Medidas para reducir y prevenir el delito de violación de datos personales: Estudio comparado entre Colombia y el Reglamente General de Protección de Datos (GDPR) de la Unión Europea en el período 2020 al 2023.

Autor:

Lady Sofia Mendez Velandia

Universidad Colegio Mayor de Cundinamarca

Programa Maestría en Derecho Penal

2024

Bogotá 2024

Medidas para reducir y prevenir el delito de violación de datos personales: Estudio comparado entre Colombia y el Reglamente General de Protección de Datos (GDPR) de la Unión Europea en el período 2020 al 2023.

Lady Sofia Mendez Velandia

Trabajo de Grado presentado como requisito para optar al título de Maestría en Derecho Penal

Asesor temático: Pablo Elías González Monguí
Asesor Metodológico: Miriam Sepúlveda López

Línea de investigación: Estado sociedad y Cultura

Universidad Colegio Mayor de Cundinamarca
Programa Maestría en Derecho Penal
2024

Dedicatoria

Deseo dedicar este proyecto de investigación a mi madre, quien ocupa un lugar fundamental en mi vida. Su constante apoyo y amor incondicional son mi mayor motivación para superar obstáculos y seguir adelante, enfrentando los desafíos que la vida presenta día a día. Esta tesis es un homenaje a ti, a tu lucha y a tu resiliencia. Espero que, con cada palabra escrita, sientas mi gratitud y mi profundo amor. Eres la razón por la que he perseguido mis sueños, y no hay mayor recompensa que dedicarte este logro. Te amo, hoy y siempre.

Agradecimientos

Quiero comenzar expresando mi agradecimiento a Dios por darme la oportunidad de estudiar y por haberme dado la fuerza interior necesaria para enfrentar todos los desafíos que encontré a lo largo de mi camino académico. Agradezco profundamente el apoyo moral e incondicional de cada uno de mis familiares, cuya presencia ha sido fundamental en mi crecimiento personal y académico. También quiero reconocer a la Universidad Colegio Mayor de Cundinamarca por ser una institución de gran renombre a nivel nacional, que me ha brindado las herramientas y el conocimiento necesario para mi formación profesional.

Resumen

La presente tesis académica, en el ámbito del Derecho penal, aborda directamente como objetivo principal analizar y proponer medidas para fortalecer la protección de datos personales en Colombia, con especial atención en la prevención y reducción del delito establecido en el artículo 269F del Código Penal, que aborda la violación de datos personales.

Para ello en primer lugar, se llevará a cabo una caracterización dogmática penal del delito mencionado, explorando sus elementos y alcances dentro del marco jurídico colombiano. Posteriormente, se realizará un estudio normativo de la Ley Estatutaria 1581 de 2012, identificando sus limitaciones e insuficiencias en cuanto a la protección de datos personales.

En tercer lugar, se realizará un análisis comparativo entre la legislación colombiana sobre protección de datos y el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Esto permitirá identificar similitudes, ventajas y diferencias, proporcionando un contexto internacional relevante para las recomendaciones formuladas.

Finalmente, se formularán estrategias socio jurídicas para fortalecer la legislación y las regulaciones vigentes en Colombia, así como para mejorar los procesos de investigación judicial en la lucha contra la violación de datos personales. Estas recomendaciones se basarán en los hallazgos de la investigación y el análisis comparativo, con el objetivo de cerrar las brechas identificadas y promover una protección más efectiva de los datos personales en el país.

Palabras claves: Violación de datos personales, articulo 269F, Ley Estatutaria 1581 de 2012, Reglamento General de Protección de Datos personales de la Unión Europea.

Abstract

The main objective of this academic thesis, in the field of Law, is to directly analyze and propose measures to strengthen the protection of personal data in Colombia, with special attention to the prevention and reduction of crime established in article 269F of the Penal Code, which addresses the breach of personal data.

To do this, first of all, a dogmatic criminal characterization of the aforementioned crime will be carried out, exploring its elements and scope within the Colombian legal framework. Subsequently, a regulatory study of Statutory Law 1581 of 2012 will be carried out, identifying its limitations and insufficiencies regarding the protection of personal data.

Thirdly, a comparative analysis will be carried out between Colombian legislation on data protection and the regulations of other countries, including the General Data Protection Regulation (GDPR) of the European Union. This will allow similarities, advantages and differences to be identified, providing a relevant international context for the recommendations made.

Finally, specific recommendations will be made to strengthen the legislation and regulations in force in Colombia, as well as to improve judicial investigation processes in the fight against personal data breaches. These recommendations will be based on research findings and comparative analysis, with the aim of closing identified gaps and promoting more effective protection of personal data in the country.

Keywords: Violation of personal data, article 269F, Statutory Law 1581 of 2012, General Data Protection Regulation of the European Union

Tabla de Contenido

Listas Especiales

Introducción

En la era digital actual, el uso masivo de internet ha dado lugar a un incremento significativo en la generación, recopilación y almacenamiento de datos personales. Estos datos, que incluyen información sensible y privada de los usuarios, son cada vez más objeto de interés para los delincuentes informáticos que buscan obtener ganancias ilícitas a través del hurto de datos personales.

La violación de datos personales se ha convertido en un delito informático de gran relevancia, con consecuencias perjudiciales para los usuarios de internet, tanto a nivel individual como a nivel colectivo. Las implicaciones pueden variar desde el robo de identidad hasta el acceso no autorizado a cuentas bancarias y la violación de la privacidad personal.

Ante esta problemática, los gobiernos de diferentes países han implementado leyes y regulaciones para proteger los datos personales de los usuarios en el ámbito digital. Sin embargo, la efectividad y las estrategias utilizadas en la protección de datos pueden variar de un país a otro, dependiendo de su marco legal, recursos disponibles y enfoque adoptado.

En Colombia, el 5 de enero de 2009, el Congreso de la República promulgó la Ley 1273, que modifica el Código Penal y establece un nuevo bien jurídico protegido denominado "De la Protección de la información y de los datos", además de preservar integralmente los sistemas que utilizan tecnologías de la información y las comunicaciones, entre otras disposiciones. En esta nueva disposición, se encuentra consagrado el tipo penal que analizamos de manera integral en esta tesis de grado, el cual se denomina Violación de Datos Personales (Artículo 269F del Código Penal).

De otro lado, el tema de datos personales se encuentra respaldada por un marco legal encabezado por la Ley Estatutaria 1581 de 2012. Esta ley establece los principios, derechos y procedimientos que garantizan la adecuada protección de la información personal de los ciudadanos colombianos.

Uno de los aspectos clave de la Ley 1581 es su enfoque en el consentimiento informado. Esto significa que las organizaciones deben obtener el consentimiento expreso de los individuos antes de recopilar, procesar o transferir sus datos personales. Además, la ley establece la obligación de las empresas y entidades gubernamentales de implementar medidas de seguridad adecuadas para proteger la confidencialidad, integridad y disponibilidad de los datos.

Además de la Ley Estatutaria 1581, existen otras normativas complementarias que refuerzan la protección de datos en Colombia. Por ejemplo, el Decreto 1377 de 2013 regula aspectos específicos relacionados con el registro de bases de datos y la atención de consultas

y reclamos por parte de los titulares de los datos. Asimismo, la Superintendencia de Industria y Comercio (SIC) es la entidad encargada de vigilar el cumplimiento de estas normativas y de imponer sanciones en caso de infracciones.

Con el fin de alcanzar este propósito, la investigación se organiza alrededor de tres pilares fundamentales. En un primer momento se identifica la caracterización dogmática penal del delito de violación de datos personales según lo establecido en el artículo 269F del Código Penal. Este análisis permitirá comprender en detalle la naturaleza y las implicaciones jurídicas de esta infracción.

Como segundo pilar realizará un estudio normativo para identificar las limitaciones e insuficiencias de la Ley Estatutaria 1581 de 2012, la cual establece disposiciones generales para la protección de datos personales en Colombia. Este enfoque crítico será fundamental para identificar áreas de mejora en la legislación existente y proponer recomendaciones específicas para su fortalecimiento.

En tercer momento se llevará a cabo un análisis comparativo de la legislación colombiana sobre protección de datos personales, representada por la Ley Estatutaria 1581 de 2012, con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Este ejercicio permitirá identificar similitudes, ventajas y diferencias entre diferentes enfoques legales, con el objetivo de extraer lecciones y buenas prácticas que puedan ser aplicables en el contexto colombiano.

Por último, se formularán estrategias socio jurídicas para fortalecer la legislación y las regulaciones vigentes en Colombia, así como las estrategias de investigación judicial, con el fin de combatir de manera efectiva el delito de violación de datos personales y proteger los derechos fundamentales de los ciudadanos en un mundo digitalizado.

En términos de metodología, este estudio adopta un enfoque teórico con un énfasis cualitativo, caracterizado por su naturaleza descriptiva y explicativa. Se emplea un método inductivo que facilita el análisis de medidas destinadas a fortalecer y prevenir el delito de violación de datos personales establecido en el artículo 269F del Código Penal colombiano.

1. Ubicación del problema

1.1. Descripción del problema

En la actualidad, la rápida evolución tecnológica y el crecimiento exponencial de la información digital han generado una preocupante vulnerabilidad frente a los delitos informáticos, en particular en lo concerniente a la violación de datos personales. Este fenómeno se ve alimentado por la ubicuidad de internet y la amplia adopción de dispositivos conectados, que han convertido los datos personales en un recurso de gran valor y, al mismo tiempo, en un blanco deseado por delincuentes.

El delito de violación de datos personales, tipificado en el artículo 269F del Código Penal colombiano, es una manifestación directa de esta problemática, y su incidencia ha ido en aumento en los últimos años. Los perpetradores de estos actos utilizan diversas técnicas, como la intrusión en sistemas informáticos y la ingeniería social, para acceder ilegalmente a información sensible y privada.

Este panorama presenta importantes desafíos tanto a nivel individual como colectivo. A nivel personal, el robo y la explotación de datos pueden acarrear graves consecuencias, desde la pérdida de privacidad y la exposición a la manipulación hasta el fraude financiero y la extorsión. Además, mina la confianza en la seguridad de los sistemas y servicios digitales, alterando la manera en que las personas interactúan y participan en la sociedad en línea.

A nivel colectivo, la violación de datos personales socava la confianza en las instituciones responsables de proteger la información personal, lo que puede tener repercusiones en la economía y la estabilidad social. La divulgación masiva de datos personales puede generar un clima de incertidumbre y desconfianza entre los ciudadanos, dificultando el desarrollo de una sociedad digital segura y confiable.

Además, la legislación colombiana en materia de protección de datos, representada por la Ley Estatutaria 1581 de 2012, puede presentar limitaciones e insuficiencias que dificultan la protección adecuada de la información personal de los ciudadanos frente a este tipo de delitos. Es esencial realizar un análisis exhaustivo de esta legislación para identificar áreas de mejora y proponer medidas concretas que fortalezcan su efectividad en la prevención y persecución de la violación de datos personales.

En este contexto globalizado, resulta crucial comparar la legislación colombiana con las normativas internacionales relevantes, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, con el fin de identificar similitudes, diferencias y buenas prácticas que puedan enriquecer el marco legal colombiano en materia de protección de datos.

Ante esta situación, se plantea la necesidad de desarrollar la siguiente investigación que aborda la problemática de la violación de datos personales, con el fin de fortalecer la legislación y las estrategias de prevención y persecución de estos delitos, garantizando así la protección de los derechos fundamentales de los ciudadanos en el entorno digital actual.

1.2. Formulación del problema

¿Cuáles son las medidas que pueden ser adoptadas para reducir y prevenir el delito de violación de datos personales, mediante un estudio comparado entre Colombia y el Reglamente General de Protección de Datos (GDPR) de la Unión Europea en el período 2020 al 2023?

1.3. Justificación

En la actualidad, la expansión de las tecnologías de la información y comunicación (TIC) ha transformado radicalmente la forma en que interactuamos, trabajamos y nos relacionamos en la sociedad. El uso generalizado de internet y el constante flujo de información digital han generado un entorno donde los datos personales se han convertido en uno de los activos más valiosos y, a la vez, más vulnerables. Este fenómeno ha sido acompañado por un aumento significativo en la generación, recopilación y almacenamiento de datos personales, abarcando desde información básica como nombres y direcciones hasta datos más sensibles como historiales médicos o información financiera.

Sin embargo, esta proliferación de datos no ha pasado desapercibida para individuos malintencionados que buscan obtener beneficios ilícitos a través del robo y la explotación de esta información. Los delincuentes informáticos, aprovechando las brechas de seguridad y las vulnerabilidades en sistemas informáticos, llevan a cabo actividades fraudulentas como el robo de identidad, el fraude financiero o la extorsión, entre otros. El delito de violación de datos personales, contemplado en el artículo 269F del Código Penal colombiano, es una manifestación clara de esta problemática.

La pertinencia de este tema radica en las consecuencias perjudiciales que tiene para los individuos y la sociedad en su conjunto. A nivel individual, el robo de datos personales puede resultar en la pérdida de privacidad, la exposición a la manipulación o el chantaje, e incluso en la pérdida de activos financieros. A nivel colectivo, estas prácticas minan la confianza en el uso de tecnologías digitales y en las instituciones responsables de proteger la información personal, lo que puede afectar la economía y la estabilidad social.

Ante este panorama, es fundamental abordar esta problemática de manera integral y proactiva, es por esto por lo que, la investigación propuesta busca contribuir a este objetivo mediante el análisis detallado de la caracterización dogmática penal del delito de violación de

datos personales, así como de las limitaciones e insuficiencias de la legislación colombiana en materia de protección de datos. Además, se pretende realizar un análisis comparativo con legislaciones internacionales relevantes, con el fin de identificar buenas prácticas y lecciones aprendidas que puedan ser aplicables en el contexto colombiano.

A través de este estudio, se espera formular recomendaciones concretas para fortalecer la legislación y las estrategias de investigación judicial, con el propósito de combatir de manera efectiva el delito de violación de datos personales y promover un entorno digital más seguro y confiable para todos los ciudadanos.

1.4. Objetivos

1.4.1 Objetivo General

Analizar las medidas que deben ser adoptadas para reducir y prevenir el delito de violación de datos personales, mediante un estudio comparado entre Colombia y el Reglamente General de Protección de Datos (GDPR) de la Unión Europea en el período 2020 al 2023.

1.4.2 Objetivos específicos:

- Caracterizar el bien jurídico tutelado del delito de violación de datos personales y su juicio de antijuricidad.

- Describir la dogmática penal del delito de violación de datos personales, establecido en el artículo 269F del Código Penal.

- Establecer un análisis comparativo de la legislación colombiana sobre la protección de datos personales, Ley Estatutaria 1581 de 2012, con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, con el fin de identificar similitudes, y diferencias.

- Proponer alternativas de intervención socio jurídicas, para fortalecer la legislación o las regulaciones vigentes en Colombia en la protección de datos personales.

2. Marco teórico conceptual:

En 2009, Colombia promulgó la Ley 1273, la cual marcó un hito en la regulación de delitos informáticos al reconocer la información como un bien jurídico protegido. Antes de la existencia de esta ley, no había una normativa específica para sancionar los delitos relacionados con el uso indebido de la tecnología y la información. Con la entrada en vigor de la Ley de Delitos Informáticos, la información se convirtió en un bien jurídico, lo que implica que, al igual que otros bienes, puede ser vulnerada y objeto de delitos penales (Ley 1273, 2009). Este reconocimiento permitió equiparar la protección de la información a la de otros derechos consagrados en el Código Penal colombiano, y desde entonces ha sido fundamental para el desarrollo de la ciberseguridad en el país (Camacho & Salvedo, 2022).

El concepto de la información como bien jurídico se sustenta en tres pilares fundamentales que configuran los delitos informáticos: confidencialidad, integridad y disponibilidad de la información. Estos pilares, conocidos como la Triada CID, constituyen la base de la seguridad de la información y son esenciales para analizar y clasificar cualquier situación relacionada con la protección de datos. Una violación a cualquiera de estos pilares implica la configuración de un delito informático (Rueda, 2020).

El primer pilar, la confidencialidad, se refiere a la protección de la información, garantizando que solo personas autorizadas puedan acceder a ella. Esto es particularmente relevante en el manejo de datos sensibles o confidenciales, como los relacionados con las autoridades o documentos clasificados. La vulneración de la confidencialidad puede llevar a la comisión de varios delitos informáticos, ya que expone información a personas no autorizadas (Salvatori, 2011). Por su parte, la integridad, como segundo pilar, asegura que la información no sea alterada sin autorización, manteniendo su exactitud y completitud.

En términos de seguridad, es crucial que los datos sean confiables y no manipulados por terceros, ya que cualquier alteración no autorizada de los mismos puede constituir un delito (Acurio, 2016). Finalmente, el tercer pilar, la disponibilidad, se refiere a la capacidad de los sistemas de información para estar accesibles cuando los usuarios autorizados lo necesiten. La falta de disponibilidad, como ocurre en los ataques de denegación de servicio, puede paralizar el acceso a la información y generar daños significativos tanto a usuarios como a organizaciones (Camacho & Salvedo, 2022; Dávila, 2020).

La Triada CID no solo ayuda a comprender la naturaleza de los delitos informáticos, sino que también es útil para analizar los ataques cibernéticos más comunes. Cada una de estas vulneraciones—ya sea a la confidencialidad, integridad o disponibilidad—constituye una amenaza para el bien jurídico de la información. Estos pilares no solo son importantes para la protección de datos a nivel individual, sino que también son críticos para la seguridad de sistemas más complejos, como los utilizados en grandes organizaciones o en infraestructuras gubernamentales. La violación de cualquiera de estos principios puede derivar en graves implicaciones legales para los responsables (Camacho & Salvedo, 2022).

En cuanto a las sanciones, la Ley 1273 de 2009 establece penas de prisión que van desde 48 hasta 96 meses (de 4 a 8 años) para quienes vulneren alguno de los pilares de la seguridad de la información. Adicionalmente, se contemplan multas de entre 100 y 1000 salarios mínimos legales mensuales vigentes, lo que refleja la severidad con la que se tratan estos delitos en el ordenamiento jurídico colombiano (Ley 1273, 2009). La tipificación y sanción de estos ciberdelitos se basa en el tipo de afectación generada, y siempre debe

garantizarse el respeto al debido proceso, tal como lo establece el artículo 29 de la Constitución Política de Colombia (Camacho & Salvedo, 2022). El proceso penal se inicia con la denuncia de la víctima ante las autoridades competentes, quienes tienen la responsabilidad de proteger el bien jurídico de la información, asegurando la correcta aplicación de la ley.

Dentro de este marco, es fundamental definir claramente los tres pilares de la seguridad de la información. La integridad se refiere a la precisión de los datos, asegurando que no hayan sido alterados sin autorización. Es común relacionar este pilar con la autenticidad, la cual algunos autores consideran como un cuarto elemento clave dentro de la seguridad de la información, aunque en su mayoría se acepta que la integridad incluye la verificación de la autenticidad de los datos (Camacho & Salvedo, 2022). En cuanto a la confidencialidad, esta garantiza que solo las personas autorizadas puedan acceder a la información, protegiéndola de accesos no autorizados, lo que es esencial para mantener la privacidad y seguridad de los datos personales o confidenciales (Salvatori, 2011). Por último, la disponibilidad asegura que los datos y sistemas estén siempre accesibles para aquellos que tengan autorización, lo cual es vital en la era digital, donde la inaccesibilidad puede generar grandes pérdidas y consecuencias, tanto para individuos como para empresas (Dávila, 2020).

La Ley 1273 de 2009 ha sido un pilar fundamental en la regulación de los delitos informáticos en Colombia, al otorgar un marco jurídico claro para la protección de la información como bien jurídico. Esta ley, centrada en la Triada CID, ha establecido sanciones específicas para quienes vulneren los pilares de la seguridad de la información, garantizando un enfoque integral para la protección de los datos y sistemas informáticos en el país. A medida que la tecnología avanza, la aplicación de esta ley sigue siendo crucial para enfrentar los nuevos desafíos que plantean los ciberdelitos y las amenazas informáticas (Camacho & Salvedo, 2022).

El juicio de antijuridicidad en el delito de violación de datos personales puede analizarse desde la perspectiva de la teoría general del delito, la cual organiza los elementos comunes a todos los delitos, como la conducta, tipicidad, antijuridicidad y culpabilidad, en un orden jurídico específico (Zaffaroni et al., 2006).

Francesco Carrara (1971) definió el delito como la "infracción a la ley del Estado, promulgada para proteger la seguridad de los ciudadanos" (p. 17). De esta manera, un delito implica un acto que afecta bienes jurídicos protegidos por el Estado, y su análisis se realiza mediante categorías dogmáticas que permiten diferenciar conductas que deben sancionarse penalmente de aquellas que no.

