LA RESPONSABILIDAD JURIDICA DEL ESTADO COMO GARANTE DE DERECHOS FUNDAMENTALES, FRENTE A LOS DELITOS INFORMATICOS DE ESTAFA EN LINEA Y ROBO DE DATOS.

THE LEGAL RESPONSIBILITY OF THE STATE AS GUARANTEE OF FUNDAMENTAL RIGHTS AGAINST COMPUTER CRIMES OF ONLINE SCAM AND DATA THEFT.

Erica Tatiana Padilla
Abogada

Corporación Universitaria Remington
Facultad de Ciencias Jurídicas y Políticas
Programa de Derecho
Año 2025.

1. RESUMEN

El Estado colombiano tiene la responsabilidad de proteger los derechos humanos en el ámbito digital mediante prevención, regulación, sanción y reparación frente a ciberdelitos informáticos como la estafa en línea y el robo de datos entre otros. Se ha avanzado en la creación de leyes, instituciones y mecanismos tecnológicos para enfrentar estos delitos, pero se enfrentan desafíos debido a la rápida evolución tecnológica, lo que implica acciones agiles y contundentes del Estado lo que requiere una actualización constante de la normativa, mayor inversión en infraestructura y cooperación internacional para garantizar una protección efectiva.

ABSTRACT

The Colombian State has the responsibility to protect human rights in the digital environment through prevention, regulation, punishment and redress against cybercrimes such as online fraud and data theft, among others. Progress has been made in the creation of laws, institutions and technological mechanisms to deal with these crimes, but challenges are faced due to the rapid technological evolution, which implies agile and forceful actions by the State, which requires constant updating of regulations, greater investment in infrastructure and international cooperation to ensure effective protection.

Palabras clave: Responsabilidad del Estado, Ciberseguridad, Delitos informáticos. Protección de Datos Personales. Robo de Datos. Estafa en línea. Ciberdelincuencia

Keywords: State Responsibility, Cybersecurity, Computer Crimes. Protection of Personal Data. Data Theft. Online scam. Cybercrime

2. INTRODUCCION

El crecimiento exponencial de las tecnologías de la información ha sido la bandera de desarrollo y avance para la humanidad en las últimas décadas pues se han dado grandes cambios y logros en todos los ámbitos de la vida de las personas naturales y jurídicas, hemos aprendido a utilizar nuevas herramientas que sirven para la optimización de la

vida, del que hacer diario, se han acortado las distancias y la comunicación se ha fortalecido.

Al día de hoy tenemos la gran oportunidad de estar conectados e informados en tiempo real, inclusive con lo que ocurre al otro lado del continente, hemos sido afortunados porque la creación de aplicaciones atreves de la internet nos ha facilitado la vida, lo que nos permite hacer y desarrollar distintas gestiones sin necesidad de desplazamientos, bastando la mera conexión.

Situaciones externas tales como la pandemia mundial que se desarrolló en marzo de año 2020, (COVID-19), nos llevaron con mayor rapidez y casi de manera obligada a utilizar aún más las herramientas tecnológicas para continuar con nuestros oficios diarios como, trabajar, estudiar, realizar transacciones, realizar reuniones, socializar, mantener la comunicación y en el ámbito judicial dar trámite y continuidad a los procesos entre otros.

En la era digital nuestros datos son expuestos lo que implica que todo este desarrollo a su vez nos ha llevado a la exposición de nuevos métodos delincuenciales para los cuales no estábamos preparados, ya que la posibilidad de acceder a mayores volúmenes de información, de conectarnos con entornos más allá de nuestros limites, también ha venido a representar una enorme amenaza para nuestra seguridad y privacidad.

El suministro de nuestros datos personales nos hace vulnerables frente a los ciberdelincuentes que mediante distintos métodos ilegales acceden a los bancos de datos de las aplicaciones y las utilizan para ejecutar delitos como la Estafa en línea y Robo de datos, pasamos de ser navegantes digitales consumidores de servicios a victimas de estos delitos que nos afectan de manera personal, económica, social y psicológica.

Por esta razón resulta importante realizar un análisis jurisprudencial del contexto de la responsabilidad jurídica que se le puede atribuir, al Estado Colombiano en el marco de los delitos digitales de Estafa en línea y Robo de datos ya que el Estado tiene el deber de garantizar la seguridad de la privacidad de la información de los ciudadanos de acuerdo a lo establecido en la constitución y le ley, la doctrina y los tratados

internacionales bajo los cuales se establece un bloque de constitucionalidad cuya finalidad es la garantía de los derechos fundamentales, la base principal de la responsabilidad contractual y extracontractual del Estado la encontramos en el artículo 90 de la constitución política de Colombia el cual determina la responsabilidad jurídica del estado y en ella se sostienen las situaciones de acción, omisión o fallas por las cuales el estado deba responder. ¨***ARTÍCULO 90. El Estado responderá patrimonialmente por los daños antijurídicos que le sean imputables, causados por la acción o la omisión de las autoridades públicas.***

En el evento de ser condenado el Estado a la reparación patrimonial de uno de tales daños, que haya sido consecuencia de la conducta dolosa o gravemente culposa de un agente suyo, aquel deberá repetir contra este¨. (Gaceta Constitucional No. 116, 1991)

En este sentido es importante observar que la responsabilidad jurídica del Estado puede radicar en la omisión o en la falta de mecanismos eficientes para mitigar, sancionar y proteger la privacidad de las personas; esto es clave al momento de observar la línea que se ha establecido para brindar una atención integral a las víctimas cuando buscan la ayuda o protección de los entes estatales, cuales son las herramientas efectivas para enfrentar las denuncias por delitos informáticos y que desafíos tienen estas modalidades de delitos para las instituciones y para el Estado mismo.

Podemos ver que en Colombia se han venido desarrollando diferentes mecanismos para hacer frente a las modalidades de delincuencia que han surgido con el uso de las tecnologías, en la sentencia, T-279 DE 2002 (Corte Constitucional, 2002) La (Corte Constitucional, s.f.) enfatizo la obligación del Estado de crear un marco normativo que garantizará el derecho fundamental a la autodeterminación informática, incluyendo

mecanismos de protección los datos personales y regulación de su manejo, protección y divulgación ((Corte Constitucional, s.f.) de Colombia, 05/09/2002)

ESQUEMA DE LA SENTENCIA T-279 DE 2002 (Corte Constitucional, 2002)

T-729/2002	**MAGISTRADO PONENTE**	**Derecho al Habeas Data**	**Contexto Normativo y Jurisprudencial**	**Poder Informático**	**Acceso a Bases de Datos Públicas en Internet**	**Principios para la Gestión de Datos**	**Recomendaciones y Conclusiones**
HABEAS DATA Contenido y alcance HABEAS DATA – Principio de operatividad	Magistrado Ponente: Dr. EDUARDO MONTEALEGRE LYNETT Referencia: expediente T-467467 Acción de tutela instaurada por Carlos Antonio Ruiz Gómez contra el Departamento Administrativo de Catastro (Alcaldía	Reconocido como un derecho fundamental autónomo Relacionado con la autodeterminación informativa Comparte protección con derechos a la intimidad y el buen nombre	Ausencia de ley estatutaria que regule integralmente La Corte ha reiterado y solicitado regulación legislativa La tutela no es suficiente para controlar el poder informático	Definido como dominio social sobre la información Conlleva riesgos: abusos, vulneraciones, manipulación Potencial para afectar derechos: privacida	Casos concretos: acceso mediante digitación de identificación Vulnerabilidad del derecho a la autodeterminación Riesgo de vulnerar seguridad y privacidad	Legalidad Finalidad Veracidad Transparencia Protección de datos sensibles	Necesidad de regulación legal integral Fortalecimiento de mecanismos de protección La protección jurídica debe garantizar la seguridad y privacidad La norma debe equilibrar el poder informático con derechos fundamentales

	Mayor de Bogotá) y la Superintendencia Nacional de Salud. Bogotá D.C., cinco (5) de septiembre de dos mil dos (2002).			d, identidad, igualdad	del ciudadano		

Este artículo se busca exponer algunos de los delitos informáticos puntualmente la Estafa en línea y el Robo de datos personales , frente a los cuales los ciudadanos nos encontramos expuestos ya que a primera vista es difícil identificar la presencia del Estado en cuanto a las garantías de protección que se deberían brindar cuando por la utilización de las tecnologías se convierten en víctimas de delitos que afectan el patrimonio, el entorno y la vida.

3. DEFINICIÓN DEL PROBLEMA

Hablamos de la Responsabilidad jurídica del Estado frente a algunos delitos informáticos, lo que nos convoca en el proceso de investigación es identificar los aspectos y pronunciamientos de las altas cortes frente a los casos en los cuales pueda ser responsable eventualmente el Estado frente a las acciones u omisiones que deba o no ejercer cuando conozca de la comisión de los delitos informáticos de Estafa en línea y Robo de datos, hechos que se generen por el acceso y uso de las tecnologías de la información y el suministro de nuestros datos personales.

También pretendemos realizar un análisis jurídico, que tenga relevancia para evidenciar que la jurisprudencia y las distintas leyes que se han venido desarrollando a la par de los grandes avances tecnológicos y el impacto que genera frente a la vida de las personas que cada día, nos adentramos más en el mundo cibernético y todo lo atractivo que presenta como herramientas que facilitan la vida, pero que a su vez nos expone a una serie de situaciones para las cuales es necesario tener unas garantías del Estado como un deber de brindar seguridad y protección a los ciudadanos en caso de que esto no suceda podríamos entrar a escenarios donde se pueda atribuir una responsabilidad del Estado por acción u omisión.

