La Regulación de los Delitos Informáticos en Colombia: Logros y Falencias en una sociedad de Cibercriminalidad en auge*

The Regulation of Cybercrime in Colombia: Successes and Failures in a booming Cybercrime society

Matías MESA GIRALDO**

Luisa Fernanda PONCE JARAMILLO***

Forma de citación: Mesa, M. Ponce, L.F. (2023) *"La Regulación de los Delitos Informáticos en Colombia: Logros y Falencias en una sociedad de Cibercriminalidad en auge".* En: (Revista XX. Vol. XX. No. XX, 2023, p. XX-XX. (Enlace)

**Estudiante de Décimo Semestre de la Facultad de Derecho de la Universidad CES. Correo electrónico: mesa.matias@uces.edu.co

*** Estudiante de Décimo Semestre de la Facultad de Derecho de la Universidad CES. Correo electrónico: ponce.luisa@uces.edu.co

RESUMEN

Este artículo estudia los delitos informáticos desde su concepción misma, los eventos históricos que motivaron su aparición y, muy especialmente, la regulación que de estos existe en Colombia, en el Título VII Bis del Código Penal “de la Protección de la Información y de los Datos”, contrastándolos con cifras que dan cuentan del aumento en número y en clase de este tipo de conductas penales, en especial desde la digitalización masiva generada por la crisis del COVID-19, para terminar hallando que la normativa actual se está quedando corta en su regulación, y que el Cibercrimen es una tendencia en aumento que debe ser atendida pronta y directamente por el Estado.

PALABRAS CLAVE

Delitos informáticos; Cibercrimen; Regulación Penal; COVID-19; Información y Datos; Tipos penales.

ABSTRACT

This article studies cybercrime from its very conception, the historical events that led to its appearance and, especially, the regulation against it that exists in Colombia, contemplated in Title VII Bis of the Penal Code “Crimes against Information and the Data”, contrasting it with figures that expose the increase in number and type of this type of criminal conduct, especially since the massive digitization generated by the COVID-19 crisis, to end up finding that the current regulations are insufficient in their regulation, and that Cybercrime is a growing trend that must be solved promptly and directly by the State.

KEYWORDS

Cybercrime; Criminal Regulation; COVID-19; Information and Data; Criminal types.

CONTENIDO

INTRODUCCIÓN

La sociedad actual se encuentra en una carrera acelerada de crecimiento tecnológico cada vez más deslumbrante, situación que, desafortunadamente, ha generado un aumento importante de la cibercriminalidad (Vita, 2020), lo cual es un efecto esperado, toda vez que el medio digital representa un auténtico mundo nuevo en muchos sentidos, siendo uno de ellos, claro está, el de las acciones no tan apegadas a la ley.

Se ha dicho que los delitos informáticos son:

"Todas aquellas conductas punibles de medios ejecutivos abiertos, que tienen una relación modal objetiva –aunque circunstancial– con el tratamiento de datos e información y los sistemas informáticos". (Maya, 2018)

Así pues, es claro que con el internet es cada día mayor la frecuencia e impacto en los dispositivos de acumulación y procesamiento de información –llámense servidores, estaciones de trabajo o simplemente PC–, los cual resultan siendo vulnerados en sus elementos más sensibles, trayendo importantes riesgos para los datos de distinto valor personal, financiero, crediticio; lo cual es trascendental para las personas, las empresas, los gobiernos y otras organizaciones, incluso a veces atacando la dignidad, la honra y vida de las personas individuales (Bechara, Mosquera, & Ledezma, 2020).

En ese sentido, el artículo 15 de la Constitución Política de Colombia indica que:

> *Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. la correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios*

> *o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.* (Constitución Política de Colombia, 1991)

Este argumento constitucional solamente demuestra que Colombia es un país que pretende estar digitalizado, pero que comprende, asimismo, que la información y los datos que son compartidos, tratados, recopilados y manipulados a través de las herramientas tecnológicas están revestidos de una importancia mayúscula, y deben gozar de una protección superior, toda vez que se han convertido en un valioso activo en el siglo XXI, como afirma (Novoa, 2021).

Es precisamente en ese escenario que entra en escena la Ley 1273 de 2009 una norma que modifica el Código Penal del año 2000, introduciendo una nueva gama de delitos, para lo cual crea un nuevo bien jurídico denominado *"De la protección de la información y de los datos"*, revolucionando así la forma en cómo el país se enfrenta a los nuevos retos que la tecnología impone para el derecho penal en su tarea de proteger las prerrogativas de las personas, evitando que criminales inescrupulosos se aprovechen de la digitalización para cometer sus fechorías.

El análisis entonces está orientado a una revisión de la regulación de los delitos informáticos en el país, teniendo como base esta norma, toda vez que está próxima a cumplir 14 años de vigencia y, sin embargo, las cifras de la cibercriminalidad en Colombia no hacen más que crecer (Lesmes, Colombia, el segundo país de América Latina con más ciberataques en 2022, 2023). Como si fuera poco, la llegada de la pandemia de COVID-19 aceleró este proceso de forma importante, puesto que la apresurada transición de muchas personas, empresas y gobiernos al mundo tecnológico representó un aumento del tráfico de información, datos y demás elementos estratégicos que circulaban a través de la red, situación que, evidentemente, fue aprovechada por los criminales virtuales, quienes vieron en la crisis sanitaria la mejor de sus oportunidades, generando así un aumento nunca antes visto de los delitos ejecutados a través de los medios informáticos.

Como ya se insinuó previamente, es innegable que, a día de hoy, los sistemas de información, la internet y la computación en la nube son el soporte para el almacenamiento, gestión y aplicación de información personal y organizacional, lo cual abre la puerta a que estos sistemas eventualmente se conviertan en el blanco perfecto para aquellas personas que pretendan robar, manipular, dañar o afectar a sus propietarios, según (Ospina & Sanabria, 2020).

Esta situación ocurre en vista de que la mayoría de la población y las organizaciones públicas y privadas se han apropiado casi en su totalidad de los sistemas informáticos para soportar su rutina de trabajo, su archivo histórico, su actividad económica, entre otros, situación que les deja vulnerables a cualquier manipulación o fallo por parte de personas que hábilmente se introducen en los sistemas, lo cual genera afectaciones de gran escala a nivel individual y colectivo.

Partiendo de allí, es razonable considerar las enormes implicaciones de que la información existente en correos electrónicos, redes sociales, reuniones privadas de trabajo o estudio o archivos laborales sufran ataques, daños o pérdidas; los efectos de fallas en bases de clientes, proveedores o nómina de una organización; las consecuencias de que se vulnere la integridad de una persona debida a la manipulación de información o la suplantación en redes (Ospina & Sanabria, 2020 refiriendo a Amato et al., 2018); incluso, puede decirse lo mismo de lo que ocurriría si un ataque cibercriminal llegue a los sistemas de infraestructura crítica de servicios –tales como represas, centrales de energía, aeropuertos, puertos, entre otros- o produzca la pérdida de información estratégica del Estado o de entidades de la administración pública, en palabras de (Ospina & Sanabria, 2020), estas son las problemáticas que realmente conciernen a la ciberseguridad.

Así pues, la revisión de la mentada Ley 1273 de 2009 y su papel actual y capacidad de reducir la comisión de delitos informáticos, se encuentra estrechamente relacionada con la norma penal, desde los presupuestos, fines y efectos de la misma, por esta razón, la investigación se hace notable para el derecho, puesto que pretende establecer criterios que las normas deberían cumplir, máxime en un contexto donde se está definiendo la política criminal de un nuevo gobierno, y donde

algunos de los valores tradicionales están comenzando a cambiar para redefinir el papel del derecho en la sociedad.

La pregunta de investigación que pretende ser respondida en este trabajo es: ¿Qué eficacia tiene la normatividad vigente sobre los delitos informáticos en Colombia en el marco de la ciberdelincuencia?

Para resolverla, se plantea el objetivo general de determinar la eficacia del marco normativo que regula los delitos informáticos en Colombia, y como objetivos específicos identificar las cifras, causas y consecuencias de la ciberdelincuencia en Colombia; establecer el campo de aplicación y vigencia del Título VII BIS del Código Penal en la actualidad jurídica del país; y analizar qué otras conductas delictivas de carácter informático están ocurriendo en el país.

El tema es relevante para el mundo académico actual del derecho, toda vez que, como se ha mencionado con anterioridad, los delitos informáticos representan actualmente un riesgo de gran magnitud para la sociedad, en vista de la, cada vez, mayor compenetración de las tecnologías en la vida de las personas (Ospina & Sanabria, 2020), así pues, ponerle la lupa a este flagelo criminal debe ser una prioridad en la investigación jurídica, pues con toda probabilidad estas conductas van a seguir en aumento, y el derecho debe tener la capacidad adecuada para responder ante esta necesidad que aqueja a la población, solución que debe darse desde la eficacia real de la norma, para lo cual es crucial conocer el estado actual de la misma, lo cual corresponde a la motivación de este artículo.

En lo referente a la metodología utilizada, es posible afirmar que el presente trabajo se circunscribe a un enfoque cualitativo, toda vez que es el más pertinente para el objetivo planteado, con respecto a este enfoque en concreto, (Duque, González, Cossio, & Martínez, 2018) afirman: "*su interés está centrado en la cotidianidad que es el espacio para comprender la realidad en el abordaje, de lo subjetivo e intersubjetivo, en los actores y escenarios en los cuales se desenvuelven sus prácticas jurídicas y sociales"* (p. 61).

Así pues, es evidente que este trabajo hace parte del enfoque cualitativo, en especial porque su concepción misma está orientada a profundizar en el análisis de la realidad observada, más que recolectar datos para probar determinadas tesis o conseguir ciertos resultados, lo cual es propio del enfoque cuantitativo de la investigación, en palabras de (Sutton, 2016).

El trabajo, además, puede ser identificado como una monografía jurídica, razón por la cual para su desarrollo precisó de una búsqueda amplia de literatura académica relacionada con en el tema de investigación, lo cual se hizo en las bases de datos acreditadas, adicionalmente, se nutrió de otro tipo de referencias, tales como noticias fidedignas de actualidad y jurisprudencia; todo esto con miras a desarrollar los objetivos propuestos y determinar la eficacia del marco normativo que regula los delitos informáticos en Colombia.

Ahora, en el presente escrito, se hace pertinente acudir al tipo de investigación hermenéutico para su desarrollo, respecto del particular, una definición de diccionario diría que la hermenéutica es el arte de interpretar textos en la búsqueda de su verdadero sentido; especial y originalmente, de los textos sagrados y/o aquellos de una temporalidad relativamente lejana. Así, el texto aparece como la materia prima esencial para el proceso de captar tal sentido (Maldonado, 2016).

Conforme a lo anterior, el trabajo de presente se acomoda en el tipo de investigación hermenéutico, lo cual ocurre de esta manera porque la intención del mismo es realizar un recorrido de la normativa que actualmente regula los delitos informáticos en Colombia, contrastarla con cifras de la Rama Judicial y de la Fiscalía General de la Nación que den cuenta de la eficacia de estas normas y, a partir de ello, determinar la utilidad real de la legislación en comento en el panorama actual del país; para ello, es necesario recoger una cantidad considerable de información, principalmente de origen académico, para posteriormente acudir a una interpretación adecuada de los textos colectados, en este momento es donde es importante el tipo hermenéutico, porque la idea no es forzar a los textos a que digan aquello que alguna persona determinada pretende, sino que es necesario sopesar

realmente la opinión contraria, encontrando así la realidad del asunto investigado (Aránguez, 2016), lo cual solo puede lograrse con una adecuada interpretación.

Como es evidente, la naturaleza cualitativa del trabajo implica cierto toque de subjetividad alrededor del mismo, sin embargo, esto no significa que no esté presente un criterio objetivo de análisis, de hecho, esta combinación resulta bastante provechosa para los objetivos del proyecto, puesto que permite el estudio real de la situación desde múltiples variables que conviene examinar con detalle y atendiendo a las particularidades de cada una de ellas.

Luego, el proceso de contraste que se genera entre la información previa del investigador y la información disponible en la literatura académica encontrada, transforma el conocimiento del tema, eventualidad que faculta la obtención de resultados novedosos en la investigación desarrollada, situación que se hace bastante provechosa cuando se trata de un tema crítico, tal como lo es el auge de los delitos informáticos en el contexto de la denominada Cuarta Revolución Industrial, permitiendo así que el análisis de textos en contraste con un problema a investigar, produzca auténtico conocimiento y los resultados obtenidos puedan ser expuestos, discutidos e incluso refutados.

Refiriéndose a la técnica utilizada en este trabajo, la primera de ellas fue la revisión documental, la cual se hizo en las bases de datos VLex, Dialnet, Scielo, Taylor & Francis y el motor de búsqueda Google Académico; posteriormente se acudió a la lectura crítica para recoger la información más relevante de cada texto y que pudiera aportar elementos de conocimiento útiles para la investigación desarrollada, generando las correspondientes citaciones que deben realizarse al insertar información de otro autor en el artículo propio.

Con respecto a los instrumentos, se usaron en el presente trabajo el informe de lectura, el análisis de contenido y las fichas bibliográficas, lo cual era esperable, teniendo en cuenta que el principal suplemento informativo del proyecto es la literatura académica, especificando que esta debió cumplir con las variables escogidas y responder adecuadamente a los objetivos planteados, para así poder generar resultados de la investigación.

En lo referente a las variables de lectura, teniendo en cuenta que el trabajo se encuentra sustentado en su mayoría en literatura académica tal como trabajos de grado, tesis, artículos de investigación y ensayos, para la selección de la información se echó mano de términos clave durante el proceso de investigación en las bases de datos utilizadas, los cuales debían estar relacionados naturalmente con el tema investigado, estos fueron: “Ley 527 de 1999”; “Ley 1273 de 2009”; “Delitos informáticos”; “Cibercrimen”; “Ciberdelincuencia”; “Información y Datos”; “Fraude por medios informáticos”.

Finalmente, en el apartado ético, la investigación que produjo el suscrito trabajo se consideró como “sin riesgo”, en el entendido que su desarrollo no genera peligros físicos, psicológicos, biológicos o de ninguna otra clase para las personas, toda vez que su marco de referencia es netamente documental, y no se requiere la participación ni intervención de sujetos externos al investigador. Por su parte, se encuentran también garantizados los principios de beneficencia, autonomía, no maleficencia y justicia, puesto que el trabajo aporta importantes beneficios para la sociedad, al evidenciar la gravedad de las conductas estudiadas, también se reconoce que la información utilizada es pública, y se ha citado debidamente, en el mismo sentido, no hay maleficencia al tratar de concientizar a la ciudadanía de una problemática criminal grave y, finalmente, el análisis objetivo y sin prejuicios de la información consultada garantiza el principio de la justicia.

CAPÍTULO I. DEL CAMPO DE APLICACIÓN Y VIGENCIA DEL TÍTULO VII BIS DEL CÓDIGO PENAL, EN LA ACTUALIDAD JURÍDICA NACIONAL

Para nadie es un secreto que la internet es uno de los más grandes logros de la humanidad, esto es tan cierto que, en este momento histórico, gran cantidad de actividades cotidianas serían inconcebibles sin la ayuda de este sistema, desde reservar un hotel para las vacaciones, hasta pagar impuestos o hacer comercio

electrónico, inclusive, el funcionamiento mismo de la Administración Pública y es que, de hecho, esta tendencia solo parece aumentar, y no es descabellado afirmar que internet se ha convertido en el nuevo “mejor amigo del hombre”; sin embargo, y de forma desafortunada, el gran alcance que ha tenido la red en el mundo, también ha sido visto como una oportunidad para personas inescrupulosas que, a lo largo de la existencia de internet, han manipulado servidores, sistemas y software para cometer conductas antijurídicas en contra de la población, y es en este contexto donde aparece el concepto de Delitos Informáticos.

De este modo, (Cortés, Ballén, & Duque, 2015) refieren que estos son:

> *Toda conducta punible, es decir típica, antijurídica y culpable señalada por el legislador; que se realiza haciendo uso indebido de la información y de cualquier medio informático empleado para su manejo, o de la tecnología electrónica o computarizada, como método, medio o fin que menoscabe, mengüe o ponga en riesgo el bien jurídico de la información y de los datos; además que con ocasión de ellos en circunstancias específicas se pueda afectar otros bienes jurídicos como la vida, la libertad, la familia, el patrimonio, la seguridad pública y la del Estado.*

De modo casi que lógico, el aumento del uso de la red informática por parte de la población, llevó al consecuente aumento proporcional de los delitos informáticos en el seno de la colectividad; esto se debe, principalmente, a la débil seguridad que presentaban los sistemas, por un lado, y por el otro, a la inexistente regulación legal al respecto; es en este escenario que el Congreso de la República de Colombia promulga la Ley 1273 de 2009, que crea el Título VII BIS del Código Penal; esta norma se crea bajo el entendido de que hay personas que utilizan su privilegiado talento y conocimiento de los sistemas informáticos para tratar de sacar provecho de ello en detrimento de sus semejantes, recurriendo a conductas que por lo novedosas no se encuentran aún tipificadas, o que si lo están, su aplicación en concreto tiene una relativa dificultad pues la adecuación típica no es lo suficientemente clara como se quisiera (Varón, 2008).

A pesar del importante esfuerzo legislativo que supuso la aprobación de esta norma, se ha podido evidenciar que las condenas por delitos informáticos en realidad son bajas en Colombia, pues según cifras del Instituto Nacional Penitenciario y Carcelario (INPEC) únicamente se registran 206 del universo de 170.195 impuestas por los jueces penales de conocimiento (Cortés, Ballén, & Duque, 2015), y este dato del año 2015 no es de poca importancia, porque en la actualidad existen multiplicidad de modalidades criminosas relacionadas con la actividad virtual, pues además de los delincuentes informáticos propiamente, existen otros tipos de delincuentes que han encontrado espacios propicios en los distintos medios de comunicación electrónica, para desarrollar sus crímenes, tales como estafadores, falsificadores, defraudadores, secuestradores, proxenetas, traficantes de armas, traficantes de drogas, traficantes de personas, creadores de pornografía, homicidas y terroristas, entre muchos otros.

En revisión de los últimos años, los hallazgos del Tanque de Análisis y creatividad de las TIC (TicTac), de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y el Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional ha establecido que en 2019 los incidentes cibernéticos en el país tuvieron un incremento del 54 % con respecto al 2018. Además, de los 28.827 casos reportados, 15.948 fueron denunciados como infracciones a la mentada Ley 1273 de 2009, o sea, hay 12.879 conductas lesivas que no encuentran tipo penal en el cual puedan encuadrarse (Bechara, Mosquera, & Ledezma, 2020).

El informe también encontró que de 2017 a 2020 se reportaron 52.901 denuncias, de las cuales lideran los hurtos que se realizan a través de medios informáticos (31.058), seguido por el robo de identidad (8.037), donde Bogotá fue la ciudad que más incidentes reportó (5.308), seguida por Cali (1.190) y Medellín (1.186) (Bechara, Mosquera, & Ledezma, 2020).

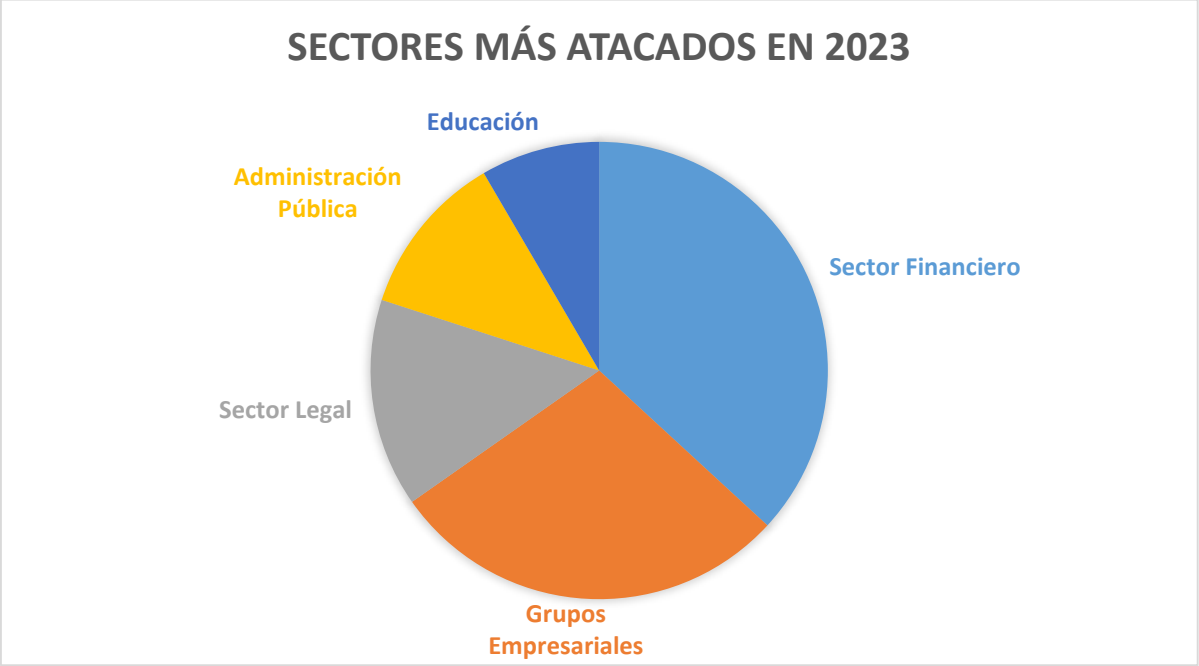
El reporte del referido (TicTac) y su programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE), en su última versión (2021-2022), evidenció que:

> *El número de denuncias instauradas ante la Fiscalía General de la Nación, las policías judiciales del CTI y la Policía Nacional (DIJIN-SIJIN), a través del aplicativo a denunciar, al finalizar el mes de noviembre del 2021 se habían registrado 46.527 denuncias por distintos delitos lo que equivale a un incremento del 21% respecto al 2020. Si se tienen en cuenta comparativamente los años 2019 y 2021, es decir sin contabilizar el año de pandemia, el incremento alcanzó un 107% acumulado entre el incremento suscitado durante el 2020 y el aumento continuo durante el 2021.* (Equipo TicTac, 2022)

Estas cifras revelaron que el ciberdelito es la tipología criminal que más está creciendo en el país durante los últimos tres años, lo cual se debe, por supuesto, a la pandemia y el significativo aumento del uso de canales digitales para transacciones y comercio, que alcanzó el 59.4% en las transacciones durante el periodo de cuarentena obligatoria y del 35% durante el 2021 con ventas estimadas en 37 billones de pesos al finalizar el año según cifras de la Cámara de Comercio electrónico de Colombia CCCE (Equipo TicTac, 2022).

Por su parte, conforme a las cifras otorgadas por el reporte *Ciberseguridad: 'Panorama regional 2022 - 2023'* realizado por GMS Seguridad, los ciberataques para el año 2023 han tenido un aumento de 65%, en comparación con el 2022. Asimismo, este grupo de reportes ha indicado que los eventos importantes que han comprometido la seguridad se encuentran concentrados en sectores como el financiero, los grandes grupos empresariales, el sector legal, la Administración Pública y el sector educativo (López, 2023), así:

Figura 1. Sectores más atacados durante los años 2022 y 2023:



Fuente: elaboración propia de los autores, con datos de: López, J.M. (2023). *Ciberataques subieron 65% siendo los bancos e industriales sus blancos más comunes*. Recuperado de La República: https://www.larepublica.co/empresas/reporte-ciberseguridad-2023-a-empresas-y-sectores-3701737

No debe dejarse de lado que existen limitantes importantes a la hora de la aplicación correcta de estos tipos penales, concretamente, la Administración Pública y de Justicia, no dispone de muchos agentes para la investigación criminal de estos asuntos, porque sencillamente, no son relevantes ni mediáticos y, en palabras de (Cortés, Ballén, & Duque, 2015), hay un concepto generalizado de que su gravedad no es tan alta, pero nada más ajeno a la realidad, y es que, según cifras de investigación independiente de la Deutsche Welle, desde la aparición de la pandemia de COVID-19, las cifras de delitos criminales en Europa y el mundo no han hecho más que crecer, al punto que, por ejemplo, se calcula que en el mundo, se están enviando más de dos millones de correos electrónicos fraudulentos cada día (García, 2020), es por esto que se evidencia un relativo abandono de este Título del Código Penal que, en vez de reducirse, cada día tiende más a aumentar, y los

servidores públicos deberán estar a la vanguardia, a fin de evitar que el país se convierta en núcleo de los delitos informáticos.

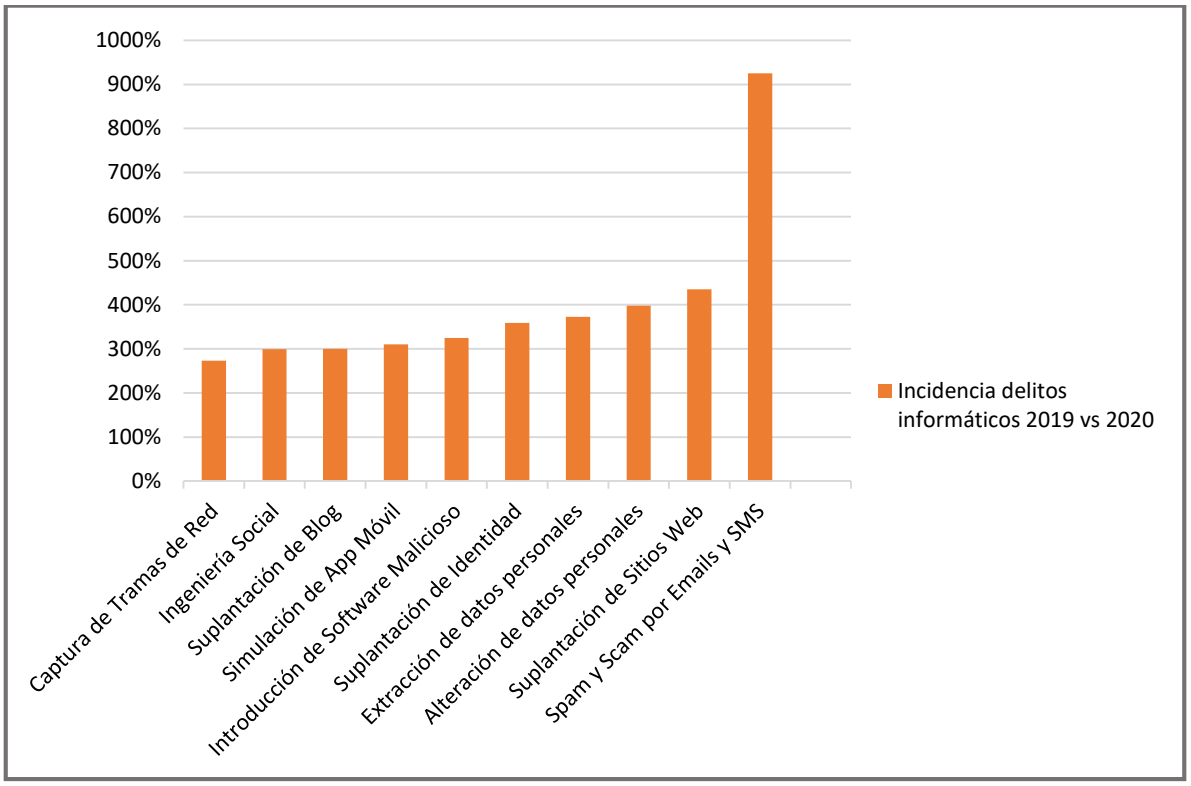
Esta realidad no puede pasar desapercibida, pues cada vez son más los autores que advierten del importante aumento que han tenido los delitos informáticos, no solo en Colombia, sino en todo el mundo, máxime en situación de pandemia, como se ha venido observando, en ese sentido se pronunció el Coronel Luis Fernando Atuesta, jefe del Centro Cibernético de la Policía Nacional, al explicar que:

> *El delito que más se produce es el hurto a través de medios informáticos, es decir, la gente es víctima de que le roben el dinero de sus bancos por medio de internet. Lo que más se ha incrementado es el uso de software malicioso y hay una propagación de virus impresionante a través de internet, lo que hace que los infractores de la ley se apoderen de claves bancarias, y es que, durante la temporada de aislamiento obligatorio, la actividad maliciosa en internet se incrementó en más del 150% y se detectaron alrededor de 200 páginas que tienen contenido malicioso* (Revista Semana - Tecnología, 2020).

Al inicio del periodo de aislamiento preventivo en Colombia para contrarrestar los efectos nocivos de la pandemia de COVID-19, en marzo de 2020, muchos autores volcaron su interés en los delitos informáticos, y previeron su aumento, sin embargo, conforme avanzó el año, esta atención disminuyó, pero no así la actividad delictiva, luego, según cifras otorgadas por el sistema SIEDCO PLUS de la Policía Nacional, desde abril de 2020, el primer mes completo de aislamiento obligatorio, los delitos informáticos presentaron un crecimiento de más de 100% en comparación con el mismo mes de 2019; este mes tuvo el aumento más significativo, con 129%, mientras que el de menor crecimiento, desde el inicio de la pandemia, fue octubre, con 85%, que no deja de ser una cifra notoriamente alta. En total, con corte al 17 de noviembre de 2020, ese año se habían presentado 36.834 delitos cometidos por medios informáticos, en contraste con la cifra de 20.107 que se registraron en el mismo periodo del año anterior (Vita, 2020).

Esto se explica porque las medidas que dictó el Gobierno Nacional para frenar la expansión del COVID-19, obligaron a las personas a quedarse en su casa y a hacer uso de las tecnologías de la información de manera brusca, muchos desconociendo buenas prácticas para protegerse de los ciberdelincuentes quienes aprovecharon esta situación, en otras palabras, los delitos migraron también al entorno digital.

Figura 2. