, el componente esencial consiste en una definición decisiva, como lo es el tratamiento que se le da a dicha información (Trillo, 2019).

En España, el derecho a la protección de datos no está consagrado expresamente en la Constitución Nacional, sino que se incorporó en sus disposiciones lo que, posteriormente, sería el sustento y el marco normativo español en el ámbito de protección de datos. Este derecho está inmerso en el artículo 18.4 de la Constitución de España, siendo el Tribunal Constitucional español el responsable de dictaminar su existencia por medio de la sentencia STC 292/2000, de 30 de noviembre de 2000, en la cual se instituyeron los atributos del derecho fundamental a la protección de datos, proclamándolo como un derecho de naturaleza autónoma y diferente del derecho a la intimidad familiar y personal. Adicionalmente, la referida sentencia explica que se protegen todos los datos de índole personal, además de los datos de tratamiento informático (Negrillo, 2021).

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de Derechos Digitales (en adelante LOPDGDD), es el resultado de la adopción del Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (en adelante RGPD), la cual presenta una nueva legislación, europea y nacional, de garantía del derecho a la protección de datos. La referida Ley Orgánica derogó la Directiva 95/46/CE y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La nueva legislación propone una sugerente apreciación acerca del impacto nacional que ha tenido “esta ambiciosa reforma legislativa tanto en el plano del sistema de fuentes normadoras del derecho de protección de datos y de su alcance constitucional como sobre los

novedosos rasgos conformadores de la garantía efectiva de este derecho" (Rallo, 2019, p. 48). En este sentido, es posible afirmar que se está ante la presencia de un nuevo derecho de protección de datos, en virtud del nuevo marco normativo multinivel en el que interactúan normas europeas y normas españolas.

El objeto de la LOPDGDD es adaptar la legislación española en materia de protección de datos al RGDP, así como complementar los preceptos del referido Reglamento para garantizar la protección de este derecho fundamental en lo concerniente al tratamiento que se le da a sus datos y a la libre circulación de estos. Adicionalmente, la LOPDGDD legitima y garantiza una serie de derechos digitales. En este sentido, el artículo 1 de la Ley Orgánica 3/2018 establece el objeto de la ley, a saber:

> Artículo 1. Objeto de la ley.
>
> La presente ley orgánica tiene por objeto:
>
> a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.
>
> El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.
>
> b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

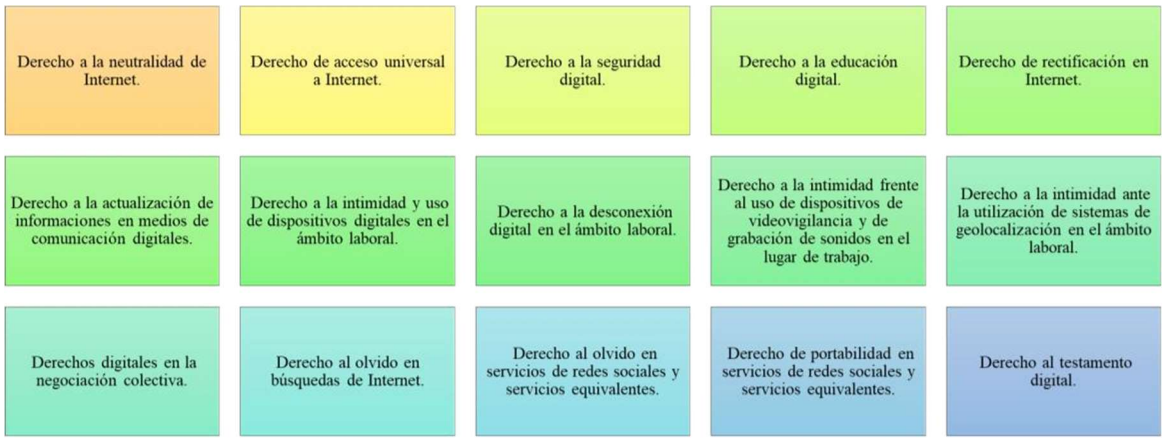
La Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales está conformada por noventa y siete (97) artículos, organizado en diez (10) títulos, veintidós

(22) disposiciones adicionales, seis (6) disposiciones transitorias, una (1) disposición derogatoria y dieciséis (16) disposiciones finales.

La legislación española en materia de protección de datos personales tiene una gran cantidad de fortalezas. Una de ellas es la claridad y amplitud de sus definiciones y conceptos que aparecen de manera expresa en el texto legal. Por ejemplo, a efectos de la LOPDGDD se consideran datos de carácter personal "cualquier información concerniente a personas físicas identificadas o identificables" (artículo 3. a)); cabe destacar que, dicha información puede ser "cualquiera numérica, alfanumérica, gráfica, fotográfica, acústica o del cualquier otro tipo" (artículo 5.1, apartado f del RGPD).

Otro beneficio que trae consigo la LOPDGDD se puede encontrar en su Título X, el cual inserta a la ley *in comento* un conjunto de disposiciones con el propósito de garantizar los derechos digitales de los españoles. El referido Título se denomina "Garantía de los Derechos Digitales" y comprende diecinueve (19) artículos, los cuales legitima y regula una serie de derechos, con la finalidad de atender la necesidad de reconocer un sistema de garantía de estos derechos que, indubitablemente, consigue su anclaje en el precepto impuesto por el apartado cuarto del artículo 18 de la Constitución de España. La figura 10 resume los derechos que reconoce y regula el Título X.

Figura 10 *Derechos Digitales consagrados en la LOPDGDD*



Aunado a lo expuesto, es imperioso resaltar que otro aspecto positivo de esta norma es que el sustento constitucional del derecho fundamental de protección de datos en España se trasladó del contexto nacional al europeo y, sobre este último anclaje, se ha regulado un derecho fundamental homogéneo en todos los países que conforman la Unión Europea (Rallo, 2019).

Por otra parte, la Ley Orgánica 3/2018, de 5 de diciembre, también tiene algunas debilidades. Algunas de ellas se presentan en el contexto de los derechos digitales, pues "en cuanto a los preceptos digitales, se trata de declaraciones de derechos sobre los que no se regulan ni se establecen mecanismos que los garanticen" (Mercader, 2022, p. 2). Adicionalmente, se puede observar una incorporación en la ley *ut supra* que ha demandado especial atención, como lo es la utilización de medios tecnológicos y datos personales en las actividades electorales.

Esta disposición autoriza la recolección de datos personales vinculadas a los puntos de vista políticos de las personas que lleven a cabo los partidos políticos en el contexto de sus actividades electorales, bajo la percepción que está amparada en el interés público, con la condición de ofrecer garantías adecuadas, sin llegar a concretarlas. "La norma permite a

los partidos políticos, coaliciones y agrupaciones electorales utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral" (Martínez, 2019, p. 259). Esta disposición normativa ocasionó debates sobre el tema, así como algunas alarmas en la sociedad debido a la posibilidad que los datos aportados por los ciudadanos se utilizaran indebidamente por parte de los partidos políticos, como por ejemplo la creación de perfiles psicológicos. A modo de síntesis, la figura 11 resume las bondades de la legislación española.

Figura 11 *Bondades de la legislación español*

3.3.2 Lecciones de la Comunidad Europea en materia de legislación sobre delitos informáticos que afectan la dignidad humana

La Unión Europea (UE) concibe la protección de datos como un derecho fundamental, lo cual queda evidenciado al estar consagrado en la Carta de Derechos

Fundamentales de la UE, específicamente en su artículo 8, que expresa que "los ciudadanos de la Unión tienen derecho a que sus datos personales se encuentren debidamente protegidos".

La disputa contra la ciberdelincuencia se enmarca en el Espacio de Libertad, Seguridad y Justicia de la Unión Europea, específicamente, dentro de la esfera de la Europa de la Justicia donde se enlazan instrumentos y mecanismos con el propósito de garantizar una cooperación judicial en materia penal. La Comisión Europea ha manifestado reiteradamente la responsabilidad que tiene en el combate contra la delincuencia informática y reducir cualquier clase de crisis en cuanto a seguridad cibernética se refiere, señalando que:

> Una respuesta eficaz ante los incidentes y crisis de ciberseguridad a gran escala a nivel de la UE requiere una cooperación rápida y eficaz entre todas las partes interesadas pertinentes y se basa en la preparación y en las capacidades de cada uno de los Estados miembros, así como en una acción común coordinada apoyada en las capacidades de la Unión. (Comisión Europea, citado por Anguita, 2018, p. 110)

En este orden de ideas y a los fines de concretar una cooperación y coordinación real entre los Estados miembros de la UE, el Tratado de Funcionamiento de la Unión Europea plantea el principio de reconocimiento mutuo y la aproximación de las legislaciones en el ámbito penal y procesal penal, consagrado en su artículo 88.1. En este sentido, para materializar estos principios el Parlamento Europeo y Consejo tienen la potestad de establecer normas acorde con el procedimiento legislativo ordinario, sin irrespetar las tradiciones jurídicas de los Estados miembros (Faggiani, 2015).

Desde el inicio, la Unión Europea pudo observar con facilidad las posibles contingencias que implican el uso indebido de las nuevas TIC, el Internet y las redes sociales. Es por ello que, ante la ausencia de un concepto determinado de ciberdelincuencia la

Comisión Europea creó su propia definición de delincuencia informática en su Comunicación de 2007 nombrada “Hacia una política general de lucha contra la ciberdelincuencia” (Alarcón & Barrera, 2017).

Según Pons (2017), en la referida Comunicación se disponía que el término ciberdelincuencia abarca tres clases de actividades delictivas. La primera, engloba los modos tradicionales de delincuencia perpetrado a través de las TIC, como la estafa. La segunda, se refiere a los contenidos ilícitos generados y/o difundidos a través de medios electrónicos de comunicación que atentan contra la dignidad humana, por ejemplo, la incitación al odio racial o de género a través de contenidos difundidos por las redes sociales. La tercera, comprende los delitos concretos de las redes electrónicas, como la vulneración de sistemas de almacenamiento y procesamiento de datos.

En este sentido, cada vez se hace más evidente la necesidad de generar un tipo penal que abarque las conductas ilícitas asociadas al derecho informático, en donde se consideren los bienes jurídicos tutelados propios de la era digital, como el derecho a la intimidad informática, a la confidencialidad, la disponibilidad de los datos y sistemas informáticos, a tener confianza en el funcionamiento de los sistemas informatizados y a la integridad (Mayer, 2017).

Cabe destacar que, el combate por parte de la Unión Europea contra la delincuencia informática data de hace muchos años. “Los términos de ciberdelincuencia, ciberdelito y análogos son más recientes, pero ello no impide que la Unión Europea se preocupara con anterioridad, por bienes jurídicos protegidos relacionados como la protección de los datos personales” (Anguita, 2018, p. 112). La cooperación de los Estados miembros ha resultado ser una gran ventaja, pues representa una excelente herramienta para contender, eficazmente,

contra la delincuencia transnacional. Otra estrategia bastante útil ha sido la homologación del derecho penal y el derecho procesal penal entre los Estados miembros de la UE.

En virtud de lo expuesto, es posible afirmar que la Unión Europea ha sido un espacio donde se han logrado avances significativos en cuanto a la armonización normativa en materia de ciberdelitos en la esfera internacional. A partir de la aprobación del Tratado de Ámsterdam se propició la creación y el desarrollo de un Espacio de Libertad, Seguridad y Justicia, amparado bajo las conclusiones del Consejo Europeo de Tampere de 1999, que posibilitó acoger iniciativas comunitarias en la primera década del siglo XXI, orientadas a implementar medidas legislativas penales comunes en los Estados miembros de la UE, con la finalidad de batallar contra la ciberdelincuencia (Sain, 2018).

En el año 2000, la Comisión Europea emite la Comunicación denominada "Creación de la Sociedad de la información más segura mediante la mejora de la Seguridad de las infraestructuras de información y la lucha contra los delitos informáticos", en la cual se esbozan los diversos análisis sobre las diferentes formas para perfeccionar la prevención de los delitos informáticos y el combate contra cualquier acto ilícito asociado a las nuevas TIC. De acuerdo con Domínguez (2003), gracias a este instrumento, fue posible para la UE sumar esfuerzos para optimizar la protección de las infraestructuras de información y comunicación, así como la implementación de disposiciones para contrarrestar el contenido criminal y dañino que hay en Internet, con el propósito de proteger los datos de carácter personal.

Posteriormente, siguiendo esta misma línea, se produce otro evento importante con la adopción del Convenio de Budapest de 2001, por parte del Consejo de Europa, pues cuando se aprobó se concibió como el principal instrumento jurídico regulatorio en materia de delitos informáticos a nivel internacional. Entre sus fortalezas constituye una herramienta fundamental a nivel internacional en el ámbito de cooperación internacional para prevenir o

erradicar el impacto de la delincuencia informática. Adicionalmente, permite la adhesión de Estados no miembros del Consejo de Europa, promoviendo la lucha contra el cibercrimen a nivel global (Díaz, 2010).

Por otro lado, para cooperar con la protección de datos personales y el derecho a la intimidad, el Parlamento Europeo aprueba la Directiva 2002/58/CE, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad el sector de las comunicaciones electrónicas, por medio del cual se autoriza a los Estados miembros a regular por ley la obligación que tienen los prestadores de servicios de preservar los datos electrónicos de tráfico de sus clientes, por razones de seguridad nacional, defensa, seguridad pública y el combate contra la cibercriminalidad.

En 2008, la Unión Europea elaboró en su seno la "Estrategia de Ciberseguridad", en donde se detallan los bienes jurídicos que deben gozar de protección, colocando como prioridad esencial los derechos fundamentales como la libertad de expresión, la intimidad y la protección de datos personales. Posteriormente, en 2017, se procedió con la sanción de la Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la UE.

Aunado a lo expuesto, existen muchos instrumentos jurídicos que han nacido en el seno de la Comunidad Europea orientados a luchar contra la cibercriminalidad y los efectos que estos producen, principalmente en la vulneración de los derechos fundamentales de los ciudadanos europeos.

3.3.3 Comparación del sistema legal de protección de datos colombiano y español

Colombia

En virtud de lo expuesto hasta ahora, es posible expresar que Colombia ha progresado, significativamente, en lo inherente a la protección de datos personales, gracias a la emisión de nuevas leyes orientadas a proteger los derechos fundamentales, así como los procedimientos y las herramientas que deben implementarse a los fines de garantizar la salvaguarda de estos derechos.

Desde la jurisprudencia constitucional colombiana empezó a concebirse el derecho de habeas data como un derecho fundamental autónomo, diferenciable de otras garantías como la intimidad y el buen nombre. Sin embargo, si se revisan los estándares que hay a nivel internacional en este ámbito para proteger efectivamente los datos personales, es imperioso implementar estrategias que, equilibradamente, afiancen su seguridad jurídica (Rojas, 2014).

Con la finalidad de dar cumplimiento a los preceptos constitucionales que garantizan el derecho a la intimidad y al habeas data nace la Ley 1266 de 2008, la cual controla el uso de datos personales que componen el historial crediticio y financiero de los individuos, representando la custodia del habeas data crediticio. No obstante, la referida ley se centró, únicamente, en el manejo de datos crediticios y financieros de las personas, razón por la que no logró abarcar la generalidad del tratamiento de datos personales en Colombia (Ariza et al., 2020).

En virtud de los vacíos y lagunas jurídicas derivadas de la Ley 1266 de 2008, se sanciona la Ley 1580 de 2012, a través de la cual se regula el derecho al habeas data con el propósito de proteger los datos personales registrados en cualquier tipo de base de datos que posibilite efectuar operaciones como recolección, almacenamiento, uso y tratamiento por parte de entidades públicas y privadas.

La protección de datos en el contexto colombiano, tiene un marco normativo encuentra su principal soporte en la Ley 1581 de 2012, la cual regula dicha custodia de la información desde su colecta hasta su transmisión, requiriendo de esta manera que el tratamiento de los datos recibidos cumpla con los criterios necesarios para asegurar la salvaguarda integral de los mismos (Aguilar, 2018).

Ahora bien, es menester señalar que la referida ley no hace distinciones de regímenes especiales que se analicen desde la perspectiva jurídica, lo que implica que la norma jurídica tiene aplicación del manejo de los datos personales que se encuentren almacenados en una base de datos, sin diferenciar entre entidades de naturaleza pública o privada, explicando que para tales efectos el manejo de datos se entenderá, según lo dispuesto en el artículo 3 de la Ley 1581 de 2012 como el "conjuntos organizados o depósitos ordenados de datos personales sujetos a tratamiento".

Por otra parte, se puede observar que la legislación colombiana que regula la protección de datos personales debe reforzarse, ya que no produce impactos relevantes debido a que la obligación que tiene la organización que "almacena los datos frente al titular de los mismos se ve reducida cuando no se logra apreciar la reparación a la que tendría lugar en el caso de manipular de forma irregular los datos que le son confiados" (Aguilar, 2018, citado por Ariza et al., 2020, p. 11).

En otro orden de ideas, es preciso volver a recalcar que, en Colombia, el marco regulatorio asociado a la protección de datos personales se reduce a la aplicación de estas normas dentro del territorio colombiano, ya que no ha suscrito Convenios Internacionales de homologación de leyes en este ámbito, como es el caso de los Estados miembros de la Unión Europea. Aunado a esto, son normas jurídicas que no han sido ajustadas a la realidad tecnológica que se tiene hoy en día, por lo que se podría afirmar que la ley vigente no es

efectiva ni eficaz en la prevención de los delitos informáticos que vulneran la dignidad humana ni en la protección de datos personales.

España

En el contexto español, la percepción de los datos personales es distinta a la colombiana y esto queda en evidencia con la estimación que aporta la sentencia STC 290/2000, en donde el Tribunal Constitucional indica que para efectos de proteger los derechos fundamentales, los datos personales engloba toda la información que pueda transgredir el interés individual por parte de un tercero, para ello se requiere que hasta los datos de índole pública se encuentren bajo disposición del titular de la información.

La Ley Orgánica 3/2018, es la norma base en lo que al tratamiento de datos personales se refiere, debido a que a través de esta norma se adapta el ordenamiento jurídico español al RGPD, como se señaló anteriormente, aspirando de esta forma la existencia real de una garantía de la salvaguarda de los datos personales, englobando de esta manera el tratamiento que debe darse a la información dependiendo de la categoría de los datos objetos y de los derechos que de allí se derivan. Esta ley, además de indicar las diversas maneras en que los datos se protegen, también hace referencia lo que atañe al encargado o responsable de tratar los datos y las dinámicas que se materializan.

Adicionalmente, la legislación española en materia de protección de datos incorpora la garantía de los derechos digitales, lo cual robustece, significativamente, el marco regulatorio español, ya que toma en consideración varios aspectos que pudieron haber escapado del legislador europeo. De igual modo, se hace referencia a la protección de los menores de edad en Internet, determinando una edad en la cual el adolescente puede otorgar su consentimiento en lo que concierne al manejo de sus datos personales, sin desvincular al

titular de la patria potestad, pero reconociendo los derechos constitucionales que todo ser humano tiene (Ariza et al., 2020).

Cabe acotar que, la LOPDGDD prevé en su artículo 70, quienes son los obligados a cumplir con el tratamiento idóneo de los datos, razón por la cual, en la referida ley se indican las posibles sanciones que puede acarrear el incumplimiento de estos preceptos normativos en cuanto al manejo de la información (Rojas, 2014).

Aunado a lo expuesto, es imperioso resaltar lo beneficioso que resulta para España y para todos los Estados miembros de la UE contar con un ordenamiento jurídico penal y procesal penal homogenizado, pues facilita la lucha contra los delitos informáticos en un marco de cooperación y coordinación, así como criterios bastante similares, desde la perspectiva jurídica, en cuanto al tratamiento de los datos personales, los derechos fundamentales objetos de protección, las acciones que son consideradas o no como delitos y el régimen legal aplicable, dependiendo de las particularidades de cada caso.

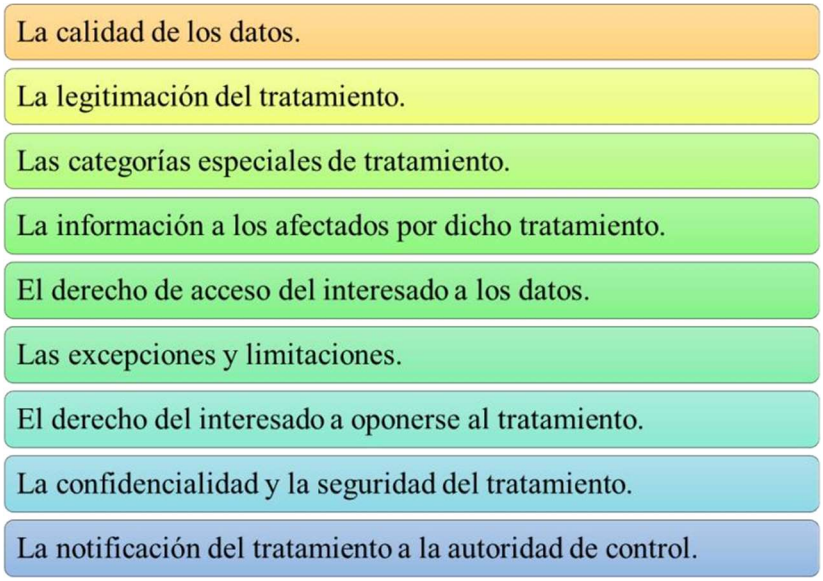
Es importante tener en cuenta que, la Unión Europea, constantemente, se mantiene revisando y actualizando sus disposiciones normativas, por lo que los resultados obtenidos en España y en cualquiera de los países que integran la UE, son más significativos y eficaces en la lucha contra la ciberdelincuencia.

3.3.4 Elementos potencialmente incorporables a la legislación colombiana para mejorar el sistema legal de protección de datos, que promuevan la disminución de los delitos informáticos contra la dignidad humana.

La Directiva 95/46/CE, es la legislación que regula los datos tratados por medios automatizados, al igual que los datos contenidos en un fichero no automatizado o que eventualmente se almacenen en el mismo; el propósito de este instrumento es instaurar un

balance entre una altísima protección de datos personales dentro de la UE; para lograrlo, establece una serie de límites generales para la recolección y uso de los datos personales e informa que cada Estado miembro debe acogerlos en sus ordenamientos jurídicos internos. Los referentes de la Directiva 95/46/CE, se enlistan en la figura 12.

Figura 12 *Referentes de la Directiva 95/46/CE*



España, al ser un Estado miembro de la Unión Europea goza de un ordenamiento jurídico en materia de protección de datos y lucha contra la cibercriminalidad, moderno, acorde con la realidad digital que se tiene hoy en día. De manera constante, la Comunidad Europea está actualizando sus normas jurídicas y homogenizando las legislaciones penales y procesales penales a los fines de poder garantizar una real protección de los derechos fundamentales de los europeos.

Entre los elementos potencialmente incorporables a la legislación colombiana es el consentimiento de los menores de edad para el tratamiento de sus datos personales, a partir de cierta edad, que en el caso de la UE es a partir de los 16 años de edad, esto promueve y protege la progresividad de los derechos de los niños, niñas y adolescente, exceptuando

aquellos escenarios en los que la ley demanda la asistencia de los titulares de la patria potestad del menor.

De igual modo, sería factible inspirarse en la clasificación de la información que tiene el RGPD, pues es más detallado y, por ende, posibilita regular y proteger mejor los datos en función de la categoría a la que pertenezca. La legislación colombiana, como se indicó anteriormente, realiza una distinción muy general y amplia de los tipos de datos, pudiendo perder de vista algunos detalles importantes.

Una de las ventajas que tiene la LO 3/2018 sobre la legislación colombiana es que detalla, expresamente, cuáles son los tratamientos concretos de los distintos tipos de datos, delimitando bien el rango de acción que tienen las entidades que almacenan, procesan y manipulan los datos de índole personal de los ciudadanos. Esto con el propósito de limitar la interpretación de las disposiciones normativas y, a su vez, evitar el uso indebido de los datos, ya que cuando la norma es concreta, no da lugar a dudas en cuanto a cuáles actos son considerados ilícitos y cuáles no.

En este orden de ideas, en la LO 3/2018 y en el RGDP se puede encontrar que las medidas de responsabilidad activa de los responsables y encargados del tratamiento de la información son bien específicas. Además de las obligaciones generales del responsable y encargado del tratamiento, se detallan: a) los supuestos de corresponsabilidad en el tratamiento; b) los representantes de los responsables o encargados del tratamiento no establecidos en la UE; c) registro de actividades de tratamiento; y, d) bloqueo de datos.

Aunado a esto, se establece una diferenciación que permite conocer cuándo se considera que una entidad es responsable o encargado del tratamiento, facilitando el proceso de determinación de responsabilidades en función de las competencias y funciones que se le

atribuye a cada uno; asimismo, se plantean escenarios en los cuales se indican cuando se considera responsable y no encargado.

Sumado a lo anterior, se incorpora la figura del delegado de protección de datos, el cual debe ser designado por el responsable del tratamiento o encargado, cuando se traten de entidades que por las funciones que desempeña, amerita de una especial protección, enlistados en el artículo 34 de la Ley Orgánica 3/2018, lo cual permite brindar especial salvaguarda. En este sentido, se expresa de forma concreta las competencias, funciones y obligaciones del delegado de protección de datos.

Por otra parte, se dedica un título entero para establecer el régimen de este tipo de transferencias, específicamente, el Título V, De las transferencias internacionales de datos, en el cual se exponen las normas que deben seguirse para poder efectuar estas operaciones. De igual modo, el Título VII, De las autoridades de protección de datos enmarca una serie de artículos que dispone cuáles son las autoridades responsables de ejercer la protección de datos, así como las funciones que se le atañen y las normas a las que debe adherirse de forma clara y taxativa.

Si bien, en la Ley 1581 de 2012 se consagran los procedimientos y sanciones, es imperioso que adopte el ejemplo de la LO 3/2018 y el RGDP, que expone de forma detallada cuáles son los procedimientos en caso de posible vulneración de la normativa de protección de datos, en siete (7) artículos que conforman el Título VIII de la LOPDGDD. Asimismo, se puede observar que en esta última ley el régimen sancionador está englobado en un título aparte, en el cual se indican de forma inequívoca quienes son los sujetos responsables, cuáles son las infracciones y sus tipos, lo cual permite que se aplique la norma penal y procesal penal vigente adecuadamente, sin dar lugar a vacíos legales.

Estas son solo algunas de las posibles incorporaciones que puede realizar Colombia en su ordenamiento jurídico para mejorar el sistema legal de protección de datos en el ámbito nacional. Sin embargo, es importante tener en cuenta que España es un Estado miembro de la Unión Europea, en donde se aplica el principio de cooperación y coordinación entre todos los Estados miembros, lo cual ha posibilitado que la lucha contra la cibercriminalidad sea efectiva.

Es un escenario totalmente distinto al caso de Colombia que de manera aislada ha hecho un gran esfuerzo en tratar de regular los delitos informáticos y de sancionar normas jurídicas orientadas a proteger los derechos fundamentales vinculados a la dignidad humana, como por ejemplo el derecho a la protección de datos personales, la intimidad y al buen nombre.

Colombia no cuenta con la cooperación y coordinación de los Estados que se encuentran en la región y tampoco cuenta con el respaldo de una organización multinivel que se encargue de llevar la batuta en el combate contra los delitos informáticos para proteger adecuadamente los derechos asociados a la dignidad humana y emita las líneas generales que han de seguirse para sumar esfuerzos y remar juntos en una sola dirección.

4. Conclusiones

El concepto de dignidad más implementado tiene una cualidad simplemente instrumental, a partir de la cual se asocia esta idea al trato o respeto adecuado a los individuos, únicamente, por su esencia de seres humanos. Si bien, no permite justificar por qué se le otorga un determinado trato a una persona o no, en el contexto del derecho ha permitido generar normas jurídicas que protejan la dignidad humana y los derechos que la conforman.

De acuerdo al criterio de la Corte Constitucional de Colombia, la dignidad es un atributo que le es inherente al ser humano, el cual se deriva de las características de las personas. Sin embargo, con el desarrollo de la tecnología y la instauración de la nueva era digital, la dignidad humana se ha visto transgredida en más de una oportunidad y en distintos escenarios, producto del uso casi irrestricto de las TIC.

El desarrollo de las nuevas tecnologías de la información y la comunicación es un hecho imparable que, si bien ha traído múltiples beneficios para la humanidad, en la actualidad, resulta indispensable adecuar el marco legal colombiano existente en materia de protección de datos personales, para lograr tener una contienda justa con la cibercriminalidad.

La Unión Europea ha incursionado en el estudio de la protección de datos personales desde finales del siglo XX, por lo que de manera constante se encuentra mejorando sus instrumentos jurídicos para poder garantizar los derechos fundamentales de los europeos. Asimismo, se puede ver que la UE ha realizado importantes avances en la armonización de los ordenamientos jurídicos de los Estados miembros en materia de derecho penal, derecho procesal penal y salvaguarda de los datos de índole personal; lo cual, a su vez, le ha proporcionado una ventaja importante en la lucha contra la ciberdelincuencia.

Ahora bien, aun cuando Colombia no goza de esos beneficios que tienen los Estados miembros de la UE, pues no cuenta con el respaldo de una organización multinivel en la región, de forma aislada ha logrado hacer algunos avances importantes, como lo es la adopción del Convenio de Budapest a la legislación colombiana.

Es evidente que, con el acelerado desarrollo de las nuevas TIC, Colombia se ha quedado un paso atrás en materia legislativa, pues sus normas no están a la par de la realidad tecnológica y digital; por ende, es importante que el Poder Legislativo colombiano haga una

revisión exhaustiva del marco legal en materia de protección de datos personales y ciberseguridad, con la finalidad de actualizarlo y adecuarlo a la situación actual.

Los instrumentos jurídicos emanados de la Unión Europea pueden servir de inspiración para que el legislador colombiano tome algunos elementos potencialmente incorporables al ordenamiento legal que regula la materia para fortalecer y mejorar las normas internas, con el propósito de garantizar la protección de la dignidad humana, así como otros derechos fundamentales de las personas en Colombia.

En este sentido, es acertado afirmar que si se incorporan algunos elementos del marco legal español a la legislación colombiana es posible mejorar el sistema legal de protección de datos y, a su vez, propiciar la disminución de los delitos informáticos contra la dignidad humana.

Referencias

Acosta, J. M. (2021). *Delitos informáticos crecieron 17% en Colombia en comparación del 2020*. Obtenido de Radio Caracol: https://bit.ly/3bklOVH

Acosta, M., Benavides, M., & García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, vol. 25, núm. 89.

Acosta-Argote, C. (2021). *Ciberdelitos subieron 37% durante el primer trimestre de 2020, en los peores meses de la crisis*. Obtenido de Asuntos Legales: https://bit.ly/3cREM6I

Agencia Española de Protección de Datos. (2005). *Guía del derecho fundamental a la protección de datos de carácter personal.* España: Agencia Española de Protección de Datos.

Aguilar, M. (2018). La ley de protección de datos en Colombia: sus inicios y examen de sus principales postulados. *Centro de Investigaciones Socio Jurídicas*, 1-56.

Alarcón, D., & Barrera, J. (2017). *Uso de Internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016.* [Tesis para optar al grado académico de Maestro en Informática Educativa. Universidad Privada Norbert Wiener].

Alarcón, M., & Blanco, J. (2021). Libertad de expresión vs. Derecho al honor: un conflicto interminable. *Temas de Comunicación*, 7-22. ISSN: 0798-7803.

Aldana, J., & Iséa, J. (2018). Derechos Humanos y Dignidad Humana. *Iustitia Socialis. Revista Arbitrada de iencias Jurídicas, III*(4), 8-23.

Ales-Uría, M. (2019). La dignidad humana y el derecho de disposición sobre el propio cuerpo. Reflexiones a partir del rechazo de tratamientos médicos y los acuerdos de maternidad subrogada. *Dikaion, 29*(1), 39-65.

Anguita, J. (2018). Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea. *Revista de Estudios en Seguridad Internacional*, 4(1), pp. 107-126. DOI: http://dx.doi.org/10.18847/1.7.7.

Arias, M., Daza, L., Ojeda, J., & Rincón-Rodríguez, F. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Universidad Santo Tomás de Aquino*, 11(28), pp. 41-66.

Ariza, J., Ayala, J., & González, L. (2020). La protección de datos en la era digital Colombia - España. *Institución Universitaria Politécnico Grancolombiano*, 1-19.

Ballén, J., Cortés, R., & Duque, J. (2015). La persecución judicial contra los delitos informáticos en el distrito judicial de Villavicencio. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, (14), pp. 4-26. ISSN 1909-7786.

Bechara, Y., Mosquera, A., & Ledezma, E. (2020). *Análisis jurídico de la Ley 1273 del 2009 y el surgimiento y expansión del delito de hurto y semejantes por medios informáticos.* Quibdó: Universidad Cooperativa de Colombia.

Bohórquez, V., & Aguirre, J. (2009). Las tensiones de la dignidad humana: conceptualización y aplicación en el derecho internacional de los derechos humanos. *SUR. Revista Internacional de Derechos Humanos*, 6(11), pp. 41-63.

Bolañoz, A., & Narváez, T. (2014). *Análisis comparativo sobre delitos informáticos en Colombia con relación a seis países en Latinoamérica.* San Juan de Pasto: Universidad Nacional Abierta y a Distancia.

Bonilla, P. (2019). El espectro actual de los delitos informáticos. *Revista Judicial, Poder Judicial de Costa Rica*, 126. 220-225. ISSN 2215-2385.

Candelario, J., & Rodríguez, M. (2015). Seguridad Informática en el Siglo XXI: Una perspectiva jurídica tecnológica enfocada hacia las organizaciones nacionales y mundiales. *Revista Especializada en Ingeniería*, 9. pp. 153-163. ISSN: 1900-6608.

Cano, A., Díaz, J., Mendieta, C., Rivas, C., & Sánchez, N. (2014). *Aporte Internacional frente a los delitos informáticos en Colombia y su ejecución por parte de las autoridades competentes.* Bogotá: Universidad Libre de Colombia.

Castillo, J. (2018). *El delito informático y su implicación en el patrimonio económico en Colombia.* Bogotá, D. C.: Universidad Militar Nueva Granada.

Chávez, E. (2018). *El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Lima Norte, 2017.* [Tesis para optar el grado académico de doctor en derecho, Universidad Nacional Federico Villarreal].

Chiluisa, D. (2021). *Los delitos informáticos y los vacíos legales que afectan a los ciudadanos.* Guayaquil: [Trabajo de titulación previo a la obtención del título de Abogado de los tribunales y juzgados de la República del Ecuador, Universidad Católica de Santiago de Guayaquil].

CISCO. (2020). Obtenido de https://bit.ly/3S3s7h7

Comisión Económica para América Latina y el Caribe. (2015). *Gobernanza Global y Desarrollo. Nuevos desafíos y prioridades de la cooperación internacional.* Grupo editorial Siglo XXI.

Comisión Europea. (2016). Obtenido de https://bit.ly/2xpg3yU

De Léon, H. (2020). La dignidad humana en la era digital. *Anuario de Derecho Constitucional Latinoamericano*, pp. 671-695. ISSN 2346-0849.

De-León-Batista, H. (2020). La dignidad humana en la era digital. *Anauario de Desrecho Contitucional Latinoamericano, XXVI*, 671-695.

Díaz, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *REDUR 8*, pp. 169-203. ISSN 1695-078X .

Domínguez, M. (2003). Las tecnologías de la información y la comunicación: sus opciones, sus limitaciones y sus defectos en la enseñanza. *Nómadas. Critical Journal of Social and Juridical Sciences*, (8), pp. 1-68. ISSN: 1578-6730.

Domínguez, M. (2019). La dignidad: principio y soporte de la persona humana. *Revista Tachirense de Derecho*, (5), pp. 77-104. ISSN: 1316-6883.

Duacuara, A., & Soto, C. (2018). *Protección de datos personales en los servicios de internet.* Bogotá: [Trabajo de grado para obtener el título de especialista en seguridad de la información, Universidad Católica de Colombia].

Enciclopedia Jurídica. (2020). Obtenido de https://bit.ly/3bkkJgB

Evaluando Cloud.com. (2016). *Amenazas de Seguridad*. Obtenido de https://bit.ly/3PHNEKs

Faggiani, V. (2015). *La justicia penal en la Unión Europea. Hacia la armonización de los derechos procesales.* [Tesis doctoral en Ciencias Jurídicas, Derecho Constitucional Europeo. Universidad de Granada].

Fuquene, E. (2019). Rol de la legislación colombiana en la evolución de la seguridad informática y de la información. *Universidad Piloto de Colombia*, 1-6.

Gallardo, L. (2020). *La dignidad humana, una aproximación al concepto en el siglo XXI.* Chiapas: [Trabajo de grado para obtener el título de Maestro en Ciencias Sociales y Humanísticas, Universidad de Ciencias y Artes de Chiapas].

Gil, M. (2015). *La violencia sexual como un atentado contra la dignidad de la mujer.* Madrid: [Tesis doctoral, Universidad Nacional de Educación a Distancia].

Gómez-Córdoba, A., Arévalo-Leal, S., Bernal-Carmargo, D., & Rosero de los Ríos, D. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por Covid-19 en Colombia. *Revista de Bioética y Derecho*, 50: 271-294.

González, J. (2016). La dignidad humana. *ACADEMO Revista de Investigación en Ciencias Sociales y Humanidades*, 3(2), pp. 1-15.

Guarnizo, M. (2020). *La naturaleza jurídica de los delitos informáticos en Colombia.* Ibagué: Universidad Nacional Abierta y a Distancia.

Guerra, M., & Oviedo, J. (2011). *De las telecomunicaciones a las TIC: Ley de TIC de Colombia (L1341/09).* Bogotá: CEPAL.

Guerrero, L. (2007). Seguridad pública y prevención del delito en el Estado social de derecho. Especial comentario a la trascendencia de la educación. *Universidad de la Sabana*, 16. 251-272. ISSN 0120-8942.

Habermas, J. (2010). La idea de la dignidad humana y la utopía realista de los derechos humanos. *Anales de la Cátedra Francisco Suárez*, 44, 105-121.

Habermas, J. (20103-25). El concepto de la dignidad human y la utopia realista de los derechos humanos. *Diánoia, 55*(64).

Hernández, R., Fernandez, C., & Baptista, P. (2006). *Metodología de la investigación (cuarta ed).*

Hidalgo, J. (2018). *Los delitos informáticos y su afectación sobre los bienes jurídicos.* 2018: [Trabajo de Titulación previo a la obtención del título de abogado de los Tribunales y Juzgados de la República, Universidad Católica de Santiago de Guayaquil].

Jimena, L. (2020). El derecho a la protección contra la pobreza y la exclusión social como paradigma del respeto de la dignidad humana. la inserción del ingreso mínimo vital en el marco de la evolución de los estándares internacionales. *Lex Social, 10*(2), 361-423.

Kant, I. (1996). *Fundamentación metafísica de las costumbres.* México: Porrúa.

Legislación Informática de Colombia. (2022). *Informática Jurícia*. Obtenido de https://bit.ly/3OGvVBV

Ley Estatutaria 1266, Diario Oficial 47.219 (Congreso de la República 31 de 12 de 2008).

Manjarrés, I., & Jiménez, F. (2012). Caracterización de los delitos informáticos en Colombia. *Pensamiento Americano*, 71-82.

Martínez, N. (2019). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Ars Iuris Salmanticensis*, 7(1), pp. 254-259. ISSN: 2340-5155. .

Martínez, V. (2013). Reflexiones sobre la dignidad humana en la actualidad. *Boletín Mexicano de Derecho Comparado*, XLVI(136), pp. 39-67.

Martínez, W. (2017). *Estudio de adhesión de Colombia al Convenio de Budapest, visto desde la legislación y seguridad informática.* Bogotá: [Monografía para optar al título de Especialista en Seguridad Informática, Universidad Nacional Abierta y a Distancia].

Mata, R. (2003). *Delicuencia informática y derecho penal.* Managua: Hispamer.

Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista chilena de derecho*, 44(1), pp. 235-260. http://dx.doi.org/10.4067/S0718-34372017000100011 .

Meléndez, F. (2012). *Instrumentos Internacionales sobre Derechos Humanos Aplicables a la Administración de Justicia.* 8va. ed. Universidad del Rosario. ISBN 978-958-738-287-7.

Mendieta, D., & Tobón, M. (2018). La dignidad humana y el Estado Social y Democrático de Derecho: el caso colombiano. *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD)*, 10(3), pp. 278-289. doi: 10.4013/rechtd.2018.103.05.

Mercader, J. (2022). Nuevas señales y paradojas de la protección de datos en la reciente doctrina de los Tribunales y de la Agencia Española de Protección de Datos. *Trabajo y Derecho*, 85, pp. 1-24.

Mesa, L., Ramírez, A., & Ramírez, N. (2020). Los derechos fundamentales de las víctimas de los ciberdelitos en Colombia. *Politécnico Gran Colombiano*, pp. 1-19. https://bit.ly/3PKE0qG.

Michelini, D. (2010). Dignidad human en Kant y Habermas. *Estudios de Filosofía Práctica e Historia de la Ideas, 12*(1), 41-49.

Molina, A., & Lamas, G. (2018). La dignidad humana: propuestas de protección. *Revista Jurídica Piélagus*, 17(02), pp. 11-18. DOI: http://dx.doi.org/10.25054/16576799.1825.

Montero, J. (2005). *La dignidad humana en la jurisprudencia constitucional colombiana: un estudio sobre su evolución conceptual.* [Trabajo de grado, Universidad Católica de Colombia].

Mosquera, K. (2020). *Adaptación normativa frente a los delitos informáticos en Colombia.* Santiago de Cali: Universidad Santiago de Cali.

Muñoz, H., Zapata, L., Requena, D., & Ricardo, L. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Revista Venezolana de Gerencia*, 2. 528-541.

Negrillo, A. (2021). *Algunas cuestiones controvertidas en torno al derecho a la protección de datos en el comercio electrónico.* [Trabajo de fin de grado para optar al título en Derecho. Universidad de Jaén].

Nogueira, H. (2007). Derecho a la propia imagen como derecho fundamental implícito. Fundamentación y Caracterización. *Revista Ius Et Praxis*, 242-285.

Oficina de la Naciones Unidas contra la Droga y el Delito. (2011). *Manual sobre la aplicación eficaz de la directrices para la prevención del delito.* Nueva York: ONU.

ONU. (1948). *Declaración de los Derecho Humanos.* París: Organización de las Naciones Unidas.

Osorio, C. (2018). *La ciberseguridad en el ámbito de la seguridad colombiana, ¿avance o retroceso?* Bogotá: Universidad Militar Nueva Granada.

Peces-Barba, G. (2005). Reflexiones sobre la evolución histórica. *Dykinson*, 15-36. DOI: 10.1400/194795.

Pelé, A. (2010). *La dignidad humana. Sus orígenes en el pensamiento clásico.* Dykinson.

Pereira, X. (2015). Seguridad informática en Colombia un largo camino. *Universidad Piloto de Colombia*, 1-6.

Polo-Roca, A. (2020). Sociedad de la Información, Sociedad Digital, Sociedad de Control. *INGURUAK, Revista Vasca de Sociología y Ciencia Política, 68*, 50-77.

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, 20, pp. 80-93. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2563.

Posada Maya, R. (2017). *Los cibercrímenes: un nuevo paradigma de criminalidad. Un estudio del título VII bis del Código Penal colombiano.* Bogotá, D.C.: Grupo Editorial Ibañez.

Posso, D. (2014). *Los delitos informáticos y la violación de los derechos constitucionales del ofendido.* Ambato: [Trabajo de Graduación, como requisito previo a la obtención del Título de Abogado de los Juzgados y Tribunales de la República del Ecuador, Universidad Técnica de Ambato].

Rallo, A. (2019). El nuevo derecho de protección de datos. *Revista Española de Derecho Constitucional*, 116, pp. 45-74. doi: https://doi.org/10.18042/cepc/redc.116.02.

Ramada, Y. (2018). *Ciberbullying: análisis de los principales Derechos Fundamentales Implicados y responsabilidades jurídicas derivadas de la conducta.* Zaragoza: Universidad de Zaragoza.

REA. (2020). *Real Academia Española*. Obtenido de https://bit.ly/3QkDnnJ

Restrepo, A. (2011). Acercamiento conceptual a la dignidad humana y su uso en la Corte Constitucional colombiana. *Diálogos de Derecho y Política*, (6), pp. 3-19. ISSN 1234567.

Rodríguez, J. (2018). *La evidencia digital como medio de prueba en los delitos informáticos.* [Monografía jurídica, Pontificia Universidad Javeriana de Colombia].

Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *NOVUM JUS*, 8(1), pp. 107-139. ISSN: 1692-6013.

Rueda, D. (2012). *Regulaciones nacionales e internacionales en materia de protección de datos personales. Retos globales en la actual era digital.* Bogotá: [Trabajo de grado para obtener el título de abogado, Universidad de los Andes].

Ruiz, C. (2016). *Análisis de los delitos informáticos y su violación de los derechos fundamentales constitucionales de los ciudadanos.* Loja: [Trabajo final de grado para obtener el título de abogada, Universidad Nacional de Loja].

Ruiz, S. (2017). *Protección de Datos y Seguridad Digital en Colombia Una propuesta sobre la necesidad de adhesión al Convenio de Budapest (2001).* Bogotá: [Trabajo de grado para optar al título de abogado, Universidad de los Andes].

Sain, G. (2018). La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal. En R. Parada, *Cibercrimen y delitos informáticos* (págs. pp. 7-32). Buenos Aires: Erreius. ISBN 978-987-4405-56-2.

Sánchez, D. (2016). *Análisis del delito de violación de datos personales (artículo 269f del Código Penal), desde una perspectiva constitucional.* [Trabajo de Tesis Académica para optar por el título de abogado, Universidad Libre de Colombia].

Serrano, E. (2014). *La práctica de delitos informáticos en Colombia.* Bogotá: Universidad Militar Nueva Granada.

Trillo, C. (2019). *Compliance Laboral en Materia de Protección de Datos Personales.* [Trabajo de investigación para optar al grado académico de magíster en derecho de la empresa. Pontificia Universidad Católica del Perú].

Trincado, C. (2021). El acceso ilícito a datos de historias clínicas informatizadas: análisis de la jurisprudencia penal desde la perspectiva de la ciberseguridad. *Derecho y Genoma Humano*, (55), pp. 159-188. DOI: 10.14679/1271.

Vargas-Téllez, G. (2021). Aproximación teórica a la prevención del delito y la seguridad pública. *Revista Ciencia Jurídica y Política*, 7(13). 83-93. ISSN 2708-9266.