La antijuridicidad es un juicio de valor negativo que recae sobre una conducta que lesiona o pone en peligro un bien jurídico sin justificación alguna (Von Liszt, 1911, citado por Mir Puig, 1994, p. 5). Se puede dividir en antijuridicidad formal y material: la primera refiere a la infracción de una norma estatal, mientras que la segunda implica un perjuicio real al bien jurídico protegido, que en este caso es la protección de datos personales (Mir Puig, 1994). Si se comprueba que una conducta afecta dicho bien, pero existe una causa de justificación como la legítima defensa o el consentimiento del sujeto pasivo, no habrá antijuridicidad formal ni material.

En cuanto a la tipicidad, esta consiste en un juicio negativo sobre la conducta que coincide con las características previstas en el tipo penal, lo que permite la aplicación del poder punitivo estatal (Velásquez, 2020). El delito de violación de datos personales, tipificado en el artículo 269F del Código Penal colombiano, se configura cuando una persona, sin autorización, obtiene, compila, sustrae, o utiliza datos personales con beneficio propio o de un tercero (Ley 906, 2004).

Este delito se clasifica como un tipo compuesto de conducta alternativa, ya que se puede cometer mediante diversas acciones, como obtener, sustraer o modificar datos. Además, se considera un tipo abierto, dado que los términos utilizados en la norma son amplios y no delimitan con precisión las conductas prohibidas, y un tipo pluriofensivo, ya que afecta tanto el bien jurídico de la información como el de la intimidad (Salgado, 2020).

Este tipo penal incluye un elemento subjetivo particular: la conducta debe realizarse con la intención de obtener algún beneficio, que no necesariamente tiene que ser económico, lo que refuerza la complejidad de su análisis dentro de la dogmática penal (Zaffaroni et al., 2006).

El Código Penal colombiano, en la Ley 599 de 2000, aborda en el Capítulo Séptimo los delitos relacionados con la intimidad y la interceptación de comunicaciones, tales como la violación ilegal de comunicaciones y el acceso no autorizado a sistemas informáticos. Estos delitos protegen derechos fundamentales como la libertad, la intimidad y la dignidad, sin embargo, la legislación inicial no contemplaba sanciones penales robustas para ciertos delitos informáticos, como el almacenamiento de contenido inapropiado relacionado con menores, lo cual limitaba su efectividad (Ojeda et al., 2010).

En respuesta, se promulgó la Ley 1336 de 2009, que fortaleció las disposiciones de la Ley 679 de 2001, imponiendo penas severas para los delitos relacionados con el turismo sexual y la pornografía infantil. No obstante, las infracciones relacionadas con el uso indebido de la tecnología requerían un bien jurídico más específico. Para abordar esta

problemática, se introdujo la protección de la "información y datos personales" como bien jurídico con la Ley 1273 de 2009, que tipificó los delitos informáticos como el acceso indebido a sistemas informáticos, la interceptación de datos y la violación de datos personales (Bonett, 2019).

Este avance normativo ha sido fundamental para que las entidades públicas y privadas puedan enfrentar los delitos informáticos, alineando a Colombia con los estándares internacionales, como el Convenio sobre Ciberdelincuencia de Budapest de 2001. La Ley 1273 ha permitido no solo la persecución penal de estas conductas, sino también la implementación de políticas y procedimientos en las organizaciones para proteger la integridad de la información y garantizar la continuidad operativa (Davenport, 1999).

Así las cosas, aunque la Ley 1273 de 2009 ha sido clave para la protección de los datos personales y la información en Colombia, aún se enfrenta a desafíos en su aplicación y adaptación a las nuevas tecnologías. Es crucial seguir fortaleciendo el marco normativo y fomentar la conciencia ciudadana sobre la importancia de proteger los datos personales (Ojeda et al., 2010).

El marco constitucional del delito de violación de datos personales en Colombia se basa en los artículos 15 y 20 de la Constitución Política (1991). El artículo 15 protege el derecho de todas las personas a la privacidad y la protección de sus datos personales, mientras que el artículo 20 garantiza la libertad de expresión y difusión, elementos esenciales para la seguridad cibernética (Constitución Política de Colombia, 1991).

En el ámbito legal, el primer avance significativo fue el Decreto 1360 de 1989, que estableció la inscripción de software en el Registro Nacional de Derecho de Autor, sentando las bases para la protección de la propiedad intelectual en el campo informático (Decreto 1360, 1989). Posteriormente, la Ley 1273 de 2009, conocida como "Ley de Delitos Informáticos", modificó el Código Penal y estableció delitos relacionados con la protección de la información contenida en sistemas informáticos (Ley 1273, 2009).

Entre los delitos informáticos, el artículo 269A del Código Penal tipifica el acceso abusivo a un sistema informático, mientras que el artículo 269B se refiere al sabotaje informático. Por otro lado, el artículo 269C aborda la intercepción ilegítima de datos informáticos, y el artículo 269D establece el delito de daño informático. Estos delitos buscan proteger la integridad y seguridad de los sistemas de información en Colombia (Ley 1273, 2009).

El artículo 269F del Código Penal colombiano tipifica el delito de violación de datos personales, que se refiere al acceso no autorizado a datos personales en sistemas informáticos

o redes sociales. Este delito tiene como objetivo salvaguardar derechos fundamentales, como la dignidad humana y la libertad ideológica (Bechara, Alan & Ledezma, 2020).

La Ley 1273 también incluye otros delitos, como el phishing (artículo 269G) y el hurto por medios informáticos (artículo 269I), todos ellos orientados a proteger la seguridad y privacidad de la información en el entorno digital.

Finalmente, la identificación de los elementos del tipo penal de violación de datos personales requiere analizar tanto el tipo objetivo (los aspectos observables de la conducta) como el tipo subjetivo (la intención del sujeto), para asegurar una correcta aplicación del derecho penal (Vega, 2016).

El tipo penal de violación de datos personales en Colombia tiene una estructura específica que incluye varios elementos clave:

- **Sujeto activo y pasivo**: El sujeto activo es la persona, natural o jurídica, que comete el delito. No requiere una cualidad especial y puede ser agravado si es un funcionario público actuando en sus funciones (Ibáñez, 2021). El sujeto pasivo es el afectado por el delito, que puede ser el Estado, entidades jurídicas o particulares (Ibáñez, 2021).
- **Objeto jurídico y material**: El objeto jurídico es la protección de los datos personales, un bien jurídico protegido que puede abarcar derechos como la intimidad (Chanjan et al., 2020). El objeto material incluye los datos personales almacenados en archivos, ficheros o bases de datos (Vega, 2016).
- **Verbos rectores**: Estos incluyen acciones como comprar, ofrecer, compilar, emplear, y obtener, que definen el comportamiento delictivo. Algunos son de mera conducta y otros requieren un resultado (Ley 1273, 2009).
- **Imputación objetiva**: El delito se imputa cuando la conducta genera un riesgo jurídicamente desaprobado que afecta los datos personales. La teoría del nexo causal tradicional es insuficiente para los delitos informáticos, por lo que se propone el uso del nexo lógico, basado en la interacción entre el sistema y el sujeto activo (Aguirre, 2020).
- **Resultado y permanencia**: El delito de violación de datos personales genera un cambio en el mundo virtual y puede tener carácter permanente si el sujeto continúa cometiendo acciones como obtener o modificar datos (Ibáñez, 2021).

- **Tipo subjetivo y antijuricidad**: El delito solo puede ser doloso, lo que significa que el sujeto activo debe tener conocimiento y voluntad de realizar las acciones. La *antijuridicidad* implica que la conducta viola la normativa penal y pone en peligro bienes jurídicos protegidos, sin causa justificada (Salgado, 2020).

El artículo 32 del Código Penal Colombiano establece diversas causales de ausencia de responsabilidad penal, es decir, situaciones en las que una persona no será penalmente responsable por una conducta típica y antijurídica. Entre las principales causales se encuentran el **c**aso fortuito y la fuerza mayor**,** el consentimiento del titular del bien jurídico cuando sea posible disponer de él, el cumplimiento de un deber legal **y** el cumplimiento de órdenes legítimas de autoridad competente, con excepción de casos de genocidio, desaparición forzada y tortura (Ley 599, 2000).

Además, se incluye el ejercicio legítimo de derechos, actividades lícitas o cargos públicos**,** y la legítima defensa ante una agresión injusta actual o inminente. También se contempla la protección de derechos ante peligros inminentes que no puedan evitarse de otra manera y la coacción o miedo insuperable. El artículo también menciona el error invencible sobre la tipicidad de la conducta o la licitud de la misma. Si el error es vencible, se impondrá una pena atenuada. Estas disposiciones reflejan que no habrá responsabilidad penal cuando se actúe dentro de los límites de estas causales, aunque el exceso en su aplicación puede acarrear sanciones atenuadas (Ibáñez, 2021).

En cuanto a la culpabilidad, la Corte Constitucional ha señalado que esta implica un juicio de reproche sobre la conducta del actor. La culpabilidad, que está basada en el principio de presunción de inocencia, es esencial para imponer una sanción penal. No se evalúan aspectos subjetivos del individuo, como su personalidad o temperamento, sino su conducta en relación con el resultado reprochable. Así, la culpabilidad permite ajustar la pena de manera proporcional, considerando el dolo, la culpa o la preterintención, y se excluye cualquier forma de responsabilidad objetiva (Corte Constitucional, sentencia C-181, 2016).

Asimismo, se reconoce la existencia de condiciones de imputabilidad disminuida, como el caso de sujetos que presentan trastornos que, aunque no los incapacitan por completo, reducen su capacidad de autodeterminación. Esto se considera un atenuante. De igual forma, la inimputabilidad ocurre cuando un sujeto no comprende la ilicitud de su conducta debido a trastornos mentales o inmadurez psicológica. En tales casos, se imponen medidas de seguridad en lugar de sanciones penales, con el objetivo de rehabilitar al individuo (Ospina, 2018; Ibáñez, 2021).

La regulación colombiana en materia de protección de datos personales establece un marco general para las entidades públicas y privadas, que abarca el tratamiento, gestión y almacenamiento de información personal, así como los derechos de los individuos sobre sus datos (Barrera, 2021). Las obligaciones de los responsables del tratamiento incluyen la conservación de la prueba de autorización del titular, la creación de una política de protección de datos de acceso público, y la documentación de los procedimientos relacionados, siendo aplicables tanto a plataformas de comercio electrónico como a los terceros que actúan en su nombre (Superintendencia de Industria y Comercio, 2017).

A pesar de estos avances, aún no existe una legislación específica que defina claramente las responsabilidades en cada fase de las transacciones electrónicas. Esto se agrava por la falta de un procedimiento de inspección y vigilancia específico para el comercio digital, lo que deja vacíos en la protección de los datos en este ámbito (Barrera, 2021). Aunque se pueden encontrar disposiciones dispersas en normativas como el estatuto del consumidor, estas no están consolidadas en un marco integral que regule el comercio electrónico (Barrera, 2021).

El Documento CONPES 3620, aprobado en 2010, reconoció la importancia de impulsar el comercio electrónico, aunque señaló la existencia de vacíos normativos. Posteriormente, el Documento CONPES 3975 de 2019, centrado en la transformación digital, también abordó la cadena de valor del comercio electrónico, pero sin enfocarse específicamente en la protección de datos (Martínez, 2019). La publicación del borrador del CONPES en 2020 sobre comercio electrónico respondió a las deficiencias detectadas durante los días sin IVA, donde la fragilidad de las plataformas digitales quedó expuesta debido al incremento en el tráfico de usuarios.

Sin embargo, persiste la falta de un enfoque sólido en la protección de datos personales en el comercio digital, lo que compromete la confianza y la seguridad en las transacciones en línea. Las experiencias internacionales ofrecen valiosas lecciones sobre cómo estructurar marcos normativos que protejan los derechos de los usuarios y garanticen un entorno seguro (Barrera, 2021).

El delito de violación de datos personales, establecido en el artículo 269F del Código Penal colombiano, refleja la necesidad de adaptar el derecho penal a la era digital. Este tipo de delitos busca sancionar el uso indebido de la tecnología, protegiendo así la privacidad y los derechos individuales en un contexto de creciente interconexión global.

De otro lado, el Reglamento General de Protección de Datos (RGPD) ha sido pionero en la aplicación extraterritorial de sus normativas, seguido por la Ley de Privacidad del

Consumidor de California (CCPA) y la legislación brasileña. En cuanto al RGPD, su artículo 3 establece que se aplica al tratamiento de datos de residentes de la Unión Europea (UE) por responsables fuera de la UE cuando el tratamiento está vinculado con la oferta de bienes o servicios o el monitoreo de comportamientos en la UE. Esto implica que una empresa colombiana que no opere físicamente en Europa puede estar sujeta a este reglamento si, por ejemplo, ofrece servicios o productos a ciudadanos de la UE (RGPD, 2016).

El concepto de "dato personal" en el RGPD es más amplio que en la legislación colombiana. El RGPD considera como dato personal cualquier información que permita identificar, directa o indirectamente, a una persona física, incluso sin conocer su identidad precisa, a través de medios como cookies o direcciones IP (RGPD, 2016). En Colombia, los datos personales se clasifican de manera más tradicional, requiriendo una combinación de varios elementos para identificar a la persona (Ley 1581 de 2012).

En cuanto a las bases legales para el tratamiento de datos personales, el RGPD reconoce seis, mientras que en Colombia solo se permite el consentimiento explícito del titular, con excepciones bajo circunstancias específicas, como en el caso de datos públicos o emergencias médicas (Ley 1581 de 2012; RGPD, 2016).

Respecto a los principios que guían el tratamiento de los datos, el RGPD introduce la "licitud, lealtad y transparencia", que obliga a garantizar que el tratamiento sea legal, justo y transparente. Estos principios son comparables a la legislación colombiana, que incorpora principios como la finalidad, pero sin el mismo nivel de desarrollo que en el RGPD (RGPD, 2016; Corte Constitucional de Colombia, 2013).

En cuanto a los derechos de los interesados, el RGPD expande los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) de la legislación colombiana, añadiendo el derecho a la "limitación del tratamiento", la "portabilidad de datos" y el derecho a "no ser objeto de decisiones automatizadas", garantizando una mayor protección de los datos personales (RGPD, 2016).

En cuanto a la gestión de brechas de seguridad, el RGPD establece plazos estrictos para notificar tanto a la autoridad como a los interesados en caso de que ocurra un incidente, mientras que en Colombia la notificación tiene un plazo de 15 días hábiles y no contempla sanciones por demoras (RGPD, 2016; Ley 1581 de 2012).

El régimen colombiano de transferencia y transmisión internacional de datos personales establece distintos requisitos y procedimientos. Para la **transferencia internacional** (de un controlador a otro controlador), se requiere el consentimiento del titular, y se debe realizar a países con un nivel adecuado de protección o bajo excepciones previstas

por la ley, registrando la transferencia en el Registro Nacional de Bases de Datos (RNBD). Además, es necesario formalizar un contrato entre los controladores. Para la **transmisión internacional** (de un controlador a un encargado), no es necesario el consentimiento del titular si hay un contrato de transmisión que cumpla con los requisitos legales y se registra en el RNBD.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea, por su parte, permite las transferencias internacionales a países con nivel adecuado de protección o bajo ciertas garantías, y prevé excepciones en casos específicos. Comparado con la normativa colombiana, el RGPD es más flexible y adaptado a situaciones diversas, ofreciendo mayores garantías.

El RGPD introduce actores como el delegado de Protección de Datos (DPD), obligatorio en ciertos casos, mientras que en Colombia se designa un Oficial de Protección de Datos (OPD) con funciones similares. También establece figuras como el representante del responsable y del encargado para empresas sin presencia en la UE, y el corresponsable para aquellas que comparten el tratamiento de datos, algo que en Colombia no está formalmente regulado.

En cuanto a las autoridades de protección de datos, tanto en el RGPD como en Colombia se garantiza su independencia y se les asignan funciones de supervisión y sanción. Sin embargo, el RGPD establece responsabilidades adicionales, como el asesoramiento en tratamiento de datos y la adopción de mecanismos de certificación, lo que amplía su alcance en comparación con la legislación colombiana.

El RGPD prevé sanciones más estrictas y detalladas que en Colombia, evaluando criterios como la gravedad de la infracción, el número de afectados y las medidas tomadas por el responsable. Las sanciones en Colombia se consideran menos disuasorias, ya que las multas están limitadas a un monto que podría no ser suficiente para garantizar el cumplimiento efectivo de la ley. En resumen, mientras que la legislación colombiana sigue los principios básicos de protección de datos, el RGPD establece un marco más robusto y detallado, destacando la necesidad de que Colombia modernice su normativa para alinearse con los estándares internacionales.

2.1. Caracterización del bien jurídico tutelado del delito de violación de datos personales y su juicio de antijuricidad.

El primer capítulo se centra en la caracterización del delito de violación de datos personales en Colombia, con un enfoque particular en el bien jurídico tutelado y su juicio de antijuridicidad. La Ley 1273 de 2009 marcó un hito en la legislación colombiana al reconocer

la información y los datos como un bien jurídico protegido, estableciendo así un marco normativo para la persecución penal de los delitos informáticos. A través de un estudio de esta normativa y de la doctrina relacionada, se busca comprender los elementos constitutivos del delito de violación de datos personales, así como las implicaciones de su tipificación para la protección de la privacidad y la seguridad en el ámbito digital.

En 2009, se promulgó en Colombia la Ley 1273, la cual establece el marco legal que introduce lo que hoy conocemos como el bien jurídico de la información. Esta normativa, conocida como la Ley de Delitos Informáticos, fue un avance relevante, ya que antes de su creación no existía una regulación específica para identificar o sancionar a un delincuente informático en el país. A partir de ese año, la información se convierte en un bien jurídico, lo que implica que, al igual que otros bienes jurídicos, puede ser objeto de delitos. (Ley 1273, 2009)

Previo a la Ley 1273 de 2009, la información no era considerada un bien jurídico. Sin embargo, desde su promulgación y hasta la actualidad, al reconocerla como tal, se les otorga una protección similar a otros derechos consagrados en el Código Penal. Esto significa que, al igual que otros bienes jurídicos, la información puede ser vulnerada, lo que da lugar a la tipificación de delitos relacionados con su protección. (Camacho & Salvedo, 2022)

La información que poseen las personas, al ser un bien jurídico de su propiedad, requiere la definición de ciertos parámetros que permitan determinar en qué punto se considera vulnerado este bien jurídico. Estos elementos permiten establecer los delitos informáticos, los cuales se agrupan en torno a tres aspectos principales:

1. La confidencialidad de la información.
2. La integridad de la información.
3. La disponibilidad de la información.

Estos tres aspectos conforman lo que se conoce como los pilares de la seguridad de la información, o la Triada CID (Confidencialidad, Integridad, Disponibilidad), y son la base sobre la cual se configuran los delitos informáticos (Rueda, 2020). Esto significa que cualquier violación a la confidencialidad, integridad o disponibilidad de la información constituye un delito. (Rueda, 2020).

Desde esta perspectiva, los tres pilares de la seguridad de la información son los elementos que configuran los delitos informáticos en Colombia, lo cual es esencial para el sistema de seguridad informática. La Triada CID permite analizar y clasificar cualquier tipo de situación informática en el contexto de los delitos.

Esta triada también es útil para examinar diferentes tipos de ataques informáticos, ejemplos que serán abordados en este artículo para familiarizar al lector con los delitos informáticos y sus métodos operativos. El punto clave aquí es entender que cualquier delito informático implica una afectación o violación a uno de los pilares de seguridad de la información, reconocido como un bien jurídico especial. Así, el marco de este artículo se basa en la Ley 1273 de 2009, que establece el marco jurídico para los delitos informáticos en Colombia. (Camacho & Salvedo, 2022)

Finalmente, en cuanto a las penas, aquellos que vulneren alguno de los pilares de la información pueden enfrentar sanciones que incluyen penas de prisión de entre 48 y 96 meses (de 4 a 8 años), según lo dispuesto por la Ley 1273 de 2009, además de multas que oscilan entre 100 y 1000 salarios mínimos legales mensuales vigentes. (Ley 1273, 2009).

Bajo esta ley, los ciberdelitos se tipifican y sancionan según el tipo de afectación y la conducta delictiva asociada. Las autoridades deben tipificar estos delitos respetando el debido proceso establecido en el artículo 29 de la Constitución. La sanción de estas conductas también depende de que las víctimas presenten las denuncias correspondientes ante las autoridades competentes, quienes son responsables de proteger el bien jurídico de la información.