¿Hasta qué punto podremos decir que se configura una responsabilidad atribuible al Estado y cual responsabilidad seria?

Para dar respuesta a esta pregunta debemos analizar si, se le puede atribuir responsabilidad jurídica al Estado colombiano por delitos informáticos como la estafa y el robo de datos y nos enfrentamos a un entorno complejo, puesto que en general, la responsabilidad del Estado puede estar vinculada a situaciones en las que la acción u omisión haya contribuido al daño causado por estos delitos, o en los que se haya fallado en cumplir con obligaciones de protección de los derechos fundamentales de los ciudadanos en el ámbito digital tales como la autodeterminación, privacidad y seguridad.

De acuerdo a esto pondremos en evidencia algunos entornos donde puede haber Responsabilidad del Estado por Omisión o Fallos en la Protección de Datos, teniendo en cuenta los deberes del estado una de sus características recae sobre las garantías de brindar seguridad y protección a todos los ciudadanos y con el uso de las nuevas tecnologías se vio abocado a emitir e implementar normas que regulen las situaciones que a las que los ciudadanos se exponen con el tratamiento de sus datos.

En tal sentido si no se implementan las medidas suficientes para prevenir y sancionar los delitos informáticos podríamos llegar a un escenario en el que le sea atribuible responsabilidad al Estado por omisión, por no haber realizado las acciones tendientes a la protección del bien jurídico tutelado.

Un ejemplo que podemos aplicar aquí es la Protección de datos personales ya que en Colombia la Ley 1581 de 2012 (Ley 1581, 2012) (Ley 1581, 2012), regula la protección de datos personales, en la cual se determina que el Estado tiene la obligación de

garantizar que las entidades públicas y privadas cumplan con esta ley, no basta solo con la emisión de la ley sino que el Estado debe tomar las medidas necesarias para garantizar la seguridad de los datos personales gestionados por entidades públicas, si el estado no vigila, o no supervisa correctamente a las entidades, se podría configurar una responsabilidad por no proteger adecuadamente los datos personales que custodia frente a robo o acceso no autorizado.

El Estado también puede ser declarado responsable por la Falta de Prevención y Supervisión, esto es, si el Estado no implementa políticas, leyes o regulaciones adecuadas para la prevención de delitos informáticos, como el fraude electrónico o el robo de datos, puede ser considerado responsable por no cumplir con su deber de prevenir el daño mediante la regulación de los posibles delitos que puedan ocurrir, en el caso de Colombia fue regulado esto mediante la legislación, la Ley 1273 de 2009 (Ley 1273, 2009) (Ley 1273, 2009) (Ley de delitos informáticos) que establece la necesidad de proteger a los ciudadanos de los delitos informáticos y de regular el acceso a la información.

La responsabilidad del Estado se podría adjudicar si el Estado no aplica adecuadamente la legislación o no está actualizando constantemente el marco normativo aplicable puesto que si la tecnología avanza y se transforma le corresponde al Estado realizar avances y transformaciones que cumplan los principios de garantía y seguridad que debe brindar a la población en los entornos informáticos, también es deber del Estado realizar acciones de prevención fomentando en los ciudadanos el uso consciente de las tecnologías, propiciando la publicación y divulgación de la ley.

Las entidades del Estado que por su funcionalidad manejan grandes volúmenes de datos de los ciudadanos, la Responsabilidad del Estado por Malas Prácticas en Entidades Públicas, estaría configurada si por falta de seguridad estas entidades fueran víctimas de ataques cibernéticos y los ciberdelincuentes llegaren a tener acceso a dicha información, si se comprobara que dicha situación pudo haberse prevenido podríamos llegar a un escenario en el que sería posible atribuir responsabilidad al Estado por no haber asegurado debidamente los sistemas de almacenaje de la información.

La falta de atención e investigación cuando una persona o entidad presentan una denuncia por ser víctima de un delito informático sea Estafa o Robo de datos, genera Responsabilidad del Estado por la Inacción o Ineficiencia en la Administración de

Justicia, lo que implica que si el Estado no realiza investigaciones efectivas y no tiene mecanismos efectivos para dar respuesta eficaz y eficiente a las víctimas de estos delitos, se constituye una falta de acción del Estado ya que no implemento las medidas adecuadas para investigar y sancionar los delitos informáticos.

Respecto de la Responsabilidad Extracontractual del Estado, la podemos observar por daño antijurídico, lo que significa que se podría decir que el Estado incurre en responsabilidad cuando se afectan derechos de los ciudadanos como resultado de una acción o inacción que genere un daño, en el contexto de delitos informáticos si no se implementan sistemas que prevengan oportunamente el robo de datos o estafas en línea, a gran escala, relacionamos aquí un hecho reciente ocurrido a las Empresas Públicas de Medellín "***EPM advierte de estafa con página falsa; usuarios estarían perdiendo sus pagos" HECHO: Empresas Públicas de Medellín informó que debido a la suplantación de su página web, fueron deshabilitados los canales de pago de facturas a través de su portal web. Según explicaron, personas inescrupulosas estaban dirigiendo los pagos de los clientes y usuarios a una cuenta bancaria de un tercero. Esta situación se comenzó a registrar desde este viernes 23 de mayo y desde EPM indicaron que esta suplantación ya fue identificada y se encuentra bajo control, también informaron que se avanza en el análisis para identificar a los responsables. "Como medida preventiva y priorizando la seguridad de nuestros clientes y usuarios, mantendremos deshabilitados nuestros canales de pago a través del sitio web de EPM, el módulo de factura en Ema y en la App EPM, hasta tener la certeza de que esta amenaza ha sido eliminada en su totalidad", señalan en el comunicado.*** (Veléz, 2025)

Se logra evidenciar que frente a la responsabilidad EPM, adopto medidas de prevención buscando salvaguardad la seguridad y privacidad de los datos de los usuarios que pagan sus servicios atreves de soportal, pero frente a las personas que ya fueron estafadas por la suplantación de su página ¿QUIEN DEBERA RESPONDER?, tendrá que recurrirse entonces al análisis jurisprudencial de la responsabilidad para lograr determinar si lo sucedido corresponde a acción, omisión o fallas por parte de la entidad y de allí se derivara que responsabilidad se le debe endilgar.

Continuamos observando que mediante diferentes normas el sistema judicial ha venido desarrollando una línea de normatividad tendiente a acabar las distintas problemáticas

y situaciones, el uso y suministro de la información a través de las tecnologías ha dado como consecuencia que las instituciones se avoquen a la atención de nuevas modalidades de delitos para los cuales se establece lo siguiente:

El Art 2 Constitución Política de Colombia: Establece el deber del Estado de proteger a sus ciudadanos, garantizando derechos fundamentales. Esto implica que el Estado tiene la obligación de prevenir delitos informáticos y actuar ante situaciones que pongan en riesgo la seguridad de los datos personales aplicando principios para la regulación tale como:

Principios de la Comisión Interamericana de Derechos Humanos: La protección del derecho a la vida privada y a la protección de los datos personales está reforzada por normas internacionales, el Estado debe cumplir con estas obligaciones internacionales, lo que refuerza la responsabilidad estatal en la protección de la ciudadanía frente a delitos cibernéticos.

Principio de Legalidad: El principio de legalidad es fundamental en el Derecho Penal y, en este contexto, las sentencias han insistido en que los delitos informáticos deben ser claramente tipificados en la ley, con el fin de evitar la arbitrariedad en las condenas.

Art 29 Constitución Política de Colombia

Protección de Datos Personales: La Corte Constitucional ha señalado la importancia de proteger los datos personales como un derecho fundamental. En casos de robo de datos, la jurisprudencia ha sido clara en que la violación de la privacidad y la identidad de las personas debe ser castigada severamente, la falta de cumplimiento de estas disposiciones puede ser considerada como un incumplimiento de la responsabilidad del Estado en la protección de información sensible. Ley 1581 de 2012 (Ley 1581, 2012) (Ley 1581, 2012).

La Ley 1273 de 2009 (Ley 1273, 2009) (Ley 1273, 2009) es clave para la creación de un marco legal en Colombia para tratar los delitos informáticos. Establece sanciones claras para los delitos como la estafa informática, el acceso no autorizado a sistemas informáticos, y el robo de datos personales o financieros.

Algunos artículos clave de la ley son:

- Artículo 269E: Este artículo tipifica el delito de acceso no autorizado a sistemas informáticos.

- Artículo 269F: Se enfoca en el robo de datos informáticos, ya sea en forma de información personal, financiera o de propiedad intelectual.

Normas de Derecho Internacional: Tratados como la Convención de Budapest sobre Cibercriminalidad (Consejo de Europa, 2001), a la que Colombia ha suscrito, exigen que los Estados establezcan medidas para prevenir y sancionar los delitos informáticos, así como mecanismos de cooperación internacional en su investigación.

Lo anteriormente expuesto nos presenta las situaciones mediante las cuales se podría deducir que es viable la atribución de responsabilidad jurídica al Estado con ocasión y en desarrollo de algunos delitos informáticos, pero también nos deja frente a un panorama un tanto complejo ya que lo que se debería probar allí es si el Estado realizo o no la o las acciones que pudieran evitar la situación o la violación de datos de las personas si la custodia de dicha información recae sobre un agente estatal, hasta que punto o bajo que criterio se puede decir que actuó u omitió.

Para entender esto es importante examinar la relación entre la responsabilidad del Estado y la protección de datos personales en el entorno digital, lo que nos lleva a observar si el Estado ha sido eficaz en la implementación de los mecanismos de protección, de los datos y la información de las personas, esto se evidencia en los pronunciamientos en la carta constitucional, mediante fallos de sentencias jurisprudencia, tratados internacionales y demás frente a casos relacionados se tienen:

la sentencia T-414 de 1992 sobre derecho a la intimidad personal y familiar/derecho a la información indica: “El dato es un elemento material susceptible de ser convertido en información cuando se inserta en un modelo que lo relaciona con otros datos y hace posible que el dicho dato adquiera sentido.

Además de ello tenemos las leyes que se han venido emitiendo y actualizando de acuerdo con los casos y/o situaciones a las que se deben enfrentar los operadores jurídicos, también se han adoptado no solo las disposiciones nacionales sino los tratados de cooperación internacional suscritos por Colombia que buscan abarcar un mayor ámbito de aplicación de la ley y garantizar la protección y la seguridad de las personas frente a la ocurrencia de los delitos informáticos

en este punto tenemos que la legislación colombiana ha venido siendo diligente en la implementación de normas que le permiten enfrentar los desafíos que han planteado las nuevas tecnologías.

4. OBJETIVO GENERAL

Analizar la responsabilidad jurídica del Estado colombiano frente a los delitos informáticos de estafa en línea y robo de datos personales, con base en el marco normativo y jurisprudencial vigente.

4.1. OBJETIVOS ESPECÍFICOS

Identificar los elementos del marco normativo colombiano aplicable a la protección de datos personales y delitos informáticos de estafa en línea y robo de datos.

Examinar una jurisprudencia emblemática sobre responsabilidad del Estado en casos de ciberdelitos de estafa en línea y robo de datos personales.

Determinar los desajustes, vacíos y contradicciones jurídicas que comprometen la garantía efectiva de los derechos fundamentales en casos de ciberdelitos de estafa en línea y robo de datos personales.

5. MARCO TEÓRICO

El marco teórico de esta investigación para esta investigación se desarrolla de la siguiente manera: observaremos algunos conceptos que son claves para una mejor compresión de la relación entre algunos delitos informáticos y la responsabilidad del Estado por lo que es importante realizar una breve definición de cada concepto.

5.1 METODOLOGÍA DE LA INVESTIGACIÓN

se aplica una metodología al proceso de investigación que se enmarca en los parámetros de enfoque cualitativo y se enmarca dentro de la investigación jurídico-dogmática, la técnica utilizada será el análisis documental de fuentes primarias (normativa nacional, jurisprudencia relevante, tratados internacionales) y secundarias (doctrina especializada), se delimita el estudio al contexto colombiano, en el periodo comprendido entre 2012 y 2025, centrado en los delitos informáticos de estafa en línea y robo de datos personales, y su relación con la responsabilidad del Estado por acción u omisión.

6. JUSTIFICACIÓN

Analizar el enfoque jurídico en el entorno de las nuevas tecnologías de la información que nos rodea actualmente y que ha generado tantos y grandes cambios sociales, culturales, económicos, políticos y en mayor medida frente a la disposición y acceso y utilización de los datos personales.

Además de ello es importante la identificación de cómo se han gestionado los casos en los que por situaciones de acción u omisión el Estado pueda llegar a ser responsable extracontractualmente, con ocasión de no haber brindado seguridad y protección a las personas como es su deber.

DESARROLLO

La falta de precaución a la hora de interactuar con las tecnologías y el suministro de nuestra información privada de manera casi que indiscriminada nos lleva a un estado de indefensión y vulnerabilidad tal vez por desconocimiento o por no asumir mayores gastos o costos en instalar programas de seguridad en los dispositivos que utilizamos, lo que aprovechan los ciberdelincuentes para acceder a nuestros sistemas y apropiarse de nuestra información con nuestros datos pueden afectar nuestro patrimonio económico o someternos mediante la estafa en línea para que accedamos a sus condiciones y entreguemos tanto bienes económicos como mayor acceso a nuestros espacios más íntimos y es allí donde terminamos siendo víctimas, “Los delitos informáticos son ejecutados por una sola persona o un grupo de individuos los cuales realizan actividades ilegales por medio de una terminal “computadora” de manera local o remota; este tipo o tipos de individuos poseen ciertas características intelectuales, que involucran un manejo especial para los sistemas informáticos” (PARRAGA, 2017),frente a estos requerimos la presencia de agentes estatales para salvaguardar y garantizar la protección de nuestra privacidad y seguridad.

Ahora bien, es importante que podamos reconocer ¿cómo determinar cuando una persona o empresa está sufriendo un delito informático, robo de sus datos o una estafa? Lo primero es definir que es un delito informático y encontramos que, según el convenio sobre la ciberdelincuencia del Consejo de Europa, suscrito en Budapest, el 23 de noviembre de 2001, Delitos informáticos son los actos que pongan en peligro la confidencialidad, la integridad, y la disponibilidad de los sistemas, redes, y datos

informáticos, así como el abuso de dichos sistemas redes y datos garantizando la tipificación como delito de dichos actos.

según MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020) – Los delitos informáticos son Conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio.

En el código penal colombiano en su título VII BIS -de la protección de la información y de los datos. Capítulo I de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. se relacionada desde el artículo 269a hasta el 269h, la tipificación de lo que se identifica como delitos informáticos.

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código

Los delitos informáticos presentan características particulares que dificultan su investigación y sanción, como el anonimato de los agresores, la rapidez con la que se pueden cometer los actos delictivos y la transaccionalidad de muchas de estas conductas. Estas condiciones exigen una respuesta estatal aún más robusta, articulada y adaptativa, que incluya tanto el fortalecimiento de las capacidades técnicas y humanas de las instituciones encargadas de la ciberseguridad como la educación ciudadana en el uso seguro de las tecnologías de la información.

En Colombia se han venido fortaleciendo instituciones como la Policía Nacional, con su unidad de policía virtual a través de la cual se ha creado una ruta para atender las denuncias y acompañara a las víctimas, esta institución tiene una línea de atención y en su página web, realiza publicaciones diarias donde se actualiza frente a los delitos informáticos, se dan recomendaciones para la prevención y se exponen los avances anuales.

Así mismo la fiscalía general de la nación mediante resolución 117 del 10 de marzo de 2023, reglamenta y conforma la Dirección Especializada Contra los Delitos

Informáticos, con el objetivo de fijar reglas para la articulación con otras dependencias en los procesos de prevención, persecución, investigación y sanción de los delitos informáticos. De acuerdo a esto las funciones de la fiscalía través de esta dirección son las de recepción de denuncias, a través de canales como la página web, puntos de atención y líneas telefónicas, colaboración internacional trabaja con organismos internacionales para rastrear delitos cibernéticos trasnacionales. Judicialización, recopila pruebas digitales (respetando la cadena de custodia) para judicializar a los responsables, prevención y sensibilización, desarrolla campañas de educación para informar a la ciudadanía sobre cómo protegerse de amenazas digitales

La estafa en línea es un delito cibernético que se comete a través de internet para engañar a las personas y robarles dinero o información personal.

los estafadores se hacen pasar por empresas o personas conocidas o de confianza, envían correos electrónicos fraudulentos, crean sitios web falsos que imitan a empresas legítimas, suplantan la identidad de otra persona, para obtener información personal la sala de casación en providencia SP070-2025 del 29 de enero de 2025, resolvió una situación de competencia entre jueces frente a la comisión de unos hechos que se desarrollaron así:

"Proceso penal en etapa de juzgamiento en contra de (7) personas por la presunta comisión de los delitos de hurto por medios informáticos y semejantes, acceso abusivo a un sistema informático y daño informático, todos agravados por la circunstancia prevista en el numeral 5 del artículo 269 H del Código Penal.

Traemos de presente una sentencia que desarrollo algunos aspectos importantes frente las situaciones de competencia de la justicia para atender situaciones por denuncia e investigación con relación a delitos informáticos.

ANÁLISIS DE UN CASO RELEVANTE

De acuerdo con el contenido del escrito de acusación, los hechos que dieron origen a la presente actuación penal son los siguientes:

> *«El 03 de noviembre del año 2020* [formuló denuncia], *la apoderada de SODIMAC COLOMBIA S.A. (HOME CENTER), empresa dedicada al retail*

(venta al detalle o comercio minorista), donde su principal función es prestar servicios como establecimiento abierto al público a nivel nacional, así mismo cuenta con el área de Venta en línea que es un canal, con un amplio portafolio de productos multimarcas, por medio de compras en Línea en la Aplicación Móvil "App" Homecenter.

En dicha denuncia refieren haber sido víctimas de una explotación a la vulnerabilidad en la aplicación pagos de la "App Homecenter", donde los aquí investigados alteraron los precios de los electrodomésticos, efectuando pagos que no correspondían ni al 10% del valor real, en total realizaron 333 compras fraudulentas por un valor de 2.285.223.057 millones de pesos, una vez obtienen los productos inician el proceso de reventa de los mismos. Así mismo, se observa la utilización y creación sistemática de cuentas a la mano como DAVIPLATA Y NEQUI usando diferentes SIM CARDS Y TELEFONOS para los registros a las plataformas de pago y así realizar transacciones.» (Hurto por medios informáticos y semejantes / Acceso abusivo a un sistema informático, 2025)

Este caso es importante en el contexto de esta investigación por cuanto se dan determinaciones claras y especificas cuando se trata de abordad las denuncias e investigaciones por delitos cibernéticos, toda vez que no puede tomar se una situación de competencias entre los jueces, como una situación para entorpecer la investigación de los denunciados ya que los delitos informáticos a l ser realizados atravesó de medios tecnológicos se avocan a un amplio espectro en el cual es complejo determinar el lugar, es decir el territorio donde se ha realizado la conducta delictiva, por cuanto para el avance en los procesos se atenderá a las disposiciones determinadas en el presente caso.

Definición de estafa en línea y tipos.

Los tipos de estafas en línea: Phishing, Robo de identidad, Venta de productos inexistentes, Fraude de comercio electrónico, Estafas de soporte técnico, Estafas de mulas de dinero.

En cuanto a las acciones del Estado Colombiano como responsable tenemos que son importantes los elementos:

Desarrollo de Infraestructura de Ciberseguridad: El Estado tiene la responsabilidad de desarrollar, mantener y actualizar una infraestructura de ciberseguridad fuete que le permita proteger la información de los ciudadanos y prevenir delitos informáticos.

Capacitación y Sensibilización: Implementar programas de capacitación y sensibilización dirigidos tanto a funcionarios públicos como a ciudadanos, con el fin de fomentar prácticas seguras en el uso de tecnologías de la información.

Cooperación Internacional: La ratificación de convenios y tratados con otros países y organizaciones internacionales puede ser vital para enfrentar delitos informáticos que trascienden fronteras.

Responsabilidad en la Ley de Protección de Datos: El Estado deberá realizar seguimiento y evaluación constante al cumplimiento de sus obligaciones bajo la legislación de protección de datos y las medidas que se implementan para garantizar que la información personal esté protegida.

Acciones Judiciales Efectivas: Examinar la efectividad de los procesos judiciales relacionados con delitos informáticos y cómo el Estado puede mejorar la administración de justicia para las víctimas.

Actualización Legislativa: Es necesaria la actualizar continuamente las leyes relacionadas con delitos informáticos para adaptarse a los rápidos avances tecnológicos y nuevas modalidades de ciberdelincuencia.

Mecanismos de Denuncia: La creación de canales efectivos y accesibles para que las víctimas de delitos informáticos puedan reportar sus casos y recibir asistencia oportuna.

Evaluación de Políticas Públicas: Realizar estudios para evaluar el impacto de las políticas públicas implementadas en el ámbito de la ciberseguridad y la protección de datos personales.

Estos elementos pueden contribuir a una gestión más integral y proactiva de la responsabilidad del Estado frente a los delitos informáticos, asegurando una protección más efectiva de los derechos de los ciudadanos y fortaleciendo la confianza en las instituciones.

Este es uno de los escenarios más conocidos y que representa mayormente la incapacidad Estatal, porque cuando surge el delito a primera vista la persona que fue o es víctima no tiene una ruta clara de a qué entidad acudir para denunciar, para solicitar o exponer lo que le ocurre y en muchas ocasiones cuando logra llegar a esos agentes

del estado que deben ser garantes y prestar la debida atención y gestión, cae en una revictimización por que los presupuestos que debe acreditar son bastante complejos y casi que se le culpa de haber brindado su información, además si no hubo constreñimiento alguno resulta un tanto más complejo demostrar cómo se permitió o se dio lugar al delito y en muchas ocasiones el trámite de la denuncia termina en el desistimiento de la víctima por que representa un desgaste físico, psicológico y emocional mayor.

7. CONCLUSIONES

De acuerdo a todo lo anterior podemos decir que El Estado sería responsable por la falta de acción o de medidas efectivas que conduzcan a una mayor vulnerabilidad de las personas naturales y jurídicas, afectando su privacidad, su intimidad, su patrimonio económico y la confianza en las instituciones estatales.

Por lo tanto, una gestión proactiva y responsable del Estado es necesaria para garantizar la protección de los derechos fundamentales, fomentar la seguridad digital y asegurar un entorno cibernético más seguro para todos y lo que se puede evidenciar que el Estado colombiano ha desarrollado una estructura normativa y judicial para afrontar los delitos informáticos, como el robo de datos y la estafa en línea. La promulgación de leyes como la (Ley 1273, 2009) y la (Ley 1581, 2012), junto con la creación de instituciones especializadas como el CAI Virtual de la Policía Nacional, y el fortalecimiento de otras instituciones como la Unidad de Investigación Criminal (UIF) de la fiscalía general de la Nación. Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Esto demuestra un compromiso significativo con la prevención, detección y sanción de estos delitos. Sin embargo, a pesar de estos avances, persisten desafíos considerables en la implementación efectiva de medidas eficaces y en la garantía de justicia para las víctimas.

Además, la jurisprudencia del (Consejo de Estado, s.f. (Consejo de Estado, s.f.)) ha reconocido que el Estado puede ser responsable no solo por acción u omisión directa de sus agentes, sino también por la inactividad frente a amenazas evidentes a los derechos de los ciudadanos. En el contexto de los delitos informáticos, esto implica que

la falta de actuación diligente ante denuncias de estafa o robo de datos puede dar lugar a reclamaciones por responsabilidad extracontractual del Estado.

Acciones de capacitación y sensibilización implementar programas de capacitación y sensibilización dirigidos tanto a funcionarios públicos como a ciudadanos, con el fin de fomentar prácticas seguras en el uso de tecnologías de la información.

Cooperación Internacional la ratificación de convenios y tratados con otros países y organizaciones internacionales puede ser vital para enfrentar delitos informáticos que trascienden fronteras.

Responsabilidad en la Ley de Protección de Datos el Estado deberá realizar seguimiento y evaluación constante al cumplimiento de sus obligaciones bajo la legislación de protección de datos y las medidas que se implementan para garantizar que la información personal esté protegida.

Acciones Judiciales Efectivas examinar la efectividad de los procesos judiciales relacionados con delitos informáticos y cómo el Estado puede mejorar la administración de justicia y la atención de las víctimas.

Actualización Legislativa es necesaria la actualizar continuamente las leyes relacionadas con delitos informáticos para adaptarse a los rápidos avances tecnológicos y nuevas modalidades de ciberdelincuencia.

Mecanismos de Denuncia la creación de canales efectivos y accesibles para que las víctimas de delitos informáticos puedan reportar sus casos y recibir asistencia oportuna.

Evaluación de Políticas Públicas realizar estudios para evaluar el impacto de las políticas públicas implementadas en el ámbito de la ciberseguridad y la protección de datos personales tendientes a desarrollar una gestión más integral y proactiva de la responsabilidad del Estado frente a los delitos informáticos, asegurando una protección más efectiva de los derechos de los ciudadanos y fortaleciendo la confianza en las instituciones.

Por tanto, es fundamental el fortalecimiento las infraestructuras de ciberseguridad, que se actualicen las normativas legales y se implementen políticas públicas que prioricen la educación y sensibilización de la ciudadanía frente a la aplicación de buenas prácticas

de uso de las tecnologías y el suministro de datos e información sensible, la cooperación internacional y el desarrollo de mecanismos eficientes para la recepción y tramite de denuncias y el seguimiento de estos delitos son elementos vitales en la lucha contra la ciberdelincuencia.

REFERENCIAS

- UNIR. (2020). *Ciberdelincuencia: qué es, concepto de ciberdelito y tipos*. https://www.unir.net/
- Consejo de Europa. (2001, noviembre 23). *Convenio sobre la ciberdelincuencia (Convenio de Budapest)*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
- Corte Constitucional de Colombia. (2002, septiembre 5). *Sentencia T-729/02*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=9903
- Corte Suprema de Justicia, Sala de Casación Penal. (2025, enero 29). *Hurto por medios informáticos y semejantes / Acceso abusivo a un sistema informático* (Radicación No. 58666). [Fecha de recuperación no requerida en APA 7]. (Si tienes enlace, agrégalo aquí)
- Congreso de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2020). *Adhesión al Convenio de Budapest contra la ciberdelincuencia, clave para Colombia en tiempos de Coronavirus*. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/126496:Adhesion-al-Convenio-de-Budapest-contra-la-ciberdelincuencia-clave-para-Colombia-en-tiempos-de-Coronavirus
- Párraga, A. C. (2017). *Análisis de los delitos informáticos en el actual sistema* (pp. 28–29). (Si es una tesis, informe o artículo, especificar tipo y editorial o universidad)

- Pino, D. S. (s.f.). *Delitos informáticos: Generalidades*. Organización de los Estados Americanos (OEA). https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- Secretaría del Senado de la República. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado: la protección de la información y los datos*. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
- Superintendencia de Industria y Comercio. (s.f.). *Sobre la protección de datos personales*. https://www.sic.gov.co/content/sobre-la-protecci%C3%B3n-de-datos-personales
- SIN AUTOR. (s.f.). *Resolución*. Sistema Único de Información Normativa – SUIN. https://www.suin-juriscol.gov.co/clp/contenidos.dll/Resolucion/30045325?fn=document-frame.htm$f=templates$3.0 (Revisa si puedes precisar el tipo y número de resolución)
- Policía Nacional de Colombia. (2024). *Balance anual CECIP 2024*. https://caivirtual.policia.gov.co/sites/default/files/observatorio/BALANCE%20ANUAL%20CECIP%202024.pdf