Dado que los delitos informáticos se estructuran alrededor de los tres pilares de la información (integridad, confidencialidad y disponibilidad), es fundamental proporcionar una breve definición de cada uno para el desarrollo del presente artículo.

En cuanto a las penas y sanciones, aquellos que infrinjan alguno de los pilares de la seguridad de la información, considerado como un bien jurídico, pueden enfrentar penas de prisión que van desde los 48 hasta los 96 meses, lo que equivale a entre 4 y 8 años de cárcel. Además, se contemplan multas que oscilan entre 100 y 1000 salarios mínimos legales mensuales vigentes, tal como lo establece la Ley 1273 de 2009. (Camacho & Salvedo, 2022 p. 7).

Desde esta perspectiva, la Ley 1273 tipifica y sanciona los ciberdelitos de acuerdo con el tipo de afectación que se genere y la conducta delictiva asociada. Las autoridades están encargadas de tipificar estos delitos, garantizando siempre el respeto al debido proceso consagrado en el artículo 29 de la Constitución Política. Asimismo, las sanciones están condicionadas a la denuncia presentada por las víctimas de estos delitos informáticos ante las autoridades competentes. Es responsabilidad del Estado, a través de sus instituciones, velar por la protección del bien jurídico de la información.

Dado que los delitos informáticos se configuran en torno a los tres pilares de la seguridad de la información (integridad, confidencialidad y disponibilidad), es fundamental definir brevemente cada uno de ellos, ya que serán esenciales para el desarrollo de este artículo.

- **Integridad**:

Como primer pilar, la integridad se refiere a la precisión y exactitud de los datos almacenados o transmitidos, garantizando que no han sido alterados, perdidos, modificados o destruidos sin autorización. Es crucial para todos los ciudadanos que la información dentro de nuestras organizaciones se mantenga íntegra (Acurio, 2016).

Además, algunos autores relacionan la integridad con la autenticidad, considerando esta última como un pilar adicional de la seguridad de la información, dado que ciertos delitos informáticos también se configuran en torno a la autenticidad de los datos. Sin embargo, la integridad se entiende como la originalidad, exactitud y completitud de la información, asegurando que no ha sido modificada por personas no autorizadas. Si esta información es alterada sin el consentimiento de quien tiene derecho legítimo sobre ella, entonces es cuando se configura un delito informático, conforme a lo estipulado por la Ley 1273 de 2009. (Camacho & Salvedo, 2022).

- **Confidencialidad**

El segundo pilar de la seguridad de la información es la confidencialidad, que se refiere a la característica que asegura que la información solo sea accesible o legible por las personas o entidades autorizadas. Este principio es aplicable cuando se trata de autoridades, documentos clasificados o información sensible, que solo debe ser conocida por un grupo específico dentro de una organización o, en algunos casos, cuando se habla de datos personales. La confidencialidad garantiza que el acceso a esta información esté restringido a quienes tienen el permiso adecuado. Si esta propiedad es vulnerada, se cometen una serie de delitos relacionados (Salvatori, 2011).

- **Disponibilidad**

El tercer pilar es la disponibilidad, que se refiere a la capacidad de un sistema, servicio o conjunto de datos de estar accesible y utilizable por los usuarios o procesos autorizados cuando sea necesario. Este concepto se vincula con la disponibilidad continua, 24 horas al día, 7 días a la semana, y 365 días al año. El acceso constante a sistemas de información, datos y plataformas es fundamental en la era digital, y la falta de disponibilidad de estos servicios puede derivar en la comisión de delitos informáticos, como los ataques de

denegación de servicio. Estos ataques buscan agotar los recursos de un sistema para que los usuarios no puedan acceder a él, incluso para acciones básicas como visualizar un sitio web. (Camacho & Salvedo, 2022).

La indisponibilidad de un sistema no solo afecta a los usuarios, sino también a las organizaciones, que pueden perder recursos y ver obstaculizadas las actividades de sus empleados o colaboradores, quienes dependen de sistemas o plataformas para realizar sus tareas cotidianas. Cuando un servicio o plataforma se vuelve inaccesible, puede generarse caos, lo que convierte la indisponibilidad en un área crítica donde también se configuran delitos informáticos (Dávila, 2020).

Para evaluar situaciones reales en las que se cometen conductas relacionadas con ciberdelitos, se deben tener en cuenta los tres pilares fundamentales de la seguridad de la información. Esto permitirá reflexionar sobre los casos de ataques informáticos que ocurren con frecuencia y determinar si han afectado de manera directa la triada CIA.

Así, una violación a la integridad, confidencialidad, disponibilidad, o incluso a la autenticidad, considerada por algunos como un posible cuarto pilar, son elementos clave que deben ser considerados al momento de tipificar un delito informático. Por ello, es esencial tener una comprensión clara de estos pilares, ya que la Ley 1273 de 2009, en su primer capítulo, establece que el Congreso de Colombia decreta la adición de un nuevo título séptimo al Código Penal, titulado "De la protección de la información y los datos". En dicho capítulo se declara que "los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos" serán considerados delitos informáticos. (Camacho & Salvedo, 2022).

2.1.2 Juicio de antijuricidad en el delito de violación de datos personales

La teoría general del delito organiza los elementos comunes a todos los delitos en un orden jurídico específico, tales como autoría, participación, dolo, culpa, acción, omisión, entre otros. Los teóricos han intentado definir lo que se entiende por delito, con el fin de delimitar sus componentes esenciales y así excluir del ámbito del derecho penal aquellas conductas que no cumplan con esos criterios.

Francesco Carrara (1971) lo describía como "la infracción a la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, que surge de un acto externo del hombre, ya sea positivo o negativo, moralmente imputable y socialmente dañino"

El delito, así entendido, consta de cuatro "categorías dogmáticas" que se ordenan de manera lógica: conducta, tipicidad, antijuridicidad y culpabilidad. Estas categorías funcionan como filtros para evitar el ejercicio irracional del poder punitivo, asegurando que se

determinen de manera inteligente la cantidad, calidad y forma de las acciones que pueden ser objeto de sanción penal (Zaffaroni et al., 2006).

A continuación, abordemos cada una de estas categorías de manera concisa, definiéndolas y señalando las causas de exclusión, con una especial atención a la tipicidad al final por razones prácticas.

La conducta se refiere a un comportamiento humano controlado y dirigido por la voluntad que genera un cambio en el mundo exterior (Mahecha, 1963). Si se trata de un hecho natural, de un animal o de una persona jurídica, no se considera conducta, ya que no hay un comportamiento humano. De igual manera, si el acto es consecuencia de fuerza mayor, un reflejo involuntario o un estado de inconsciencia, tampoco se considerará conducta, pues no está bajo el control de la voluntad humana. Incluso si se trata de un pensamiento que no se ha exteriorizado, no habrá conducta, ya que la voluntad no ha llegado a manifestarse externamente. El principio del acto o de la objetividad material indica que, sin conducta, no hay delito.

La antijuridicidad es un juicio de valor negativo que recae sobre una conducta, dado que esta ha lesionado o puesto en peligro, sin una causa justificada, un bien jurídico protegido por el tipo penal. Según Von Liszt (1911), citado por Mir Puig (1994, p. 5), se puede distinguir entre antijuridicidad material, que es la mencionada anteriormente, y antijuridicidad formal, que se refiere a "la infracción de una norma estatal, ya sea un mandato o prohibición del ordenamiento jurídico".

Si la conducta no afecta ni pone en peligro el bien jurídico, no habrá antijuridicidad material. En cambio, si la conducta sí afecta o pone en riesgo el bien jurídico, pero existe una causal de justificación, como la legítima defensa, el consentimiento del sujeto pasivo o el estado de necesidad justificante, tampoco habrá antijuridicidad formal. La antijuridicidad refleja los principios de lesividad y proporcionalidad, de modo que, si no hay un perjuicio real o si el sacrificio de la norma conlleva mayores beneficios que el daño causado, no se configurará un delito.

La culpabilidad, por su parte, es un juicio negativo que se aplica no solo sobre la conducta, sino principalmente sobre el sujeto que la llevó a cabo, en la medida en que este ha cometido un acto injusto a pesar de que le era exigible, desde el punto de vista jurídico, abstenerse de hacerlo. Según Jescheck (1996), "la culpabilidad implica que se valora negativamente las máximas que guiaron al autor en la formación de su voluntad, permitiendo así que el hecho le sea personalmente reprochable" (p. 597). Si la conducta se comete bajo un error invencible de prohibición, en un estado de necesidad exculpante o por parte de una

persona inimputable, no habrá culpabilidad. Este concepto concreta el principio de culpabilidad, lo que significa que, si el acto no puede atribuirse al autor por dolo, culpa o preterintención, no habrá delito.

La tipicidad, por último, es un juicio negativo que se formula sobre la conducta cuando esta coincide o se ajusta a las características previstas por el legislador en el tipo penal (Velásquez, 2020, p. 346). Si la conducta se comete bajo un error de tipo, en cualquiera de sus formas, no habrá tipicidad. La tipicidad refleja, entre otros, el principio de legalidad, de manera que, si no existe una ley previa, escrita, clara y precisa, no se podrá configurar un delito. El tipo penal, como núcleo de la tipicidad, se deriva de la expresión latina "tipus", que si

- ***Antijuridicidad formal:***

Formalmente, en el delito de violación de datos personales, la antijuridicidad se configura cuando el sujeto activo realiza la conducta descrita en el artículo 269F del código penal, infringiendo así la normativa penal vigente. En consecuencia, se establece la antijuridicidad formal.

- ***Antijuridicidad material***

En cuanto a la antijuridicidad material, una vez confirmada la antijuridicidad formal del delito de violación de datos personales, es necesario examinar si el hecho efectivamente lesionó o puso en riesgo el bien o interés jurídico protegido, como la protección de la información y los datos, entre otros, sin justificación alguna. significa "modelo o representación de algo". (Salgado, 2020).

Es, en esencia, la descripción que hace el legislador de una conducta, tanto en su aspecto objetivo como subjetivo, con el fin de prohibirla, ordenarla o regular el deber de cuidado. Como señalan Zaffaroni y otros autores, "el tipo penal es la fórmula legal que habilita el ejercicio formal del poder punitivo y permite al derecho penal limitar las hipótesis de conflictos que pueden ser objeto de decisión jurídica" (Zaffaroni et al., 2006).

Los tipos penales pueden clasificarse de diversas maneras, según diferentes criterios. En esta ocasión, nos enfocaremos en su clasificación basada en su estructura, la conducta descrita, el sujeto activo, el bien jurídico protegido, y la forma en que se individualiza la conducta. Además, se hará un análisis sobre el tipo penal de violación de datos personales contemplado en la Ley 1273 de 2009.

Para ello, Se seguirá la clasificación presentada por el profesor Velásquez (2020) en su obra *Fundamentos de Derecho Penal* (p. 408-214).

- **Clasificación de los tipos penales según su estructura:**
  - Tipos fundamentales: aquellos que describen una o varias conductas de manera independiente, sin depender de otro tipo penal.
  - Tipos subordinados: aquellos que se basan en un tipo básico o fundamental, pero añaden elementos que lo modifican.
  - Tipos autónomos: describen la misma conducta que un tipo básico fundamental, pero incluyen elementos adicionales que alteran su naturaleza.
- **Clasificación de los tipos penales según la conducta descrita:**
  - Tipos elementales o simples: se refieren a una sola conducta, representada por un único verbo rector.
  - Tipos compuestos: aquellos que describen múltiples conductas.
- Compuestos mixtos o de conducta alternativa: describen varias conductas, pero la ejecución de cualquiera de ellas basta para considerar consumada la conducta típica.
- Compuestos complejos: describen diversas conductas que, si se consideraran por separado, generarían diferentes tipos penales, pero el legislador las agrupa bajo un solo tipo penal independiente.
- Tipos de mera conducta: no requieren que una determinada modificación en el mundo exterior ocurra tras la realización de la conducta descrita.
- Tipos de resultado material: identifican un cambio específico en el mundo exterior, que debe ocurrir de manera separada en el tiempo y el espacio de la conducta misma.
- Tipos abiertos: aquellos que no definen de manera exacta la conducta que describen. Utilizan términos con un significado amplio y relativamente indeterminado (Corte Constitucional, C-091, 2017).

Tipos cerrados: aquellos que delimitan con precisión la conducta que describen.

- **Clasificación de los tipos penales según el sujeto activo de la conducta:**
  - Tipos de sujeto activo común: no requieren una cualidad específica en el sujeto activo de la conducta.
  - Tipos de sujeto activo calificado: exigen que el sujeto activo posea una cualidad especial para la comisión de la conducta descrita.

Clasificación de los tipos penales según el bien jurídico protegido:

- Tipos monofensivos: describen conductas que pueden afectar un único bien jurídico.
- Tipos pluriofensivos: describen conductas que pueden afectar múltiples bienes jurídicos.

Clasificación de los tipos penales según la forma de individualización de la conducta:

- Tipos comisivos: aquellos que establecen la acción prohibida.
- Tipos omisivos: aquellos que describen la acción que se ordena realizar.

- Tipos dolosos: aquellos en los que se individualiza la conducta considerando la intención o el objetivo del sujeto.
- Tipos culposos: aquellos que se enfocan en cómo se exterioriza la conducta, sin considerar la intención en sí misma.

Una vez se ha revisado la dogmática a la tipicidad y al tipo penal, pasando por la teoría del delito y las categorías dogmática, se procede a mirar el tipo penal de violación de datos personales

> "Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión" (Ley 906, 2004, art 269f).

El anterior delito see clasifica como un tipo de la siguiente manara:

(i) compuesto de conducta alternativa**:** la acción típica se consuma mediante cualquier acto de obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o utilizar datos personales ajenos;

(ii) abierto: carece de una delimitación precisa en la conducta que describe, al incluir múltiples elementos normativos imprecisos, tales como "ficheros", "códigos personales" o "medios similares";

(iii) pluriofensivo: generalmente, este tipo de conducta afecta tanto al bien jurídico de la información y los datos como al de la intimidad, tal como se establece en el Título III, Capítulo VII del Código Penal.

A diferencia de los tipos mencionados anteriormente, este tipo incluye **un** elemento subjetivo particular**,** que se suma al dolo, el cual establece que la conducta debe llevarse a cabo con la intención de obtener algún tipo de beneficio. Este beneficio no necesariamente

tiene que ser de carácter económico y puede favorecer tanto al autor de la acción como a un tercero.

2.1.3 Bien jurídico tutelado especial en los delitos cibernéticos

El Código Penal colombiano Ley 599, (2000), en el Capítulo Séptimo del Libro Segundo, Título III: Delitos contra la libertad individual y otras garantías, aborda las infracciones relacionadas con la intimidad, el secreto y la interceptación de comunicaciones:

- Artículo 192: Violación ilegal de comunicaciones.
- Artículo 193: Ofrecimiento, venta o adquisición de dispositivos aptos para interceptar comunicaciones privadas.
- Artículo 194: Divulgación y uso indebido de documentos confidenciales.
- Artículo 195: Acceso no autorizado a un sistema informático.
- Artículo 196: Violación ilícita de comunicaciones o correspondencia oficial.
- Artículo 197: Uso indebido de equipos de transmisión o recepción.

Estos preceptos están en línea con el artículo 357, que regula los daños en infraestructuras de servicios de comunicación, energía y combustibles. En 2001, la Ley 679 estableció un marco legal para prevenir y combatir la explotación, la pornografía y el turismo sexual que involucren a menores de edad. Esta normativa impuso restricciones a proveedores, administradores y usuarios de redes de información globales en cuanto al alojamiento de contenido sexual o pornográfico que involucre a menores. Sin embargo, la ley solo contempla sanciones administrativas (Artículo 10), dejando un vacío respecto a sanciones penales, lo que limita su eficacia frente a verdaderos delitos informáticos. (Ojeda, et al, 2010).

Para corregir esta omisión, el 21 de julio de 2009 se promulgó la Ley 1336, que fortalece la Ley 679 de 2001 en la lucha contra la explotación y la pornografía infantil, así como el turismo sexual con menores. En su Capítulo VI, establece penas de prisión de 10 a 20 años y multas entre 150 y 1.500 salarios mínimos mensuales vigentes (SMLMV) para los delitos relacionados con el turismo sexual y el almacenamiento e intercambio de pornografía infantil. (Ojeda, et al, 2010).

Entre los bienes jurídicos, derechos y libertades que con mayor frecuencia resultan vulnerados a través de la comisión de delitos informáticos se encuentran la libertad, la intimidad, la dignidad, la honra, el buen nombre y otros aspectos esenciales para mantener una calidad de vida adecuada para la víctima. No obstante, la protección de estos bienes

corresponde a otras tipologías delictivas, lo que ha generado la necesidad de contar con un bien jurídico específico orientado a sancionar de manera exclusiva los delitos informáticos.

En respuesta a esta necesidad, el ordenamiento jurídico colombiano estableció el bien jurídico de la información y los datos personales, con el propósito de crear una base normativa que permita la persecución penal de este tipo de conductas. Dado que estas transformaciones en las dinámicas socio-jurídicas han impulsado nuevas conductas susceptibles de tipificarse como delitos, se ha vuelto indispensable que el ámbito académico aborde estos desafíos. La cibercriminalidad, por tanto, ha emergido como un tema de estudio abundante en la doctrina jurídica. (Bonett, 2019).

Con la promulgación de la Ley 1273 de 2009, se incorporaron en Colombia los delitos informáticos, tipificándolos de la siguiente manera: acceso indebido a un sistema informático (modificado en el Código Penal); obstrucción ilícita de un sistema informático o red de telecomunicaciones; interceptación de datos informáticos; daño a sistemas informáticos; utilización de software malicioso; hurto mediante medios informáticos y similares; violación de datos personales; suplantación de sitios web con el fin de capturar datos personales, y transferencia no autorizada de activos. (Ojeda, et al, 2010).

Este marco legal ha representado un aporte significativo y una herramienta eficaz para que tanto entidades públicas como privadas enfrenten los delitos informáticos, proporcionando definiciones claras sobre los procedimientos y políticas de seguridad de la información. A su vez, permite la instauración de acciones penales contra quienes realicen las conductas tipificadas en la ley. Gracias a este avance normativo, Colombia se ha alineado con los países miembros de la Comunidad Económica Europea (CEE), que han extendido los acuerdos internacionales en materia de protección de la información y recursos informáticos a través del Convenio sobre Ciberdelincuencia, firmado en Budapest, Hungría, en 2001, y en vigor desde julio de 2004. (Ojeda, et al, 2010).

Con los avances jurídicos alcanzados en materia de "protección de la información y los datos, así como la preservación integral de los sistemas que emplean tecnologías de la información y comunicaciones", las organizaciones pueden salvaguardar una parte significativa de sus sistemas integrados de información, abarcando datos, procesos, políticas, personal, entradas, salidas, estrategias, cultura corporativa, recursos tecnológicos y el entorno externo (Davenport, 1999). Este enfoque no solo contribuye a garantizar la calidad de la información, sino que también incluye la gestión y el control dentro del concepto de protección integral.

En cuanto a la Ley 1273 (2009), su capítulo I se enfoca en respaldar de manera específica el trabajo de los grupos de Auditoría de Sistemas, ya que se centra en asegurar la calidad y seguridad de la información dentro de las organizaciones, abordando los "ataques contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos". Esta normativa refuerza el valor de la información como un activo clave para las organizaciones, que debe ser protegido adecuadamente para garantizar la continuidad operativa, optimizar el retorno de la inversión y aprovechar las oportunidades del entorno, además de mitigar y combatir los riesgos y delitos que puedan afectarla.

La gestión eficaz de la seguridad de la información en las organizaciones comienza con la implementación de políticas, estándares, procedimientos y controles adecuados, alineados naturalmente con las particularidades del negocio. En este contexto, el capítulo I de la Ley 1273 de 2009 cumple un rol fundamental al apoyar este objetivo, al igual que los estándares nacionales e internacionales que promueven una administración eficiente de la información.

En conclusión, el delito de violación de datos personales en Colombia ha experimentado una evolución con la promulgación de la Ley 1273 de 2009. Esta normativa ha reconocido la información como un bien jurídico tutelado, estableciendo un marco legal para la protección de la privacidad en el ámbito digital. A través del análisis de los elementos constitutivos del tipo penal y su relación con otros delitos informáticos, se evidencia la importancia de esta figura delictiva en el contexto actual. Sin embargo, persisten problematicas en la aplicación de la ley y en la adaptación a las nuevas tecnologías. Por tanto, es fundamental continuar fortaleciendo el marco normativo y promoviendo la conciencia ciudadana sobre la importancia de proteger los datos personales. (Ojeda, et al, 2010).

2.2 Dogmática penal del delito de violación de datos personales, establecido en el artículo 269F del Código Penal.

El segundo capítulo se enfocará en describir la dogmática penal del delito de violación de datos personales, regulado por el artículo 269F del Código Penal Colombiano. Este delito forma parte de la evolución de los delitos informáticos, los cuales han surgido con el avance de la era digital y la creciente dependencia de la sociedad en las tecnologías de la información y las comunicaciones. En este sentido, se analizará cómo la legislación colombiana ha incorporado este delito dentro de su marco penal, reflejando la necesidad de proteger un nuevo bien jurídico: la información personal y los datos. El capítulo explorará el contexto histórico de los delitos informáticos, su génesis en Colombia, y las implicaciones legales y

constitucionales del delito de violación de datos personales, destacando su impacto en la protección de los derechos fundamentales en la era digital.

2.2.1 La evolución de los delitos informáticos:

Con el avance de la modernidad, los delitos informáticos, especialmente aquellos relacionados con la violación de datos personales, han surgido debido a la creciente dependencia de la sociedad contemporánea en las tecnologías de la información y las comunicaciones. En la actualidad, se considera que estamos en la era de la globalización y la tecnología, donde la sociedad se desenvuelve en todos los aspectos de la vida, desde lo social y cultural hasta lo laboral y económico, gracias a las herramientas tecnológicas que continúan emergiendo para mejorar y fortalecer las condiciones de vida de las personas. (Sánchez, 2016).

En este mismo sentido, se comprende que el problema jurídico abordado en esta tesis de Derecho, Ciencias Políticas y Sociales no está limitado a un solo país, sino que es de naturaleza transnacional. Para cometer el delito penal en cuestión, no es necesario estar físicamente en el mismo lugar que la víctima, sino que puede ser perpetrado desde cualquier parte del mundo con acceso a Internet o a sistemas informáticos que contienen información personal y sensible. Este tipo de delito, que implica la violación o el acceso no autorizado a datos íntimos, personales y documentos, constituye una infracción penal punible por la ley, al ser una violación de los derechos humanos fundamentales consagrados en la constitución. (Sánchez 2016, p. 31).

La sociedad de la era de la información y las telecomunicaciones surge a raíz de la revolución de los computadores y la informática, especialmente después de la segunda mitad del siglo XX. Esta evolución se intensifica y expande con la apertura económica, la integración regional, el comercio internacional y la globalización, así como con el acceso generalizado a la vanguardia tecnológica. Los dispositivos desarrollados por el ser humano han generado una dependencia en las personas, lo que ha facilitado incluso la vulneración de la dignidad humana a través de nuevas conductas punibles que aprovechan los avances científico-tecnológicos.

Este fenómeno ha dado lugar a un nuevo mundo cibernético o virtual complejo, en el cual el derecho ha debido intervenir, ya que es responsabilidad del Estado regular, sancionar, resolver y juzgar las controversias y fenómenos sociales que surgen en esta nueva realidad "cibernética". Como resultado, el derecho ha evolucionado para crear un nuevo objeto jurídico de especial protección, conocido como "Protección de la información y de los datos",

un bien jurídico explícitamente establecido en el título séptimo del Código Penal Colombiano de 2000.

2.2.2 Genesis y concepto del delito informático de violación de datos personales en Colombia

En Colombia, la regulación de los delitos informáticos ha sido una prioridad debido al riesgo que representan para los derechos humanos, la seguridad nacional, la estabilidad económica y los derechos individuales. Para abordar esta problemática, el país ha adoptado el Convenio sobre Ciber-criminalidad de Budapest del 23 de noviembre de 2001, mediante el cual se compromete a garantizar la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos. Se reconoce que la protección de los datos personales es crucial en la era de las tecnologías de la información y las comunicaciones. (Sanchez, 2016).

Asimismo, se establece que el uso fraudulento de sistemas informáticos, bases de datos, redes sociales y similares será sancionado conforme al derecho penal y constitucional, dado que constituye una violación de bienes jurídicos protegidos y garantías constitucionales fundamentales. Este enfoque refleja el compromiso de Colombia con la protección de la seguridad digital y los derechos individuales en un entorno cada vez más digitalizado.

En la era actual, marcada por la conectividad y el acceso a la información a través de dispositivos electrónicos y digitales, surge una problemática relacionada con los delitos informáticos. Estos delitos representan una amenaza que pone en peligro y vulnera los bienes jurídicos de personas naturales, jurídicas y entidades estatales mediante conductas ilícitas que utilizan medios informáticos con el fin de obtener un beneficio propio o en nombre de terceros. A continuación, se presentan definiciones de delitos informáticos recopiladas de diversos autores. (Sánchez, 2016, p 52).

Los delitos informáticos, también conocidos como crímenes informáticos, son acciones u omisiones que se consideran típicas, antijurídicas y culpables cuando se dirigen contra entidades estatales, personas jurídicas o naturales. Estas acciones se realizan utilizando un sistema de tratamiento de la información, y su resultado es causar un perjuicio a la víctima, ya sea mediante lesiones o poniendo en riesgo bienes jurídicos, con el propósito de obtener un beneficio, ya sea para sí mismo o para un tercero, independientemente de si dicho beneficio es de carácter patrimonial o personal, y si se persigue con o sin ánimo de lucro (Huerta; Libano, 1998 citado en Acurio Del Pino, 2016).

Delincuencia informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier

sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera (Acurio Del Pino, 2016, p.14)

Una diferente definición de delitos informático, la ofrecen los autores Ojeda et al. (2010) en la que indican lo siguiente:

Es toda conducta ilícita, ya sea por acción u omisión, que realiza una persona mediante el uso de cualquier recurso informático y que, como consecuencia, afecta un bien informático jurídico y/o material que se encuentra legalmente protegido, haciéndose penalmente responsable por tal hecho. (p.51)

A partir de las definiciones previas, se elabora el siguiente concepto de delitos informáticos: se refiere a conductas punibles realizadas por acción u omisión, que son típicas, antijurídicas y culpables, llevadas a cabo por un sujeto activo con conocimientos técnicos y científicos en informática, telemática u otros campos relacionados. Estas conductas implican el uso indebido de cualquier medio informático con el fin de modificar, socavar, destruir, manipular, obtener, divulgar, sustraer, interceptar, entre otros actos, algún sistema informático o componente e información específica. El propósito de estas acciones es obtener un beneficio propio o en nombre de un tercero, lo cual resulta en la lesión o puesta en peligro de uno o más bienes jurídicos y/o materiales protegidos del sujeto pasivo.

Se empieza a definir el concepto de datos personales, para ello se encuentra que la ley estatutaria 1266 (2008), la define de la siguiente manera:

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

f) Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquéllos que no sean semiprivados o privados, 9 de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;

g) Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.

h) Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular

- **Violación de datos personales**

En el marco jurídico de Colombia, se introdujo el delito de violación de datos personales a través del artículo 269F del Código Penal, mediante la adición realizada por la Ley 1273 (2009), la cual establece lol siguiente:

El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Ley 1273, 2009).

Considerando lo mencionado anteriormente, se define y describe la violación de datos personales como una conducta punible que es antijurídica, típica y culpable. Esta acción es llevada a cabo por el sujeto activo sin el consentimiento del titular, utilizando cualquier medio informático, telemático o dispositivos para recopilar, modificar, interceptar, obtener, ofrecer, emplear, sustraer, vender, enviar, intercambiar, comprar o divulgar archivos, ficheros, bases de datos u otros elementos que contienen datos personales, sean estos semi privados, públicos, sensibles o privados. También se incluyen los códigos personales, que son combinaciones de números, letras y símbolos utilizados por el titular para proteger y acceder a estos datos.

El objetivo del sujeto activo es obtener un beneficio propio o en nombre de un tercero, al tiempo que se lesiona el interés jurídico de la protección de la información y los datos, pudiendo afectar uno o más bienes jurídicos y/o materiales protegidos del sujeto pasivo. Esta conducta conlleva una condena que va desde cuarenta y ocho (48) hasta noventa y seis (96) meses de prisión, además de una multa que oscila entre 100 y 1000 salarios mínimos legales mensuales vigentes. (Ibañez, J, 2021).

2.2.3. Marco Constitucional y legal del delito de violación de datos personales en Colombia

El siguiente apartado de Marco Constitucional y Legal en relación con la protección de datos personales y los delitos informáticos en Colombia se fundamenta en los artículos 15 y 20 de la Constitución Política de 1991. Estos artículos establecen el derecho a la protección de los datos personales y la inviolabilidad de la privacidad, al tiempo que garantizan la

libertad de expresión y difusión de información, factores clave para la seguridad en el entorno digital. A nivel normativo, la regulación sobre delitos informáticos comenzó con el Decreto 1360 de 1989 y se consolidó con la Ley 1273 de 2009, que tipifica una serie de delitos relacionados con el acceso abusivo, sabotaje y daño a sistemas informáticos. Esta ley, que modifica el Código Penal Colombiano, introduce nuevas figuras delictivas como el phishing, el malware y el hurto informático, todas destinadas a proteger la integridad y confidencialidad de los sistemas de información.

- ***Marco Constitucional:***

En la Constitución Política de la República de Colombia (1991), que fue publicada en el Diario Oficial de la República de Colombia, se establecen los derechos cibernéticos basados en el artículo 15. Dicho artículo afirma el derecho de todas las personas a la protección de sus datos personales, y establece la responsabilidad del Estado en garantizar este derecho. Además, se reconoce el respeto a la libertad de recopilación, procesamiento y circulación de datos, así como la inviolabilidad de todas las formas de comunicación privada.

Asimismo, el artículo 20 de la Constitución garantiza la libertad de expresión y difusión, lo que también contribuye a la seguridad cibernética de los ciudadanos. Estos dos artículos son fundamentales para salvaguardar la seguridad y privacidad de los individuos en el entorno digital. (Constitución Política de Colombia, 1991).

- ***Marco legal:***

La legislación en Colombia sobre delitos informáticos tuvo sus primeros avances con el Decreto 1360 de 1989, publicado en el Diario Oficial de la República de Colombia. Este decreto reglamentó la inscripción de software en el Registro Nacional de Derecho de Autor, lo cual brindó un marco normativo para abordar reclamaciones por violación de derechos de los desarrolladores de software. A partir de esa fecha, se empezó a contar con un marco jurídico para proteger la propiedad intelectual de los creadores de aplicaciones y soluciones informáticas. (Decreto 1360, 1989).

Sin embargo, fue en 2009 cuando se promulgó la "Ley de Delitos Informáticos" o "Ley 1273", publicada en el Diario Oficial de la República de Colombia. Esta ley modificó el Código Penal Colombiano de 2000 y su objetivo principal es la protección de datos e información contenidos en sistemas informáticos. En términos generales, la ley tipifica varios delitos informáticos. (Ley 1273, 2009).

Uno de los delitos establecidos en el Artículo 269A del Código Penal Colombiano es el acceso abusivo a un sistema informático, conocido como espionaje informático. Este delito

se comete cuando personas especializadas en sistemas informáticos acceden a ellos con el propósito de obtener información o bases de datos que puedan ser utilizadas para obtener beneficios económicos o adquirir información vital. Esto aplica tanto para personas físicas como para entidades jurídicas, especialmente cuando la información es indispensable para su funcionamiento y desarrollo de actividades laborales. Esta definición se encuentra en concordancia con el grupo de investigación Seguridad y Delitos informáticos Segudelin, (2010), que establece lo siguiente:

Cuando el pirata informático o hacker aprovecha la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad informática establecidos por las organizaciones, para extraer beneficios económicos o para indagar o demostrar la capacidad y recursos que ofrece la tecnología de la información. (p54).

En el Código Penal Colombiano de 2000, en su Artículo 269B, se define el delito de sabotaje informático como el acto de impedir u obstaculizar el funcionamiento normal de un sistema informático o el acceso a los datos de información contenidos en él. Los ciberdelincuentes buscan despojar a los propietarios de sus cuentas personales de correo electrónico o redes sociales, donde se encuentran una gran cantidad de datos. Además, esto puede llevar a otro delito, como la extorsión, cuando los delincuentes cibernéticos obtienen recursos económicos al presionar y amenazar a los propietarios para recuperar el acceso a sus sistemas informáticos. (ley 1273, 2009).

La intercepción deliberada e ilegítima de datos informáticos en transmisiones no públicas dirigidas hacia un sistema informático, originadas desde un sistema informático o realizadas dentro del mismo, también se considera un delito. Esto incluye las emisiones electromagnéticas provenientes de un sistema informático que transporta dichos datos informáticos. Esta figura jurídica se implementó en el Código Penal Colombiano como resultado de la Ley 1273, en su artículo 269C. (Ley 1273, 2009).

El Código Penal Colombiano establece el delito de sabotaje informático en el Artículo 269B, que implica impedir el funcionamiento normal de un sistema informático, mientras que la intercepción ilegítima de datos informáticos está tipificada en el artículo 269C. Ambos delitos buscan proteger la seguridad y la integridad de los sistemas de información en Colombia.

En relación con lo mencionado anteriormente, se puede observar que esta conducta cibernética tiene como objetivo principal la intercepción por parte de los ciberdelincuentes de un sistema de información, conocido como "origen", con la intención de modificar, obtener y obstruir la información emitida por dicho sistema. Esto afecta directamente la

confidencialidad tanto de personas físicas como de entidades jurídicas, y guarda una estrecha relación con el artículo 269A, ya que ambos buscan proteger la información y los datos de carácter confidencial almacenados en sistemas informáticos tanto de empresas como de individuos. (Elizalde et al, 2021).

Asimismo, el artículo 269D, que aborda el daño informático, se refiere a aquellas personas que, sin autorización, destruyen, dañan, borran, deterioran, alteran o suprimen datos informáticos, así como un sistema de tratamiento de información o sus partes o componentes lógicos. Este delito puede considerarse como una forma de sabotaje informático en concordancia con el artículo 269B mencionado anteriormente.

En la misma ley, se introduce el delito de malware en el artículo 269E. Este delito se produce cuando los ciberdelincuentes crean, adquieren, venden, envían, distribuyen o introducen programas, comúnmente conocidos como virus, en sistemas informáticos con el fin de causar un daño irreversible. Estos programas pueden ser utilizados directamente para acceder a las bases de datos de personas físicas o entidades jurídicas. (Ley 1273, 2009).

El artículo 269F aborda la conducta ilícita de violación de datos personales, también conocida como hackeo o hacking informático. Este delito ocurre cuando un ciberdelincuente accede sin consentimiento a un sistema informático o a una red social con el objetivo de obtener datos, en este caso, datos personales. Según Bechara, Alan & Ledezma (2020), este artículo tiene como objetivo principal proteger los derechos fundamentales de la persona, como la dignidad humana y la libertad ideológica.

El último artículo del primer capítulo, el 269G, aborda un término actual e innovador para cometer delitos: el phishing. En el Código Penal Colombiano, se denomina suplantación de sitios web para capturar datos personales. Esto se relaciona directamente con el artículo 269J del segundo capítulo de la ley, el cual hace referencia a la transferencia no consentida de activos, lo que implica la manipulación de información bancaria con el fin de obtener beneficios económicos sin el consentimiento del propietario de dicha información.

Por último, el artículo 269I del segundo capítulo introduce la conducta ilícita de hurto por medios informáticos y similares. Este delito ocurre cuando una persona, superando medidas de seguridad informáticas, manipula un sistema informático con el propósito de apoderarse de un bien mueble ajeno, con la intención de obtener beneficio económico para sí mismo o para otro. (Elizalde et al, 2021).

En resumen, estos artículos dentro del Código Penal Colombiano abordan diversas formas de delitos cibernéticos, como la violación de datos personales, el phishing, la

transferencia no consentida de activos y el hurto por medios informáticos. Estos delitos buscan proteger la seguridad y la privacidad de la información en el entorno digital.

- **Identificación y descripción de los elementos del delito del tipo penal de violación de datos personales.**

A continuación, se llevará a cabo la identificación y descripción de los elementos del delito establecido en el tipo penal de violación de datos personales, ya que resulta fundamental para las partes involucradas en el proceso comprender la estructura de dicho tipo penal con el fin de evitar posibles afectaciones a la teoría del caso, nulidades o errores en la defensa o acusación. Se considera relevante abordar aspectos como el tipo objetivo y subjetivo, la antijuricidad y la culpabilidad.

De acuerdo con Vega (2016), los tipos penales consisten en una serie de enunciados gramaticales contenidos en las normas penales, los cuales se encuentran ubicados en la parte especial del Código Penal y describen abstractamente comportamientos que vulneran bienes jurídicos. (p. 56).

Según el código penal colombiano, la adecuación típica debe abordarse tanto objetiva como subjetivamente, lo que se conoce como tipo penal complejo. El tipo objetivo se refiere a lo que puede ser percibido por los sentidos y acontece fuera de la mente del sujeto, mientras que el tipo subjetivo se refiere a lo que ocurre dentro de la mente del sujeto, es decir, la relación entre la mente del sujeto y la realización de la conducta. (Vega, 2016).

- ***El sujeto activo***

Se trata de la persona natural o jurídica que comete el delito descrito en la norma, específicamente aquel que lleva a cabo las acciones u omisiones descritas en el tipo penal de violación de datos personales. Este tipo penal es mono subjetivo, ya que su conformación requiere únicamente la participación de un único sujeto activo, aunque no se excluye la posibilidad de que sea realizado por dos o más sujetos activos. El sujeto activo es indeterminado, ya que no requiere una cualidad especial para cometer el delito, pero se contempla una circunstancia agravante si dicho sujeto activo es un funcionario público en ejercicio de sus funciones, lo cual está especificado en el artículo 269H numeral 2. (Ibañez, J, 2021).

- ***Sujeto pasivo***

El sujeto pasivo, en el contexto del derecho penal, se refiere a uno o más individuos legales o naturales que son afectados por la infracción del delito, viendo vulnerado así su derecho legalmente protegido. Es decir, es la parte que sufre el daño por parte del

perpetrador. En el caso del delito de violación de datos personales, el sujeto pasivo puede ser indeterminado, abarcando tanto al Estado Colombiano (como representante de la sociedad), entidades jurídicas como también a individuos particulares. (Ibáñez, J, 2021, p. 12).

- ***Objeto Jurídico:***

El objeto o interés jurídico, según Chanjan et al. (2020), se refiere al bien jurídico protegido por el código penal, definido como el "objeto de protección de cada delito, el cual consiste en los intereses sociales, principios o derechos que se quieren tutelar en cada delito" (p.12). Este bien jurídico protegido se relaciona con la protección de la información y los datos. Este tipo penal básico puede ser pluriofensivo, ya que puede afectar más de un interés jurídico, como el derecho a la intimidad, entre otros. Se trata de un tipo penal resultado de lesión, pues al llevar a cabo la acción de alguno de los verbos rectores se menoscaba o daña el bien jurídico tutelado.

- ***Objeto material.***

El objeto material de este tipo penal puede ser fenomenológico o inmaterial, según lo explica Vega (2016). Vega indica que el objeto material es fenomenológico cuando la conducta descrita en el tipo penal se dirige hacia un fenómeno jurídico que no es una cosa o una persona en sí misma (p.61). En el caso del delito de violación de datos personales, el objeto material consiste en datos personales y códigos contenidos en archivos, ficheros, bases de datos u otros medios similares.

- ***Verbos rectores:***

Este tipo penal presenta verbos rectores compuestos, alternativos o disyuntivos, ya que cualquier acción que se ejecute constituye el delito. Además, estos verbos rectores están separados por comas (,) o por la letra "o". En el caso específico de la violación de datos personales (artículo 269F), los verbos rectores de mera conducta son los siguientes: comprar, ofrecer, compilar, emplear, intercambiar, vender, divulgar y enviar. Por otro lado, los verbos rectores de resultado son: obtener, sustraer, interceptar y modificar. (Ley 1273, 2009).

En el delito de violación de datos personales, se incluyen circunstancias que agravan la pena, las cuales se detallan en el artículo 269H de la Ley 599 (2000):

> Artículo 269H. circunstancias de agravación punitiva. Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
>
> 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de Otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

- ***Imputación objetiva:***

Según la imputación objetiva, no se consideran prohibidos aquellos comportamientos o conductas que están socialmente permitidos, como el uso de sistemas informáticos y dispositivos electrónicos. Sin embargo, cuando el sujeto activo traspasa los límites de lo socialmente aceptado, generando así un riesgo jurídico desaprobado para el propietario de los datos personales y códigos, el titular no debe haber autorizado al sujeto activo para que dicho riesgo jurídico exista. Existe causalidad cuando se comete el delito a través de verbos rectores de mera conducta, como emplear, ofrecer, intercambiar, vender, enviar, comprar, divulgar y compilar, o mediante verbos rectores de resultado, como obtener, sustraer, interceptar y modificar. El vínculo causal se establece cuando las acciones u omisiones relacionadas con los verbos rectores tienen una conexión o incidencia directa con el resultado de la violación de códigos y/o datos personales privados, semiprivados o sensibles contenidos en archivos, ficheros, bases de datos o medios similares. (Ibañez, J, 2021, p. 15).

No obstante, según Aguirre (2020), se ha reconocido la necesidad de actualizar la teoría del delito en relación con los delitos o crímenes informáticos. En la actualidad, la imputación objetiva se basa en el nexo causal, el cual se considera insuficiente y generador de inseguridad jurídica, ya que tradicionalmente se ha requerido una conducta física y tangible junto con un resultado externo para atribuir responsabilidad al sujeto. Sin embargo, esto no sería aplicable a los delitos informáticos, que son virtuales y no se manifiestan físicamente. Por lo tanto, se propone utilizar el nexo lógico en tipos penales como la violación de datos personales, que implica la interacción entre un mandato emitido y la respuesta del sistema, lo

que conduce a la manipulación y obtención de los datos personales, generando así un riesgo jurídicamente desaprobado. Este concepto se conoce como interacción IN PUT - OUT PUT.

El resultado implica un cambio fenomenológico en el mundo exterior, aunque en este caso se refiere al mundo virtual. Para que esto ocurra, es necesario que exista una causalidad, es decir, la acción del sujeto al llevar a cabo alguno de los verbos rectores mencionados en el artículo 269F, estableciendo así un vínculo con el resultado que implica el cambio fenomenológico de violar códigos y/o datos personales privados, semiprivados o sensibles contenidos en archivos, ficheros, bases de datos o medios similares.

El delito de violación de datos personales es de resultado permanente para algunos de los verbos rectores, ya que el sujeto activo puede continuar lesionando el bien jurídico tutelado en el tiempo según su voluntad. Esto significa que el sujeto activo puede mantenerse en el tiempo realizando los verbos rectores del artículo 269F, como obtener, sustraer, interceptar y modificar códigos y datos personales. Además, existen verbos rectores de mera actividad o conducta, como ofrecer, compilar, vender, comprar, emplear, intercambiar, divulgar y enviar, los cuales no admiten tentativa. (Ibañez, J, 2021).

- ***Tipo Subjetivo***

En cuanto al tipo subjetivo, el delito de violación de datos personales solo puede cometerse mediante la modalidad de la conducta dolosa. Esto se debe a que el código penal no especifica expresamente otras modalidades de conducta, como la culpa o la preterintencional, para este delito, de acuerdo con el artículo 21 del código penal. Para que exista dolo en este delito, el sujeto activo debe tener conocimiento, comprensión o dominio de los hechos constitutivos y desear realizarlos, o haber previsto su probabilidad o posibilidad, dejando su realización al azar. En este delito, no hay elementos adicionales al dolo, como el ánimo, la intención o el propósito. (Ibañez, J, 2021, p.17).

La antijuridicidad se entiende en dos sentidos: formal y material. En su sentido formal, implica un juicio de valor negativo sobre una conducta (acción u omisión) que viola la normativa penal. No toda conducta está en contra de la normativa penal; por lo tanto, en su sentido material, la antijuridicidad se fundamenta en la lesión o puesta en peligro real de uno o más bienes protegidos por la ley penal, sin una causa justificada. Es decir, para que exista antijuridicidad material, el acto no debe estar amparado por ninguna de las causales de ausencia de responsabilidad establecidas en el artículo 32 del código penal. (Salgado, 2020).

> Artículo 32. ausencia de responsabilidad. No habrá lugar a responsabilidad penal cuando:
>
> 1. En los eventos de caso fortuito y fuerza mayor.

2. Se actúe con el consentimiento válidamente emitido por parte del titular del bien jurídico, en los casos en que se puede disponer del mismo.

3. Se obre en estricto cumplimiento de un deber legal.

4. Se obre en cumplimiento de orden legítima de autoridad competente emitida con las formalidades legales. No se podrá reconocer la obediencia debida cuando se trate de delitos de genocidio, desaparición forzada y tortura.

5. Se obre en legítimo ejercicio de un derecho, de una actividad lícita o de un cargo público. 6. Se obre por la necesidad de defender un derecho propio o ajeno contra injusta agresión actual o inminente, siempre que la defensa sea proporcionada a la agresión. Se presume la legítima defensa en quien rechaza al extraño que, indebidamente, intente penetrar o haya penetrado a su habitación o dependencias inmediatas.

7. Se obre por la necesidad de proteger un derecho propio o ajeno de un peligro actual o inminente, inevitable de otra manera, que el agente no haya causado intencionalmente o por imprudencia y que no tenga el deber jurídico de afrontar
El que exceda los límites propios de las causales consagradas en los numerales 3, 4, 5, 6 y 7 precedentes, incurrirá en una pena no menor de la sexta parte del mínimo ni mayor de la mitad del máximo de la señalada para la respectiva conducta punible.

8. se obre bajo insuperable coacción ajena.

9. Se obre impulsado por miedo insuperable.

10. Se obre con error invencible de que no concurre en su conducta un hecho constitutivo de la descripción típica o de que concurren los presupuestos objetivos de una causal que excluya la responsabilidad. Si el error fuere vencible la conducta será punible cuando la ley la hubiere previsto como culposa.
Cuando el agente obre en un error sobre los elementos que posibilitarían un tipo penal más benigno, responderá por la realización del supuesto de hecho privilegiado.

11. Se obre con error invencible de la licitud de su conducta. Si el error fuere vencible la pena se rebajará en la mitad.
Para estimar cumplida la conciencia de la antijuridicidad basta que la persona haya tenido la oportunidad, en términos razonables, de actualizar el conocimiento de lo injusto de su conducta.

12. El error invencible sobre una circunstancia que diere lugar a la atenuación de

la punibilidad dará lugar a la aplicación de la diminuente. (Ley 599, 2000).

Las causales de justificación son situaciones en las que la realización de un delito, como el establecido en el artículo 269F del Código Penal, está permitida debido a que está respaldada por el legislador al entrar en conflicto con otros intereses, los cuales pueden tener prioridad en circunstancias particulares. Por ejemplo, un fiscal que investiga un delito y, para ello, lleva a cabo acciones de indagación e investigación, sujetas a control previo o posterior por parte del juez de garantías contra un individuo. Estas acciones implican obtener códigos y/o datos personales. La actuación del fiscal y otros colaboradores se justifica mediante causales como la 3, 4 y 5, dependiendo del caso específico, lo que conlleva a la ausencia de antijuridicidad material como consecuencia. (Ibáñez, 2021).

Según la sentencia C – 181 de 2016, la culpabilidad se define de la siguiente manera:

La culpabilidad es aquel juicio de reproche sobre la conducta del actor que permite imponer una sanción penal a su acción típica y antijurídica. Tiene como fundamento constitucional la consagración del principio de presunción de inocencia y el avance hacia un derecho penal del acto, conforme al artículo 29 Superior. En ese sentido, el desvalor se realiza sobre la conducta del actor en relación con el resultado reprochable, más no sobre aspectos internos como su personalidad, pensamiento, sentimientos, temperamento entre otros. Conforme a lo anterior, está proscrita cualquier forma de responsabilidad objetiva, pues la base de la imputación es el juicio de reproche de la conducta del sujeto activo al momento de cometer el acto. Por último, la culpabilidad permite graduar la imposición de la pena de manera proporcional, puesto que el análisis no se agota en la verificación del dolo, la culpa o la preterintencion, sino que, además, debe tenerse en cuenta el sentido específico que a la acción u omisión le imprime el fin perseguido por el sujeto. (Corte Constitucional, sentencia C 181, 2016).

Para que una conducta sea considerada culpable, es necesario que el sujeto activo sea imputable, tenga conciencia de la antijuricidad y se le pueda exigir un comportamiento diferente. En el caso del presente delito, esto ocurre cuando se realiza un juicio de reproche o evaluación sobre la conducta del sujeto, quien tiene la capacidad de comprender y querer el carácter injusto de su acción. Es decir, el sujeto es consciente de que al realizar ciertos actos incurre en el delito de violación de datos personales según el artículo 269F del código penal, pero aun así decide llevar a cabo la conducta, teniendo la opción de actuar de manera diferente. En consecuencia, si una conducta es antijurídica, típica y culpable, es punible y merecedora de una pena.

Sin embargo, pueden existir condiciones de imputabilidad disminuida o inimputabilidad. La primera se presenta cuando el sujeto sufre de un trastorno que no le impide comprender la ley penal ni lo hace incapaz frente a ella, pero sí disminuye su capacidad de autodeterminación o comprensión de la ley penal. En estos casos, se debería considerar como un atenuante de la pena. Ejemplos de esto pueden ser la pobreza extrema, la ira intensa y el dolor, la ignorancia o la marginalidad, según lo establecido en los artículos 56 y 57 del código penal, (Ospina, 2018).

La segunda condición es la inimputabilidad, que ocurre cuando el sujeto sufre de condiciones como trastorno mental, inmadurez psicológica o diversidad sociocultural, entre otros estados similares. Esto significa que el sujeto no comprende la capacidad ilícita de su conducta y carece de la capacidad de autodeterminación. En consecuencia, una conducta inimputable es punible si es antijurídica y típica, y si se comprueba la ausencia de causales de irresponsabilidad, como el error de tipo y de prohibición. Por esta razón, se le impone al sujeto una medida de seguridad según lo establecido en el artículo 69 del código penal, con el fin de proteger y rehabilitar al individuo. (Ibáñez, 2021 p. 20).

En conclusión, el análisis presentado en este capítulo refleja la complejidad y relevancia del delito de violación de datos personales en el contexto actual de la era digital. La dogmática penal de este delito, tipificado en el artículo 269F del Código Penal Colombiano, muestra cómo la legislación ha evolucionado para proteger un bien jurídico fundamental: la información personal. Esta protección es esencial no solo para salvaguardar la privacidad de los ciudadanos, sino también para garantizar el respeto a sus derechos fundamentales frente a nuevas amenazas tecnológicas.

2.3 Marco normativo colombiano sobre la protección de datos personales, Ley Estatutaria 1581 de 2012, identificando las similitudes y diferencias con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea,

El presente capítulo tiene como objetivo establecer el marco normativo colombiano sobre la protección de datos personales, con especial atención a la Ley Estatutaria 1581 de 2012. Esta ley, que regula la protección de datos personales en Colombia, se analizará en comparación con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, considerado uno de los estándares más rigurosos a nivel global. A lo largo del capítulo, se identificarán las similitudes y diferencias entre ambas normativas, con el fin de resaltar las convergencias en principios fundamentales y las divergencias en cuanto a enfoques, obligaciones y derechos. Este análisis permitirá estableceré el grado de alineación

entre la normativa colombiana y los estándares internacionales, así como las posibles áreas de mejora para fortalecer el régimen de protección de datos en Colombia.

2.3.1 Legislación colombiana sobre la protección de datos personales

La Constitución Política de Colombia, en su Artículo 15, establece el derecho fundamental de las personas a conocer, actualizar, retirar y rectificar su información personal, resaltando la importancia de garantizar las libertades individuales en todos los procesos relacionados con los datos personales. Según Calle (2009), la Corte Constitucional ha liderado el desarrollo del artículo 15, ampliando los conceptos de datos personales y los derechos derivados de su tratamiento a través de su jurisprudencia.

A pesar de varios intentos, no se logró la aprobación de proyectos de ley que buscasen regular integralmente el tratamiento de datos personales. No fue sino hasta el año 2008 que se promulgó la Ley 1266, como señala García (2015), la cual aborda el derecho de habeas data y la gestión de información o datos personales en el ámbito financiero y crediticio.

La mencionada ley, como su título lo sugiere, establecía disposiciones generales sobre el habeas data y regulaba el tratamiento de la información contenida en bases de datos personales, especialmente aquella de naturaleza financiera, crediticia, comercial, de servicios y proveniente de terceros países. A lo largo de esta normativa, se introdujeron definiciones precisas y se establecieron una serie de principios fundamentales, tales como el principio de veracidad o calidad de los registros o datos, el principio de finalidad, el principio de circulación restringida, el principio de temporalidad de la información, el principio de interpretación integral de derechos constitucionales, el principio de seguridad y el principio de confidencialidad.

Se reconoce la trascendencia de esta normativa como piedra angular en la consagración del derecho fundamental al habeas data, así como en la estructuración de todos los procesos relacionados con la recolección y tratamiento de la información. Esta legislación establece de manera precisa los derechos de los titulares de la información y los procedimientos para realizar reportes negativos a las centrales de riesgo, entre otros aspectos relevantes. (Gil, 2017)

Posteriormente, en 2012, se promulga la Ley 1581, cuyo alcance es aún más amplio. Chaparro (2014) subraya la importancia de los principios consagrados en esta ley, como la definición de los derechos de los titulares de la información para conocer, actualizar, rectificar y retirar sus datos personales de las bases de datos tanto públicas como privadas.

Además, se establecen reglas fundamentales, como la necesidad de obtener la autorización del titular por medios válidos para almacenar y procesar datos personales

(Galvis, 2012). Asimismo, se establece la obligación de informar al titular sobre cómo se tratará la información y con qué propósito se llevará a cabo dicho tratamiento.

Es evidente, entonces, que esta normativa aborda una gama mucho más amplia de aspectos en materia de protección de datos en comparación con la Ley 1266 de 2008.

En el ámbito de la reglamentación de la Ley 1581 de 2012, se emitió el Decreto 1377 de 2013, normativa que establece claramente que la recolección de datos personales debe realizarse en consonancia con la finalidad establecida por la persona natural o jurídica encargada de recopilarlos. Según Cubillos (2017), salvo en situaciones excepcionales contempladas por la Ley, es imperativo obtener la autorización expresa del titular de los datos para su recolección.

Además, este decreto establece límites temporales para el almacenamiento de datos, los cuales deben ajustarse al principio de razonabilidad y necesidad, tal como señala Sánchez (2015). Este principio se fundamenta en la garantía del derecho a la intimidad, el cual ostenta un carácter fundamental según lo establecido en la Constitución Política de 1991.

Es importante destacar que la Superintendencia de Industria y Comercio ha desplegado un amplio trabajo en relación con la protección de datos personales. A través de guías prácticas, esta entidad ha delineado las obligaciones impuestas a las entidades, tanto públicas como privadas, responsables de la recolección y tratamiento de datos personales. Este enfoque práctico contribuye a una mejor comprensión y aplicación de las normativas en materia de protección de datos, promoviendo así el cumplimiento efectivo de las disposiciones legales en esta área.

La "Guía sobre el tratamiento de datos personales para fines de marketing y publicidad", elaborada por la Superintendencia de Industria y Comercio (2019), ofrece una perspectiva integral sobre la protección de datos en el contexto de las nuevas tecnologías de la información, el comercio electrónico y el marketing digital. Dentro de este compendio, destaca el concepto de responsabilidad demostrada, el cual representa un pilar fundamental para garantizar la adecuada gestión de la información personal.

La noción de responsabilidad demostrada implica que quienes se encargan de recopilar y procesar datos personales adopten medidas concretas orientadas a proteger dicha información. En este sentido, las empresas y entidades públicas deben comprometerse en la implementación de medidas necesarias, útiles, efectivas, oportunas y eficientes para cumplir con las obligaciones legales establecidas en materia de protección de datos y el derecho al habeas data.

En consonancia con lo anterior, Recio (2017) subraya la importancia primordial de la responsabilidad demostrada en el ámbito de la protección de datos personales. Este principio asegura que la recopilación, el tratamiento y la transferencia de información personal se realicen conforme a las normativas vigentes, al tiempo que se adoptan medidas efectivas para salvaguardar la privacidad de los individuos involucrados.

Las directrices elaboradas por la Superintendencia de Industria y Comercio no solo representan una guía esencial para las organizaciones en la gestión de datos personales, sino que también reflejan un compromiso claro con la protección de la privacidad y la seguridad de la información. Estas directrices, al estar diseñadas de manera específica para adaptarse a las distintas finalidades de la recolección de datos, ofrecen un marco integral que aborda no solo la recolección y el almacenamiento de datos, sino también las medidas necesarias para garantizar su seguridad y confidencialidad.

En este sentido, es imperativo destacar el papel activo de Colombia en la promoción de estándares de protección de datos a nivel iberoamericano. La participación en la formulación de estos estándares no solo demuestra el liderazgo de Colombia en la región, sino que también evidencia su compromiso con el establecimiento de principios éticos y legales sólidos en el tratamiento de datos personales. Dichos estándares, como señala Maqueo y colaboradores (2017), no solo consolidan la normativa existente, sino que también amplían su alcance al abordar aspectos específicos como el derecho a la indemnización y los criterios para la cooperación internacional en materia de protección de datos.

Esta colaboración regional en la definición de estándares de protección de datos no solo contribuye a fortalecer la seguridad jurídica y la confianza de los ciudadanos en el manejo de sus datos, sino que también promueve la armonización de prácticas y la colaboración entre países en la lucha contra la ciberdelincuencia y el abuso de la información personal. En un entorno globalizado y digitalizado, donde las fronteras son cada vez más permeables, la cooperación internacional en materia de protección de datos se vuelve crucial para garantizar la privacidad y la seguridad de los individuos en el ámbito digital.

En el ámbito de la protección de datos personales en el contexto del comercio electrónico, es necesario reconocer que la ausencia de una ley específica ha dejado un vacío normativo que requiere atención. Si bien no existe una legislación concreta que aborde este tema de manera integral, es relevante mencionar que se han realizado alusiones al respecto en documentos CONPES relacionados con el big data y el comercio electrónico. Estos documentos, aunque no proporcionan una regulación detallada, sí evidencian la importancia y la necesidad de abordar la protección de datos en el entorno digital. (Barrera, 2021).

Por otro lado, la intervención de la Superintendencia de Industria y Comercio a través de la emisión de directrices es fundamental en la definición de pautas para la recolección, almacenamiento y gestión de datos personales en canales y plataformas electrónicas. Estas directrices sirven como un marco de referencia para las empresas y entidades involucradas en el comercio electrónico, proporcionando lineamientos claros sobre las prácticas adecuadas para garantizar la privacidad y seguridad de los datos de los usuarios.

En este sentido, la guía publicada por la Superintendencia de Industria y Comercio, (2020) subraya la necesidad de que todos los actores en la cadena de valor del comercio electrónico realicen una evaluación exhaustiva de los datos a los que tendrán acceso durante las transacciones. Esta evaluación no solo implica considerar la relevancia y sensibilidad de los datos, sino también identificar y mitigar posibles riesgos asociados con su recolección y tratamiento. Asimismo, la guía enfatiza la importancia de implementar medidas sólidas de seguridad y privacidad para proteger la información personal de los usuarios (Superintendencia de Industria y Comercio, 2020).

2.3.2. La adecuación de la regulación colombiana en la protección de datos en el ámbito del comercio y los canales digitales

En Colombia, se ha establecido una normativa que regula la protección de datos personales, la cual abarca de manera general las responsabilidades tanto de entidades públicas como privadas en relación con el tratamiento, gestión y almacenamiento de dicha información, así como los derechos de los individuos sobre sus datos personales.

En este contexto, las obligaciones de los responsables del tratamiento de datos personales incluyen una serie de acciones como la conservación de la prueba de autorización del titular, la creación de una política de protección de datos personales de acceso público y la documentación de los procedimientos relacionados con la protección de datos, entre otras. Estas obligaciones se aplican no solo a entidades tradicionales, sino también a aquellas plataformas y empresas que operan en el ámbito del comercio electrónico, así como a los terceros que actúan en su nombre. (Barrera, 2021)

Esta extensión de responsabilidades ha sido delineada en la guía establecida por la Superintendencia de Industria y Comercio en 2017 en relación con la protección de datos en el comercio electrónico. Esta guía proporciona directrices claras sobre cómo las empresas que operan en el entorno digital deben cumplir con las obligaciones legales en materia de protección de datos, asegurando así la integridad y seguridad de la información personal de los usuarios (Superintendencia de Industria y Comercio, 2017).

Actualmente, carecemos de una legislación específica que, a través de una identificación exhaustiva de la cadena de valor en las transacciones de comercio electrónico, establezca responsabilidades claras para todos los actores involucrados. Además, la falta de un procedimiento de inspección, vigilancia y control específico para este ámbito deja aspectos fundamentales desprotegidos en lo que respecta a la regulación del comercio electrónico. (Barrera, 2021)

A pesar de que podemos encontrar disposiciones dispersas en diversas normativas, como el estatuto del consumidor o regulaciones sobre identificación electrónica, estas no están consolidadas en una norma o decreto específico que regule de manera integral la protección de datos en el contexto del comercio electrónico. Dichas normas, aunque existentes en el ordenamiento jurídico colombiano, se centran en regular otras áreas distintas al comercio electrónico, lo que crea un vacío normativo en este importante ámbito.

Es crucial resaltar que, reconociendo la importancia de establecer una regulación específica en el ámbito del comercio electrónico, en 2010 se aprobó el Documento CONPES 3620 sobre "Lineamientos de política para el impulso del comercio electrónico en Colombia". Este documento se enfoca en acciones concretas destinadas a promover el desarrollo del comercio electrónico en el país. Sin embargo, advierte sobre la existencia de vacíos normativos en esta área, así como de barreras que obstaculizan el crecimiento y posicionamiento de plataformas y canales digitales.

Además, en 2019 se emitió el Documento CONPES 3975 titulado "Política nacional para la transformación digital e inteligencia artificial". Aunque este documento introduce algunas nociones sobre la cadena de valor del comercio electrónico, no se centra específicamente en la regulación necesaria para proteger a todas las partes involucradas en las transacciones electrónicas (Martínez, 2019). Estas iniciativas reflejan el reconocimiento por parte del gobierno de la importancia del comercio electrónico y la necesidad de abordar cuestiones regulatorias para su crecimiento y desarrollo en el país.

Además, es importante resaltar que la publicación del borrador del Documento CONPES sobre comercio electrónico en 2020 fue una respuesta directa a las debilidades evidenciadas durante los "días sin IVA". Estos eventos revelaron la fragilidad de las plataformas electrónicas ante un aumento repentino y significativo en el tráfico de usuarios, lo que generó una serie de problemas técnicos y operativos.

Sin embargo, es preocupante observar que, a pesar de la atención prestada a estas deficiencias, aún persiste una falta de énfasis en la protección de datos personales en el ámbito del comercio electrónico. Este aspecto es de vital importancia, ya que la seguridad y

privacidad de la información de los usuarios son fundamentales para garantizar la confianza y el buen funcionamiento del comercio digital.

En este contexto, resulta relevante mencionar las experiencias internacionales que han abordado de manera específica y efectiva la regulación de la protección de datos en el comercio electrónico. Estos casos ofrecen lecciones valiosas sobre cómo diseñar marcos normativos sólidos que protejan los derechos de los usuarios y promuevan un entorno seguro y confiable para las transacciones en línea. (Barrera, 2021).

Para concluir, el delito de violación de datos personales, establecido en el artículo 269F del Código Penal Colombiano, refleja la creciente necesidad de adaptar el derecho penal a los desafíos que plantea la era digital. La evolución de los delitos informáticos ha obligado a los legisladores a proteger bienes jurídicos novedosos, como la información personal, que en la actualidad constituye un derecho fundamental en el marco de una sociedad cada vez más interconectada. La regulación de este tipo de conductas delictivas no solo busca sancionar a quienes vulneran la privacidad y los datos de las personas, sino también fortalecer la protección de los derechos individuales frente al uso indebido de tecnologías avanzadas. Así, el ordenamiento jurídico colombiano, al integrar este delito, se alinea con la tendencia global de otorgar mayor importancia a la seguridad digital y a la integridad de los datos personales, garantizando así una mayor protección en un entorno en constante transformación tecnológica.

2.3.3 Análisis comparativo de la legislación colombiana sobre la protección de datos personales, con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, con el fin de identificar similitudes, y diferencias.

Este aparado, ofrece un análisis comparativo entre el marco regulatorio de la protección de datos personales en Europa y Colombia. Se pretende identificar y analizar las principales instituciones y diferencias en ambos regímenes, destacando la importancia de entender el estándar europeo, que es más exigente y avanzado que el colombiano. Para ello se tendrá en cuenta nueve aspectos a comparar: La extraterritorialidad, el concepto de dato personal, las bases legales para el tratamiento de datos personales, los principios en el tratamiento de datos personales, los derechos de los interesados para la protección de sus datos personales, brechas de seguridad en los datos personales, transferencia internacional de los datos personales, los actores relevantes, delegados de protección de datos personales, autoridad de protección de datos personales y por ultimo las sanciones.

- ***Extraterritorialidad:***

El Reglamento General de Protección de Datos (GDPR) fue pionero en establecer el cumplimiento extraterritorial de sus normativas, seguido por leyes similares en lugares como California, con la Ley de Privacidad del Consumidor de California (CCPA), y Brasil. A continuación, se detallan las condiciones que cada una de estas normas impone:

- **Reglamento General de Protección de Datos (GDPR)**

El artículo 3, numeral 2, del GDPR establece que este reglamento se aplica al tratamiento de datos personales de residentes de la Unión Europea (UE) por parte de un responsable o encargado fuera de la UE, siempre que el tratamiento esté relacionado con:

- La oferta de bienes o servicios a personas en la Unión Europea, sin importar si se les requiere pago.
- El monitoreo del comportamiento de ciudadanos de la Unión Europea dentro de su territorio.
- Esto significa que una empresa colombiana, aunque no tenga presencia en Europa, estaría sujeta al GDPR si:
- Ofrece bienes o servicios a residentes de la Unión Europea (por ejemplo, a través de una página web dirigida a ciudadanos europeos).
- Realiza actividades de tratamiento de datos personales que implican el control del comportamiento de ciudadanos de la UE (como el rastreo de cookies o la creación de perfiles de usuarios).
- Además, el artículo 27 del GDPR requiere que, si un responsable o encargado del tratamiento de datos no tiene sede en la Unión Europea, debe designar por escrito a un representante dentro de la UE. Esta obligación no aplica si el tratamiento de datos es ocasional y no incluye categorías especiales de datos personales (como datos sensibles). Este representante es responsable de responder a las consultas de las autoridades de control y de los titulares de datos sobre asuntos relacionados con el tratamiento de sus datos personales (Reglamento General de Protección de Datos de la Union europea, 2016).

Nuestra legislación no contempla la extraterritorialidad. De hecho, cuando se promulgó la ley 1581 (2012), no existía una normativa global que abordara este tema. La extraterritorialidad se incorporó posteriormente con el reglamento europeo, diseñado para un

contexto en el que los servicios pueden prestarse desde cualquier lugar del mundo. No obstante, es importante destacar que, debido a este aspecto y a la transferencia internacional de datos personales desde países europeos, es esencial comprender la regulación europea.

- ***El concepto de Dato personal***

El concepto de dato personal en el Reglamento General de Protección de Datos (RGPD) es considerablemente más amplio que el definido en la legislación colombiana. Según el RGPD, no es necesario que una persona esté identificada por su nombre y apellido para que la información sea considerada como dato personal. Si los datos asociados permiten crear un perfil específico o aislar comportamientos, esa información ya se considera personal, incluso si no se sabe exactamente de quién se trata.

Este enfoque rompe con la idea de que para identificar a una persona se necesitan sus datos explícitos como nombres o identificación. En el contexto de internet, mecanismos como las cookies, direcciones IP o huellas digitales pueden aislar a un usuario específico sin necesidad de conocer su identidad exacta. Según el artículo 4 del RGPD, se considera información personal cualquier dato que permita identificar, directa o indirectamente, a una persona física, ya sea a través de un nombre, un número de identificación, datos de localización, o identificadores en línea, entre otros. (Escuela de privacidad, 2020)

El RGPD también pone especial énfasis en la elaboración de perfiles, utilizando datos personales para evaluar comportamientos y adaptar tratamientos específicos según el interés del responsable de los datos. Por ejemplo, un portal de comercio electrónico no necesita saber el nombre o la identificación de un usuario para enviarle publicidad; con el perfil creado a partir de su comportamiento en el sitio, esa información se considera ya como dato personal.

En contraste, la legislación colombiana requiere que la información permita identificar a la persona en mayor o menor medida, a partir de la combinación de varios datos personales. La Ley 1581 de 2012 clasifica los datos en públicos, semiprivados, privados y sensibles, según su nivel de divulgación aceptable. Aunque la normativa colombiana sigue un enfoque más tradicional, la Corte Constitucional ha señalado que los datos personales deben identificar a una persona en cierta medida, pero no necesariamente al mismo nivel que lo hace el modelo europeo.

- ***Bases legales para el tratamiento de datos personales***

Las bases legales para el tratamiento de datos personales son los fundamentos que lo legitiman. En Colombia, solo se reconoce una base legal, que es el consentimiento o la autorización explícita del titular de los datos. En cambio, el Reglamento General de

Protección de Datos (RGPD) de Europa contempla seis bases legales, donde el consentimiento es solo una de ellas y tiene la misma importancia que las demás. Estas bases incluyen el consentimiento, la ejecución de un contrato, el cumplimiento de obligaciones legales, la protección de intereses vitales, el interés legítimo y el interés público.

Aunque la ley colombiana establece que el consentimiento es la única base legal, el artículo 10 de la Ley 1581 (2012), introduce excepciones donde no se requiere el consentimiento, como en casos de información solicitada por entidades públicas, datos públicos, urgencias médicas, tratamientos para fines históricos, estadísticos o científicos, y datos relacionados con el Registro Civil.

Es crucial no confundir estas excepciones con las bases legales del RGPD, ya que son contextos diferentes. Además, el RGPD exige que las bases legales se informen previamente al interesado, y el responsable debe justificar la base legal utilizada para evitar sanciones.

- ***Los principios en el tratamiento de datos personales***

El Reglamento General de Protección de Datos (2016), introduce principios novedosos para el tratamiento de datos personales, aunque es importante reconocer la labor de la Corte Constitucional en Colombia, que ha establecido principios adicionales no contemplados en la legislación. A continuación, se presentan los principales principios del RGPD y cómo se comparan con la visión colombiana:

- **Principio de licitud, lealtad y transparencia**: Estos tres principios están integrados en uno solo. La licitud exige que el tratamiento de datos esté basado en una justificación legal, alineándose con el principio de legalidad en Colombia. La lealtad implica que los datos se usen de acuerdo con los fines previamente informados y que no se haga un uso desleal que pueda perjudicar al titular, lo cual está relacionado con el principio de finalidad en Colombia, aunque no se menciona explícitamente. La transparencia, reconocida tanto en el RGPD como en la legislación colombiana, es un derecho del titular y una obligación del responsable, que debe garantizarse en todo momento del tratamiento.
- **Principio de limitación de la finalidad**: Este principio establece que los datos personales solo deben tratarse para los fines explícitos y legítimos para los que fueron recogidos, considerando también la evolución de esos fines en el contexto de internet. Si surgen nuevas finalidades, estas deben comunicarse al interesado, asegurando que cumplan con ciertos criterios. En caso de incompatibilidad con la finalidad inicial, se debe obtener nuevo consentimiento del titular. En Colombia, existe un principio

similar llamado de finalidad, aunque sin la palabra "limitación" y sin el mismo nivel de desarrollo que en el RGPD. Sin embargo, ambos comparten el objetivo de asegurar que los datos se utilicen solo para los fines autorizados por el titular.

- ***Derechos de los interesados para la prpoteccion de sus datos personales***

En la legislación europea, los derechos de protección de datos personales mantienen los mismos fundamentos que la normativa anterior, similares a los derechos ARCO en la legislación colombiana: Acceso, Rectificación, Oposición y Cancelación (ahora denominado Supresión del Dato o derecho al olvido). Sin embargo, el Reglamento General de Protección de Datos (2016), introduce tres nuevos derechos no contemplados en la legislación colombiana:

1. **Limitación del Tratamiento**: Permite a los interesados solicitar que sus datos personales no sean utilizados, aunque se conserven. Este derecho puede ejercerse cuando se duda de la exactitud de los datos, cuando el interesado prefiere que los datos no se eliminen, cuando los datos ya no son necesarios para el responsable, pero el interesado los desea conservar, o cuando el interesado se opone al tratamiento. El RGPD sugiere métodos como trasladar datos a otro sistema, restringir el acceso, o retirar datos de internet temporalmente.
2. **Derecho a la Portabilidad de Datos**: Ofrece a los interesados la capacidad de recibir sus datos personales en un formato estructurado y de uso común, y de transferir esos datos a otro responsable cuando el tratamiento se realice por medios automatizados, siempre que el consentimiento del interesado o la ejecución de un contrato respalde el tratamiento.
3. **Derecho a no ser objeto de decisiones automatizadas**: Garantiza que las personas no sean sometidas a decisiones automáticas que tengan efectos legales significativos sobre ellas, como la elaboración de perfiles. Este derecho exige que cualquier decisión automatizada pueda ser revisada por una persona con la autoridad para ajustar o cambiar dicha decisión.

Adicionalmente, el RGPD incluye el Derecho de Información, que está presente también en la legislación colombiana, pero con una descripción más detallada en el RGPD, abarcando aspectos específicos sobre cómo y cuándo debe proporcionarse esta información.

Brechas de seguridad de los datos personales

l Reglamento General de Protección de Datos (2016), y la legislación colombiana regulan los incidentes de seguridad en el tratamiento de datos personales, pero presentan diferencias y similitudes en sus enfoques.

- **En el RGPD**:

- **Notificación a la Autoridad**: Debe realizarse dentro de las 72 horas siguientes a la detección de una brecha de seguridad. Si el plazo no se cumple, se deben explicar las razones del retraso.
- **Notificación al Interesado**: Si la violación representa un alto riesgo para los derechos y libertades de las personas, se debe informar al interesado sin demora.
- **Exención de Notificación**: No es necesario notificar a la autoridad si la violación no supone un riesgo para los derechos y libertades de las personas.
- **Responsabilidad del Encargado**: Está obligado a informar al responsable en caso de brechas de seguridad.

- **En la legislación colombiana**:
  - **Notificación a la Autoridad**: Debe realizarse dentro de los 15 días hábiles posteriores a la detección de la brecha. No se especifica un mecanismo para justificar retrasos.
  - **Notificación al Interesado**: Aunque la ley colombiana no exige explícitamente la notificación al titular, esto está recomendado en la Guía de Responsabilidad Demostrada.
  - **Exención de Notificación**: Aunque no se menciona explícitamente, es razonable suponer que una brecha sin impacto en datos personales no requeriría notificación.
  - **Responsabilidad del Encargado**: No está claramente estipulada en la legislación, pero se sugiere en la Guía de Gestión de Incidentes incluir esta obligación en los contratos de transmisión de datos.

Mientras el RGPD proporciona directrices más detalladas y específicas para la notificación y gestión de incidentes de seguridad, la legislación colombiana ofrece un marco general que también aborda estas situaciones, aunque con algunos procedimientos y tiempos diferentes.

- ***Brechas de seguridad de los datos personales***

El Reglamento General de Protección de Datos (2016), regula los incidentes de seguridad en los artículos 33 y 34, estableciendo la obligación de notificar a la autoridad de protección de datos y al interesado, así como los plazos de notificación. En caso de brechas de seguridad, la notificación debe realizarse a más tardar 72 horas después de haber tenido constancia del incidente. Si se notifica fuera de este plazo, es necesario justificar el motivo del retraso.

En Colombia, la legislación obliga al responsable a informar a la autoridad cuando hay violaciones a los códigos de seguridad que afecten los datos personales, con un plazo de 15 días hábiles para notificar al Registro Nacional de Bases de Datos (RNBD). Sin embargo, la ley no establece ninguna sanción ni procedimiento en caso de retraso en la notificación, a diferencia del RGPD. (Escuela de Privacidad, 2020).

En cuanto a la necesidad de notificación, el RGPD permite eximir al responsable de notificar si la violación no representa un riesgo para los derechos de los afectados. En Colombia, no se menciona explícitamente, pero es razonable aplicar una lógica similar.

En relación con la comunicación al interesado, el RGPD obliga a informar sin dilación si la brecha supone un riesgo alto. En Colombia, aunque no está formalmente legislado, la Guía de Responsabilidad Demostrada recomienda informar al titular, permitiéndole tomar medidas para minimizar el impacto. Además, el RGPD impone al encargado de tratamiento la obligación de notificar al responsable cualquier incidente, mientras que en Colombia esta obligación no está regulada, aunque se recomienda incluirla en los contratos.

El Reglamento General de Protección de Datos (2016), ha sido pionero en la aplicación extraterritorial de sus normativas, seguido por la Ley de Privacidad del Consumidor de California (CCPA) y la legislación brasileña. En cuanto al RGPD, su artículo 3 establece que se aplica al tratamiento de datos de residentes de la Unión Europea (UE) por responsables fuera de la UE cuando el tratamiento está vinculado con la oferta de bienes o servicios o el monitoreo de comportamientos en la UE. Esto implica que una empresa colombiana que no opere físicamente en Europa puede estar sujeta a este reglamento si, por ejemplo, ofrece servicios o productos a ciudadanos de la UE (Reglamento General de Protección de Datos de la Union europea, 2016).

El concepto de "dato personal" en el RGPD es más amplio que en la legislación colombiana. El RGPD considera como dato personal cualquier información que permita identificar, directa o indirectamente, a una persona física, incluso sin conocer su identidad precisa, a través de medios como cookies o direcciones IP (RGPD, 2016). En Colombia, los datos personales se clasifican de manera más tradicional, requiriendo una combinación de varios elementos para identificar a la persona (Ley 1581 de 2012).

En cuanto a las bases legales para el tratamiento de datos personales, el RGPD reconoce seis, mientras que en Colombia solo se permite el consentimiento explícito del titular, con excepciones bajo circunstancias específicas, como en el caso de datos públicos o emergencias médicas (Ley 1581 de 2012; RGPD, 2016).

Respecto a los principios que guían el tratamiento de los datos, el RGPD introduce la "licitud, lealtad y transparencia", que obliga a garantizar que el tratamiento sea legal, justo y transparente. Estos principios son comparables a la legislación colombiana, que incorpora principios como la finalidad, pero sin el mismo nivel de desarrollo que en el RGPD (Corte Constitucional de Colombia, 2013).

En cuanto a los derechos de los interesados, el RGPD expande los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) de la legislación colombiana, añadiendo el derecho a la "limitación del tratamiento", la "portabilidad de datos" y el derecho a "no ser objeto de decisiones automatizadas", garantizando una mayor protección de los datos personales (Escuela de privacidad, 2020).

Finalmente, en cuanto a la gestión de brechas de seguridad, el RGPD establece plazos estrictos para notificar tanto a la autoridad como a los interesados en caso de que ocurra un incidente, mientras que en Colombia la notificación tiene un plazo de 15 días hábiles y no contempla sanciones por demoras (RGPD, 2016; Ley 1581 de 2012).

- ***Transferencia Interacional de Datos Personales***

En el ámbito colombiano, la transferencia y transmisión internacional de datos personales se rige por requisitos y procedimientos específicos:

- **Transferencia Internacional (Controller to Controller):**
  - **Consentimiento del Titular**: Se debe obtener la autorización del titular de los datos (Art. 9, Ley 1581, 2012).
  - **Países con Nivel Adecuado de Protección**: La transferencia debe hacerse a países que figuren en la lista de países con protección adecuada (numeral 3.2, Capítulo 3, Título V, Circular Única de la SIC). Si el país no está en la lista, se deben seguir excepciones según el Art. 26, Ley 1581 (2012), aunque siempre se requiere el consentimiento del titular. Además, se puede solicitar una Declaración de Conformidad a la SIC y registrar la transferencia en el Registro Nacional de Bases de Datos (RNBD).
  - **Contrato entre Controladores**: Incluso si el país tiene un nivel adecuado de protección, se debe firmar un contrato entre los controladores.
- **Transmisión Internacional (Controller to Processor):**
  - **Contrato de Transmisión**: No se requiere el consentimiento del titular ni la notificación previa si existe un contrato de transmisión de datos con los requisitos legales (Art. 24 y 25, D. 1377/13). Si no se firma un contrato, se debe obtener el consentimiento del titular o cumplir con los parámetros para la transferencia.

- **Registro en el RNBD**: La transmisión debe ser registrada en el RNBD.
- **Información al Titular**: No existe una normativa específica para informar al titular sobre la transmisión internacional de datos, pero se debe proporcionar información en las políticas internas y avisos de privacidad.

- **RGPD (Reglamento General de Protección de Datos):**

  Transferencias Internacionales:

- Permitidas a países con un nivel adecuado de protección declarado por la Comisión Europea, incluyendo los miembros de la Unión Europea.
- Si el país no tiene una decisión de adecuación, se deben aportar garantías adecuadas para proteger los derechos de los interesados.

- **Excepciones**:
  - Existen excepciones en situaciones como el consentimiento explícito del interesado, incapacidad del interesado para consentir, transferencias desde registros públicos, o cuando las transferencias no son repetitivas y afectan a un número limitado de personas.

Así las cosas, mientras que la normativa colombiana y el RGPD regulan de manera detallada la transferencia y transmisión internacional de datos, el RGPD ofrece un marco más flexible y adaptado a situaciones específicas con mayores garantías para los interesados. (Escuela de privacidad, 2020)

- ***Actores Relevantes***

El RGPD introduce novedades significativas en cuanto a los actores involucrados en el cumplimiento de la protección de datos personales, que tienen algunas diferencias y similitudes con la legislación colombiana:

1. Responsable y Encargado:
   - En el RGPD, el responsable es quien decide los fines y medios del tratamiento de los datos personales, mientras que el Encargado procesa los datos en nombre del responsable. Estas definiciones coinciden en esencia con las de la legislación colombiana, aunque el RGPD proporciona una definición más detallada del responsable.
2. Representante del Encargado y del responsable:

El RGPD establece la figura del representante para organizaciones que no tienen presencia física en la Unión Europea, pero están obligadas a cumplir con el reglamento. Estas organizaciones deben designar un representante en la UE por escrito. Esta figura no tiene un equivalente específico en la legislación colombiana.

3. Corresponsable:

   El Corresponsable en el RGPD se refiere a dos o más responsables que determinan conjuntamente los objetivos y medios del tratamiento de datos. Aunque esta figura no está explícitamente definida en la legislación colombiana, la Superintendencia de Industria y Comercio (SIC) ha reconocido su existencia en la práctica. Por ejemplo, en resoluciones relacionadas con Facebook Colombia SAS, la SIC determinó que Facebook y su filial en Colombia son corresponsables del tratamiento de datos personales de los usuarios colombianos en la red social.

- ***Delegados de protección de datos personales***

El Reglamento General de Protección de Datos (RGPD) introduce formalmente el rol del delegado de Protección de Datos (DPD), definido en sus artículos 37, 38 y 39. Este DPD es obligatorio para ciertos organismos y empresas, especialmente aquellas que realizan observaciones sistemáticas a gran escala o manejan categorías especiales de datos, como los relacionados con condenas penales.

En comparación, la legislación colombiana, a través del Decreto 620 de 2020, no menciona específicamente la figura del delegado de Protección de Datos. En cambio, requiere que los responsables y encargados del tratamiento designen una persona o área para gestionar la protección de datos personales, conforme a la Guía de Responsabilidad Demostrada de la Superintendencia de Industria y Comercio (SIC). Esta figura en Colombia se conoce como Oficial de Protección de Datos (OPD) y su función se centra en garantizar el cumplimiento de las normativas de protección de datos, responder a consultas y reclamos, y supervisar las políticas internas de protección de datos.

El RGPD detalla una serie de obligaciones para el DPD, como informar y asesorar sobre el cumplimiento del reglamento, supervisar su aplicación, y actuar como punto de contacto con la autoridad de control. La Guía de Responsabilidad Demostrada de la SIC, aunque no menciona un DPD, establece roles y responsabilidades similares para el OPD, con el objetivo de asegurar la implementación efectiva de las políticas de protección de datos en la organización. (Escuela de privacidad, 2020).

- ***Autoridad de protección de datos personales***

Suecia fue pionera al establecer la figura de la "Autoridad de Protección de Datos Personales" en su legislación mediante la ley 289 (1973). Posteriormente, Alemania, Francia y Reino Unido siguieron su ejemplo. En 2001, el Convenio 108 incorporó un Protocolo Adicional que exigía a las partes designar autoridades de control de protección de datos. La Directiva 95/46/CE, introducida después, obligó a los Estados miembros a crear autoridades independientes para la protección de datos personales, una disposición que también está regulada en el RGPD en los artículos 51 y siguientes.

- **Características clave del RGPD en relación con las autoridades de control:**

Independencia: Las autoridades de control deben ser independientes tanto del poder público como del sector privado. Según el artículo 52 del RGPD, deben operar con total autonomía en el desempeño de sus funciones y el ejercicio de sus poderes.

Periodicidad**:** El RGPD establece que el mandato de los miembros de la autoridad de control debe ser de al menos cuatro años, con posibilidad de renovación. Los países pueden fijar períodos más largos y decidir cuántas veces se puede renovar el mandato. En Colombia, el período también es de cuatro años, pero el cargo es de libre nombramiento y remoción, lo que no garantiza la duración del mandato. (Escuela de privacidad, 2020).

Funciones: Tanto la autoridad de control europea como la colombiana tienen funciones similares, como velar por el cumplimiento de la legislación de protección de datos, imponer sanciones, y supervisar y controlar el cumplimiento de la ley. Sin embargo, el RGPD también asigna funciones adicionales a las autoridades de control que no están contempladas en la legislación colombiana, como ofrecer asesoramiento en operaciones de tratamiento de datos, fomentar mecanismos de certificación, elaborar códigos de conducta, adoptar cláusulas contractuales tipo, y aprobar normas corporativas vinculantes.

- ***Sanciones:***

El Reglamento General de Protección de Datos (RGPD) establece criterios detallados para la imposición de sanciones en materia de protección de datos personales. Los factores que se consideran incluyen:

- Naturaleza, gravedad y duración de la infracción.
- Alcance o propósito de la operación de tratamiento.
- Número de personas afectadas y el nivel de daños sufridos.
- Intencionalidad o negligencia en la infracción.

- Medidas tomadas por el responsable o encargado para mitigar los daños.
- Grado de responsabilidad del responsable o encargado, considerando las medidas técnicas u organizativas aplicadas.
- Cooperación con la autoridad de control para remediar la infracción y mitigar sus efectos.
- Categorías de datos afectados por la infracción.
- Forma en que la autoridad de control conoció la infracción, especialmente si fue notificada por el responsable o encargado.
- Adhesión a códigos de conducta o mecanismos de certificación.
- Factores agravantes o atenuantes aplicables.
- Beneficios financieros obtenidos o pérdidas evitadas a través de la infracción.

El RGPD también garantiza que las personas afectadas por daños materiales o inmateriales puedan recibir una indemnización del responsable o encargado. Las acciones legales deben ser interpuestas ante los tribunales competentes del país respectivo.

En Colombia, las multas pueden llegar hasta el equivalente de 2,000 salarios mínimos mensuales legales vigentes, un monto que algunos consideran insuficiente como factor disuasorio. Las sanciones se gradúan considerando:

- Dimensión del daño o peligro a los intereses jurídicos protegidos por la ley.
- Beneficio económico obtenido por el infractor o terceros.
- Reincidencia en la comisión de la infracción.
- Resistencia, negativa u obstrucción a la investigación o vigilancia por parte de la Superintendencia de Industria y Comercio.
- Renuencia o desacato a las órdenes impartidas por la Superintendencia.
- Reconocimiento o aceptación expresa de la infracción antes de la imposición de la sanción. (Escuela de privacidad, 2020).

En suma, la Ley Estatutaria 1581 de 2012 de Colombia y el Reglamento General de Protección de Datos (GDPR) de la Unión Europea presentan un marco común en términos de los principios básicos para la protección de datos personales, como la legalidad, transparencia y seguridad. Sin embargo, existen diferencias significativas en cuanto a la robustez y alcance de cada normativa. Mientras el GDPR impone obligaciones más estrictas y detalladas, como la designación obligatoria del delegado de Protección de Datos (DPD) y el principio de extraterritorialidad, la legislación colombiana carece de ciertos mecanismos de supervisión y control que podrían fortalecer su aplicación.

Estos contrastes evidencian la necesidad de ajustar y modernizar el régimen colombiano para alinearse más con los estándares internacionales, brindando así una mayor protección a los derechos de los titulares de datos en un entorno globalizado y digital. La aproximación a los lineamientos del GDPR ofrece una oportunidad para mejorar el marco normativo colombiano y asegurar una mejor gestión de los datos personales.

A continuación, se presenta un cuadro comparativo que detalla las similitudes y diferencias entre la legislación colombiana, específicamente la Ley 1581 de 2012, y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, promulgado en 2016.

Tema	Legislación Colombiana (Ley 1581 de 2012 y decretos complementarios)	Reglamento General de Protección de Datos (RGPD)
Extraterritorialidad	No contempla el principio de extraterritorialidad.	Aplicable a empresas fuera de la UE si tratan datos de ciudadanos de la UE o monitorean su comportamiento (Art. 3.2). Además, requiere designar un representante en la UE (Art. 27).
Concepto de dato personal	Define dato personal como aquel que identifica a una persona directamente o mediante la combinación de varios datos.	Amplio concepto de dato personal: cualquier información que permita identificar, directa o indirectamente, a una persona física (Art. 4), incluyendo identificadores en línea como IP o cookies.
Bases legales para el tratamiento	Requiere consentimiento explícito del titular para el tratamiento de datos personales.	Contempla seis bases legales, entre ellas el consentimiento, ejecución de un contrato, cumplimiento de

Tema	Legislación Colombiana (Ley 1581 de 2012 y decretos complementarios)	Reglamento General de Protección de Datos (RGPD)
	Existen algunas excepciones (Art. 10).	obligaciones legales, protección de intereses vitales, interés público y legítimo (Art. 6).
Principios en el tratamiento de datos	Contempla principios como legalidad, finalidad, veracidad, acceso y circulación restringida, seguridad, confidencialidad (Art. 4).	Introduce principios de licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación de almacenamiento, integridad y confidencialidad (Art. 5).
Derechos de los interesados	Derechos ARCO: Acceso, Rectificación, Cancelación y Oposición (Art. 8).	Añade nuevos derechos: portabilidad de datos, limitación del tratamiento, y derecho a no ser objeto de decisiones automatizadas (Art. 15-22).
Brechas de seguridad	Notificación a la autoridad dentro de 15 días hábiles (RNBD). No se establece plazo específico para notificación a los titulares (Guía de Responsabilidad Demostrada).	Notificación a la autoridad dentro de las 72 horas siguientes (Art. 33), y al interesado sin demora si existe un alto riesgo (Art. 34).
Transferencia internacional de datos	Requiere consentimiento del titular y se permite solo a países con nivel adecuado de protección o con excepciones (Art. 26).	Transferencias permitidas a países con nivel adecuado de protección o mediante garantías como cláusulas contractuales tipo.

Tema	Legislación Colombiana (Ley 1581 de 2012 y decretos complementarios)	Reglamento General de Protección de Datos (RGPD)
		Excepciones para situaciones específicas (Art. 44-49).
Actores relevantes	Responsable y encargado del tratamiento (Art. 2). No se contempla la figura del representante ni del corresponsable de datos, pero algunos roles se infieren de la normativa y resoluciones de la SIC.	Introduce el corresponsable, el representante de responsables y encargados fuera de la UE, y otros actores clave (Art. 26-30).
Delegado de protección de datos	No contempla un delegado de Protección de Datos (DPD), pero sí requiere la designación de una persona o área encargada de la protección de datos personales (Decreto 620 de 2020).	Requiere la designación de un DPD para ciertos tratamientos de datos a gran escala o sensibles (Art. 37-39).
Autoridad de protección de datos	Superintendencia de Industria y Comercio (SIC) como autoridad de control. Funciones incluyen sanciones, registro de bases de datos, inspecciones y auditorías (Art. 19-21).	Autoridades independientes de protección de datos en cada Estado miembro con funciones similares a las de la SIC, pero con mayor autonomía y capacidad de emitir directrices (Art. 51-59).
Sanciones	Sanciones impuestas por la SIC, que varían dependiendo de la infracción (Art. 23, Ley 1581/2012).	Sanciones administrativas pueden llegar hasta el 4% de la facturación global anual de una empresa

Tema	Legislación Colombiana (Ley 1581 de 2012 y decretos complementarios)	Reglamento General de Protección de Datos (RGPD)
		o 20 millones de euros, lo que sea mayor (Art. 83).

Fuente propia

3. Formulación de hipótesis

Dada la creciente importancia de la protección de datos personales en el contexto digital, la adopción de medidas específicas en Colombia contribuye significativamente al fortalecimiento de la protección de datos y a la prevención y reducción del delito establecido en el artículo 269F del Código Penal. Se espera que la identificación de la caracterización dogmática penal del delito de violación de datos personales, el análisis de las limitaciones e insuficiencias de la Ley Estatutaria 1581 de 2012, así como el estudio comparativo de la legislación colombiana con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, permitan formular recomendaciones concretas para fortalecer la legislación y las regulaciones vigentes en el país. Estas medidas podrían mejorar la efectividad de la protección de datos personales y contribuir a la lucha contra el delito de violación de datos en Colombia.

3.1 Categorías:

Para comprender adecuadamente el fenómeno de los delitos informáticos, es fundamental explorar diversas categorías que permiten estructurar y entender este tipo de conductas ilícitas. A lo largo del análisis, se abordarán conceptos clave como la definición y naturaleza de los delitos informáticos, sus implicaciones legales y los bienes jurídicos que buscan proteger. Además, se examinará la clasificación de los datos personales según la normativa colombiana vigente, la cual distingue entre datos públicos, semiprivados y privados, con el objetivo de proporcionar una visión integral sobre la protección de la información en el entorno digital.

- **Delitos informáticos o cibernéticos**

Los delitos informáticos, o crímenes cibernéticos, se definen como aquellas acciones u omisiones que son consideradas típicas, antijurídicas y culpables cuando se dirigen contra organismos gubernamentales, entidades jurídicas o individuos. Estas conductas se llevan a cabo mediante el uso de sistemas informáticos, y su objetivo es generar un daño a la víctima, ya sea a través de la lesión directa o poniendo en riesgo bienes jurídicos protegidos. Estas acciones pueden buscar un beneficio personal o para terceros, sin importar si dicho beneficio es patrimonial o personal, ni si se realiza con fines lucrativos o no (Huerta; Libano, 1998, citado en Acurio Del Pino, 2016).

- **La delincuencia informática:**

La delincuencia informática abarca cualquier acto o conducta ilícita que pueda ser clasificada como criminal, destinada a alterar, desestabilizar, destruir o manipular algún

sistema informático o sus componentes, con la intención de causar daño o poner en peligro cualquier bien jurídico protegido (Acurio Del Pino, 2016, p. 14).

Por su parte, Ojeda et al. (2010) proporcionan una definición distinta de los delitos informáticos, señalando que estos se refieren a cualquier comportamiento ilícito, ya sea por acción u omisión, en el que una persona utiliza un recurso informático y como resultado afecta un bien jurídico informático o material protegido legalmente, lo que conlleva responsabilidad penal (p. 51).

Con base en las definiciones mencionadas, se puede afirmar que los delitos informáticos implican conductas punibles realizadas tanto por acción como por omisión, que son típicas, antijurídicas y culpables. Estas acciones son ejecutadas por individuos con conocimientos técnicos en informática, telemática u otros campos afines. Tales conductas suponen el uso indebido de medios informáticos con el fin de modificar, destruir, manipular, obtener, interceptar o divulgar información, o bien para sustraer sistemas o componentes informáticos. El fin de estas acciones es obtener un beneficio, ya sea personal o para un tercero, causando daño o poniendo en riesgo bienes jurídicos o materiales protegidos del sujeto pasivo.

- **Datos personales**

En cuanto a los datos personales, la Ley Estatutaria 1266 de 2008 en Colombia define los datos personales como cualquier tipo de información que pueda vincularse a una o varias personas identificadas o identificables, o que esté asociada a una persona natural o jurídica. Los datos que no son personales no están sujetos a las disposiciones de protección de datos de dicha ley. Se presume que cuando la ley menciona un "dato", se refiere al uso de datos personales. Los datos personales pueden clasificarse en tres categorías: públicos, semiprivados y privados.

- **Datos públicos**

Los datos públicos son aquellos calificados como tales por la ley o la Constitución, y abarcan información contenida en documentos públicos, sentencias judiciales ejecutoriadas no sometidas a reserva, y datos relacionados con el estado civil de las personas.

- **Datos semiprivados y privados:**

Los datos semiprivados son aquellos que no son íntimos ni reservados, pero cuyo conocimiento puede interesar tanto al titular como a un sector de la sociedad, como los datos financieros o crediticios. Por último, los datos privados son aquellos de naturaleza íntima o reservada, relevantes únicamente para el titular de estos.

- **Concepto de violación de datos personales en Colombia**

En Colombia, el delito de violación de datos personales fue incorporado al Código Penal mediante el artículo 269F, introducido por la Ley 1273 de 2009. Esta norma sanciona a quien, sin autorización, obtenga, sustraiga, modifique, o divulgue datos personales contenidos en archivos, bases de datos u otros medios similares, ya sea con beneficio propio o de terceros. La pena para esta conducta es de 48 a 96 meses de prisión, junto con una multa que varía entre 100 y 1000 salarios mínimos legales mensuales vigentes (Ley 1273, 2009).

Este delito se considera una conducta punible que vulnera la protección de la información y los datos personales, independientemente de si los datos son privados, semiprivados, públicos o sensibles, e incluye la apropiación de códigos personales, que son claves para el acceso seguro a los datos. La finalidad del sujeto activo es obtener un provecho propio o para terceros, lo que conlleva un perjuicio sobre los bienes jurídicos protegidos del titular de los datos (Ibañez, 2021).

4. Marco Metodológico:

4.1 Línea de investigación

El trabajo de investigación descrito se enmarca en la Línea 02: Estado, sociedad y cultura, ya que aborda problemáticas sociales y públicas relacionadas con la protección de datos personales en el contexto del derecho penal en Colombia. Esta línea de investigación se centra en comprender las tensiones y desafíos que surgen al implementar los derechos a nivel nacional e internacional, así como en analizar cómo estos derechos afectan a diferentes grupos dentro de la sociedad.

En particular, el estudio se enfoca en la intersección entre el derecho penal, la protección de datos y la regulación nacional e internacional en materia de privacidad. Al analizar el delito establecido en el artículo 269F del Código Penal colombiano, que trata sobre la violación de datos personales, y proponer medidas para prevenir y reducir este tipo de delito, el trabajo busca abordar una problemática relevante en la sociedad contemporánea.

Además, al llevar a cabo un estudio comparativo entre la legislación colombiana sobre protección de datos y las regulaciones de otros países, incluyendo el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, el estudio no solo proporciona un análisis exhaustivo de la situación nacional, sino que también contextualiza el problema dentro de un marco internacional más amplio.

4.2. formas de investigación

Es fundamental resaltar que este estudio se sitúa dentro del ámbito teórico, también referido como investigación especulativa según lo planteado por Primo Yúfera (1994). En

esta modalidad de investigación, se hace uso del pensamiento y procesos mentales tales como la imaginación, la intuición, la abstracción y la deducción para crear modelos, explicaciones o teorías sobre fenómenos que no son observables directamente.

4.3. Método de la investigación:

Según Vázquez (2010), el enfoque deductivo implica la inferencia lógica de conclusiones específicas a partir de principios universales o premisas generales. En este proceso, se parte de afirmaciones amplias o principios generales y se aplican reglas de inferencia lógica para alcanzar conclusiones más concretas o específicas. Este método es ampliamente utilizado en la lógica y en el razonamiento matemático, donde se emplea para demostrar teoremas y establecer relaciones entre proposiciones. La característica sobresaliente del enfoque deductivo radica en su capacidad para garantizar la verdad de las conclusiones siempre que las premisas iniciales sean verdaderas y las reglas de inferencia sean válidas. En síntesis, el método deductivo proporciona un marco lógico para la argumentación y la demostración, permitiendo la validación de conclusiones a partir de premisas generales.

4.4 Paradigma de la investigación

Cabe mencionar por otra parte que la investigación realizada tiene un enfoque cualitativo, con una orientación disciplinar socio jurídica, que busca hallar la solución al problema planteado en el presenta trabajo de investigación.

4.5 Tipo de la investigación

La presente investigación es de tipo tanto explicativo, dado que, se realiza la descripción de una problemática social a partir de la definición de conceptos y situaciones del fenómeno que se está investigando, y por otro lado se explican las causas que llevan a la realización de la problemática social que se encuentra presente en la actualidad.

Hernández Sampieri (1997) señala que los estudios explicativos van más allá de simplemente describir conceptos o fenómenos, así como de establecer relaciones entre ellos, al adentrarse en la búsqueda de las causas que subyacen a los eventos físicos o sociales. Este tipo de investigación se enfoca en entender por qué ocurre un fenómeno y en qué condiciones se presenta, así como en explicar las relaciones entre dos o más variables. Por ejemplo, mientras que un estudio descriptivo podría revelar las intenciones del electorado antes de una elección, y un estudio correlacional podría relacionar estas intenciones con variables como la edad y el sexo de los votantes, la magnitud de la propaganda política y los resultados de elecciones anteriores, un estudio explicativo profundizaría al investigar por qué algunas

personas votarán por un candidato específico y otras por diferentes candidatos, y qué factores influyen en esa decisión.

4.6 Técnica de recolección de la información

La técnica de recolección de la información que se utiliza en la actual investigación es la técnica de análisis documental, toda vez que se ha recopilado la teoría necesaria para llevar a feliz término el trabajo, de esta manera se ha recopilado la norma, la jurisprudencia y los diferentes documentos pertinentes, con ellos se lograra el cotejo y análisis de la información que se ha reunido.

Según Peña (2007), el análisis documental se concibe como un procedimiento ideado por el individuo para estructurar y presentar el conocimiento contenido en los documentos, los cuales pueden ser tan numerosos que excedan la capacidad de lectura y comprensión. Este proceso se centra en examinar y condensar la información contenida en tales documentos, aplicando principios lingüísticos para identificar el contenido esencial que puede asociarse a términos específicos o conjuntos de ellos, ya sea de manera individual o en estructuras discursivas.

5. Conclusiones

A partir de la hipótesis planteada, se concluye que la protección de datos personales en Colombia debe ser una prioridad, especialmente en un entorno digital que evoluciona rápidamente. La caracterización dogmática del delito de violación de datos personales, en conjunto con el análisis crítico de la Ley Estatutaria 1581 de 2012, revela limitaciones significativas que afectan la efectividad de las medidas de protección actuales. Al comparar la legislación colombiana con el GDPR de la Unión Europea, se identifican estándares y prácticas que pueden ser adoptados para mejorar la situación en el país.

La evolución de los delitos informáticos ha estado estrechamente ligada al avance de la modernidad y al crecimiento exponencial de las tecnologías de la información y las comunicaciones. En un mundo cada vez más interconectado, donde la sociedad contemporánea depende en gran medida de la tecnología, los delitos informáticos, especialmente aquellos relacionados con la violación de datos personales, han surgido como una preocupación significativa.

Es evidente que nos encontramos en una era de globalización y tecnología, donde las herramientas tecnológicas están integradas en todos los aspectos de la vida cotidiana, desde lo social y cultural hasta lo laboral y económico. Sin embargo, este avance también ha dado lugar a nuevos desafíos, especialmente en lo que respecta a la protección de la información personal y la seguridad digital.

La naturaleza transnacional de estos delitos implica que no se limitan a las fronteras de un solo país, sino que pueden ser perpetrados desde cualquier lugar del mundo con acceso a Internet o sistemas informáticos. Esta realidad plantea desafíos únicos para la regulación y el cumplimiento de la ley en un entorno digital en constante cambio.

En Colombia, la regulación de los delitos informáticos se ha convertido en una prioridad, reconociendo el riesgo que representan para los derechos humanos, la seguridad nacional y la estabilidad económica. La adopción del Convenio sobre Ciber-criminalidad de Budapest y la promulgación de leyes nacionales reflejan el compromiso del país con la protección de la seguridad digital y los derechos individuales en un entorno digitalizado.

Es fundamental comprender que los delitos informáticos no solo representan una amenaza para la seguridad digital, sino que también tienen implicaciones significativas en términos de derechos individuales y protección de datos personales. Por lo tanto, es responsabilidad del Estado regular y sancionar estas conductas ilícitas, así como garantizar la confidencialidad, integridad y disponibilidad de los sistemas informáticos y datos.

La introducción del delito de violación de datos personales en el marco jurídico colombiano, a través del artículo 269F del Código Penal por la Ley 1273 (2009), representa un hito importante en la protección de la información y la seguridad digital en el país. Esta disposición legal establece claramente las conductas punibles relacionadas con la obtención, modificación, divulgación y uso no autorizado de datos personales, así como los códigos personales, con consecuencias penales significativas que van desde la prisión hasta multas sustanciales.

La violación de datos personales se define como una conducta típica, antijurídica y culpable, perpetrada por el sujeto activo sin el consentimiento del titular, utilizando medios informáticos o telemáticos para acceder, modificar, divulgar o utilizar datos personales contenidos en sistemas informáticos. Esta acción no solo afecta la privacidad y seguridad de los individuos, sino que también constituye una infracción a los derechos fundamentales consagrados en la Constitución Política de Colombia.

En el ámbito constitucional, la protección de datos personales se encuentra respaldada por el artículo 15, que reconoce el derecho de todas las personas a la protección de sus datos personales, y el artículo 20, que garantiza la libertad de expresión y difusión, ambos pilares fundamentales para salvaguardar la seguridad y privacidad en el entorno digital.

Además, la legislación colombiana ha evolucionado para abordar diferentes formas de delitos informáticos, como el acceso abusivo a sistemas informáticos, sabotaje informático, interceptación ilegítima de datos, daño informático, malware, phishing, transferencia no

consentida de activos y hurto por medios informáticos. Estas disposiciones legales buscan proteger la integridad de la información y los sistemas informáticos en un mundo cada vez más digitalizado

La comprensión de los elementos del delito de violación de datos personales es esencial para todas las partes involucradas en el proceso legal. La identificación y descripción detallada de estos elementos, tanto objetivos como subjetivos, así como la consideración de la antijuricidad y la culpabilidad, permiten una aplicación justa y eficaz de la ley en casos relacionados con la violación de la privacidad y la seguridad de la información.

Desde el punto de vista objetivo, se identifica al sujeto activo como aquel que realiza las acciones u omisiones descritas en el tipo penal, sin excluir la posibilidad de la participación de múltiples sujetos activos. Por otro lado, el sujeto pasivo abarca tanto al Estado como a entidades jurídicas y personas naturales que sufren el daño de la infracción.

El objeto jurídico protegido es la seguridad y privacidad de la información y los datos personales, siendo este tipo penal pluriofensivo al afectar diversos intereses jurídicos. Los verbos rectores, tanto de mera conducta como de resultado, describen las acciones que constituyen el delito.

La imputación objetiva establece que el sujeto activo debe traspasar los límites socialmente aceptados generando un riesgo jurídico desaprobado, lo cual se relaciona con la teoría de la interacción IN PUT - OUT PUT en delitos informáticos. La causalidad se establece mediante un vínculo directo entre las acciones del sujeto activo y el resultado del delito.

En cuanto al tipo subjetivo, el delito de violación de datos personales se comete solo mediante dolo, sin contemplar otras modalidades de conducta como la culpa o la preterintención.

La antijuridicidad, tanto formal como material, implica un juicio negativo sobre la conducta del sujeto que viola la normativa penal, sin justificación alguna. Las causales de justificación pueden excluir la antijuridicidad material en ciertos casos, como el ejercicio legítimo de funciones investigativas.

La culpabilidad implica un juicio de reproche sobre la conducta del sujeto, quien debe ser imputable y consciente de la antijuridicidad de sus acciones. Se consideran condiciones de imputabilidad disminuida o inimputabilidad en ciertos casos especiales.

la legislación colombiana sobre la protección de datos personales ha evolucionado significativamente en las últimas décadas, especialmente con la promulgación de la Ley 1266 en 2008 y la Ley 1581 en 2012. Estas leyes han establecido un marco legal sólido que

reconoce y protege los derechos fundamentales de los individuos sobre su información personal.

La Ley 1266 sentó las bases para el derecho al habeas data y reguló el tratamiento de datos personales en el ámbito financiero y crediticio, mientras que la Ley 1581 amplió su alcance, abordando una gama más amplia de aspectos relacionados con la protección de datos. Estas leyes han sido complementadas por decretos y guías emitidas por la Superintendencia de Industria y Comercio, que han proporcionado orientación adicional sobre cómo cumplir con las disposiciones legales.

Sin embargo, en el contexto del comercio electrónico, aún existe un vacío normativo que requiere atención. Aunque se han emitido documentos CONPES que reconocen la importancia del comercio electrónico y proponen medidas para su impulso, la falta de una legislación específica que regule integralmente la protección de datos en este ámbito deja aspectos fundamentales desprotegidos.

Es necesario que Colombia avance hacia una regulación más específica y completa en el ámbito del comercio electrónico, que aborde de manera detallada las responsabilidades de todos los actores involucrados y garantice la protección de los datos personales de los usuarios. La experiencia internacional puede ofrecer importantes lecciones sobre cómo diseñar marcos normativos sólidos que promuevan un entorno seguro y confiable para las transacciones en línea, lo que podría ser fundamental para el desarrollo continuo y sostenible del comercio electrónico en el país.

las limitaciones e insuficiencias de la Ley Estatutaria 1581 de 2012, que establece disposiciones generales para la protección de datos personales en Colombia, revelan una serie de desafíos que deben abordarse para garantizar una protección efectiva de la privacidad y la seguridad de la información. A pesar de representar un avance significativo en la regulación de este ámbito crucial, esta legislación enfrenta diversas carencias que requieren atención y acción tanto a nivel nacional como internacional.

En primer lugar, la ausencia de disposiciones extraterritoriales en la Ley Estatutaria 1581 de 2012 se destaca como una limitación importante, especialmente en un mundo cada vez más interconectado y globalizado. La falta de consideración de la naturaleza transfronteriza de los servicios y el tratamiento de datos podría obstaculizar la protección efectiva de los datos personales de los ciudadanos colombianos, especialmente en el contexto de la transferencia internacional de datos.

Además, la rigidez en las bases legales del tratamiento de datos personales en Colombia, donde el consentimiento sigue siendo la principal autorización, contrasta con la

diversidad de bases legales reconocidas en el Reglamento General de Protección de Datos de la Unión Europea. Esta limitación podría afectar la capacidad de las organizaciones para adaptarse a diferentes contextos y necesidades, así como para garantizar un tratamiento adecuado y legal de los datos personales.

Otra área de preocupación es la falta de incorporación de nuevos derechos y principios en la protección de datos, como los establecidos en el Reglamento Europeo, que amplían el alcance y la profundidad de la protección de la privacidad en el entorno digital. La omisión de estos derechos adicionales en la legislación colombiana podría dejar a los ciudadanos colombianos en desventaja en términos de control sobre sus datos personales y protección frente a prácticas invasivas.

Asimismo, la falta de desarrollo y concreción de mecanismos de responsabilidad proactiva en la normativa nacional resalta la necesidad de una mayor claridad y especificidad en la implementación de medidas de protección de datos por parte de las organizaciones. La brecha entre la legislación colombiana y el enfoque europeo en este sentido sugiere la importancia de fortalecer las disposiciones normativas y los mecanismos de supervisión para garantizar un tratamiento responsable y ético de los datos personales.

La definición limitada de datos personales en la Ley Estatutaria 1581 de 2012 refleja una visión tradicional que puede no ser adecuada para abordar los desafíos actuales en la protección de la privacidad en línea. La falta de reconocimiento de la amplia gama de información que puede identificar o vincular a una persona en el contexto digital podría limitar la eficacia de la legislación colombiana en la protección de la privacidad en entornos cada vez más complejos y sofisticados.

Si bien la Ley Estatutaria 1581 de 2012, representa un avance significativo en la protección de datos personales en Colombia, sus limitaciones e insuficiencias plantean desafíos importantes que deben abordarse para garantizar una protección efectiva y actualizada de la privacidad y la seguridad de la información en el país. Es fundamental revisar y actualizar la legislación para incorporar disposiciones extraterritoriales, ampliar las bases legales del tratamiento de datos, reconocer nuevos derechos y principios, fortalecer los mecanismos de responsabilidad proactiva y adaptar la definición de datos personales a las realidades cambiantes del entorno digital.

6. Alternativas de solución e intervención socio jurídicas

6.1. Proyecto de ley para modificar la ley colombiana

Como una de las principales alternativas de solución, se plantea la actualización y modificación de la legislación colombiana en lo referente a la protección de datos personales,

específicamente la Ley 1581 de 2012. Con este fin, se está elaborò un proyecto de ley que busca modernizar y fortalecer el marco normativo, alineándolo con los estándares internacionales, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Esta actualización permitirá abordar de manera más efectiva los nuevos desafíos del cibercrimen y la creciente vulnerabilidad de la información personal en el entorno digital.

6.2 participación en el programa radial de la Universidad Colegio Mayor de Cundinamarca

El día 15 de octubre del presente año, en el programa radial de la Universidad Colegio Mayor de Cundinamarca, se socializo lo relacionado al tema de investigación, para que la comunidad en general conociera problemática que se está abordando en el presente trabajo

6.3 Elaboración de un block pedagógico

Se elaboró un block pedagógico con el propósito de educar a la ciudadanía sobre la importancia de la protección de datos personales. Este material educativo tiene como objetivo concientizar a las personas sobre los riesgos actuales que enfrentan sus datos y proporcionarles herramientas prácticas para proteger su información, fomentando así una cultura de seguridad digital y responsabilidad en el manejo de los datos personales.

7.Referencias Bibliográficas

-Acurio Del Pino, S. (2016). Delitos Informáticos: Generalidades, 10 - 20 https://bit.ly/49O1ZOL

-Barrera j, (2021) Regulación sobre protección de datos personales en el mundo digital en el Estado Colombiano. [Tesis de maestria, Universidad libre Catolica de Colombia.] https://bit.ly/3V0WpV2.

-Bechara, Y., Mosquera, A. y 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 [tesis de licenciatura, Facultad de Derecho de la Universidad Cooperativa de Colombia]. https://bit.ly/44hj4iQ

Bonett, E, (2019), Análisis del Bien Jurídico de la Protección de la Información y de los Datos en Colombia a partir de la Ley 1273 de 2009.

-Calle, S. B. (2009). Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia. Precedente. Revista Jurídica. 119-136. https://bit.ly/3V2MdM3

-Cansino, M. (2019). Diez delitos cometidos por medio de redes sociales. Revista Techlandia.

-Chanjan Documet, R., Cabral Mori, E., Janampa Almora, A., & Gonzalez Cieza, M. (2020). Manual Sobre Persecución Penal de Delitos de Corrupción y Técnicas de Investigación periodística. https://bit.ly/3xNsd6O

-Chaparro, M. F. (2014). Legislación informática y protección de datos en Colombia, comparada con otros países. INVENTUM. https://bit.ly/4dIsA2R.

-Congreso de la República de Colombia. (1989 23 de junio). Decreto 1360 Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor. https://bit.ly/4baw501

-Congreso de la República de Colombia. (2000, 24 de julio) Ley 599 del 2000, Código Penal Colombiano https://bit.ly/3SgzEI4

-Congreso de la República de Colombia. (2008 31 de diciembre). Habias data, ley estatutaria 1266, Diario Oficial No. 47.219. https://bit.ly/3Ut2R75

-Congreso de la República de Colombia. (2009 05 de enero). Codigo penal, ley 1273 Diario Oficial No. 47.223. https://bit.ly/44dvcBE

-Congreso de la República de Colombia. (2012, 18 octubre). Ley 1581 Por la cual se dictan disposiciones generales para la protección de datos personales Diario Oficial No. 48.587. https://bit.ly/3X1gDjd.

-Constitución Política de Colombia (1991), Constitucional No. 116. https://bit.ly/3gkhQyI

-Cubillos, Á. (2017). La explotación de los datos personales por los gigantes de internet. Estudios en derecho a la información. https://bit.ly/3UZmZOw.

-Dávila, Y. (2020). Los Delitos Informáticos en el Derecho Colombiano y desde la Perspectiva del Derecho Comparado. Bogotá: Universidad Católica de Colombia.

-Elizalde R, Flores H & Castro H. (2021). Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho comparado, ius Comitiãlis. https://bit.ly/3w4t7eL

-Escuela de privacidad, (2021). Guía comparativa del reglamento general de protección de datos europeo y el régimen colombiano de protección de datos personales. https://bit.ly/4dAVGBv

-Galvis, L. (2012). Protección de datos en Colombia, avances y retos. Revista Lebret, 4(4), 195-214. https://bit.ly/3ydXvnt.

-García E., Y. (2018). Criminalidad en el siglo 21. Editorial Unión.

-García Vargas, C. (2015). La incidencia del modelo español en el registro nacional de bases de datos colombiano como herramienta de supervisión y control. En: J. Becerra, G. D. Flórez Acero, C. García Vargas, C. Rojas Orjuela Vargas, M. E.

-Gil, C. (2017). El debido proceso en la Ley de Habeas Data. Rev. CES Derecho., 8(1), 191-204. https://bit.ly/3ynwZIz

-Grupo de Investigación Seguridad y Delitos Informáticos (Segudelin) (2010). Delitos informáticos y entorno jurídico vigente en Colombia. https://bit.ly/4d9kxfl

-Ibañez, J, (2021) Análisis del tipo penal de violación de datos personales en Colombia. https://hdl.handle.net/10901/20277

-Jescheck, H. H. (1996). Tratado de derecho penal parte general. Perú: Instituto Pacífico

-Koll K., S. (2010). La criminalidad virtual. Editorial BYM.

-La información, el nuevo bien jurídico que crea delitos informáticos en Colombia.1 Information, the new legal right that creates computer crimes in Colombia. Gina Paola López Camacho y Sandy Johanna Salcedo Barrera 2

-Lima, M. de la Luz. (2017). La época de la información y sus delitos. Editorial Universidad del Rosario.

Loredo J. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo.

-Mahecha, B. G. (1963). Curso de derecho penal general. Bogotá D.C.: Lerner Puig, S. M. (1994). Antijuridicidad objetiva y antinormatividad en Derecho Penal. En B. O. estado, & M. d. Justicia (Edits.), Anuario de derecho y ciencias penales

-Martínez Devia, A. (2019). La Inteligencia Artificial, el Big Data y la Era Digital: Una Amenaza para los Datos Personales. Rev. Prop. Inmaterial, 27, 5 https://bit.ly/3UF1a5v.

-Ojeda Pérez, J. E., Rincón Rodríguez, F., Arias Flórez, M. E., & Daza Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. https://bit.ly/49TPxgu

Organización de las Naciones Unidas. Declaración Universal de los Derechos Humanos. 1948

-Ospina Corrales, S. (2018). El Principio de Culpabilidad: Fundamento Constitucional y Alcances de la Norma Rectora del Arículo 12 del Codigo Penal. https://bit.ly/49OYU0X

-Parlamento Europeo y del Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD). https://bit.ly/4bIVvSV.

-Perspectiva criminológica y dogmática de los de los delitos relacionados con el bien jurídico de la información y de los datosJuan José Ospina Grajale 2021pontificia universidad

-Pinilla, S. (2018). Se podría pagar cárcel por ocho años por delitos cibernéticos y cuantiosas multas. Policía Nacional.

-Recio, M. (2017). Big data: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas. Revista de Derecho, Comunicaciones y Nuevas Tecnologías. https://bit.ly/3V31MD6.

-Rivera, A. (1995). Dimensiones de la informática en el derecho. Bogotá.

-Rodríguez A., J.D. (2017). Análisis de los delitos informáticos presentes en las redes sociales en Colombia y su regulación.

-Rueda, A. (2020). La confdencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español. Aragon: Universidad del Gobierno de Aragón

-Salgado González, Á. (2020). Tipicidad y Antijuricidad. Anotaciones Dogmaticas. Revista Juridica https://bit.ly/49Wi30Rç

-Salvatori, D. (2011). Los delitos contra la confidencialidad la disponibilidad y la integridad de los datos y sistemas informáticos. Universidad Católica

-Sánchez Acevedo & J. Torres Ávila. (2014). El derecho y las tecnologías de la información y la comunicación (TIC) (pp. 15-38). Bogotá: Universidad Católica de Colombia. https://bit.ly/3UKTE8X.

Sánchez Acevedo & J. Torres Ávila. El derecho y las tecnologías de la información y la comunicación (TIC) (pp. 101-160). Bogotá: Universidad Católica de Colombia. https://bit.ly/3K19HuD.

-Sánchez Acevedo, M. E. (2015). El régimen de responsabilidad de la Administración Pública colombiana por la publicación de contenidos mediante el uso de las tecnologías de la información y comunicación (TIC). En: J. Becerra, G. D. Flórez Acero, C. García Vargas, C. Rojas Orjuela Vargas, M. E.

-Sánchez D, (2016), Análisis del delito de violación de datos personales (artículo 269f del código penal) desde una perspectiva constitucional, [Tesis de pregrado, Universidad libre seccional Cali.] https://bit.ly/3WcXDhe

-Silva Aguirre, D. (2020). La Imputación Objetiva del Nexo Lógico en el Tipo Penal de Violación de Datos Personales. Revista Estrado. https://bit.ly/49KBkCw

-Superintendencia de Industria y Comercio. (2019). Guía sobre el tratamiento de datos personales para fines de marketing y publicidad. Delegatura Para La Protección De Datos Personales. Publicación Oficial. https://bit.ly/3JZyOxU.

-Vega Arrieta, H. (2016). El análisis gramatical del tipo penal. Justicia https://bit.ly/4b8qaZg

-Velásquez, F. V. (2020). Fundamentos del derecho penal. Bogotá D.C.: Tirant lo Blanch

-Zaffaroni, E. R., Alagia, A., & Slokar, A. (2006). Manual de derecho penal parte general. Buenos Aires: Edlar.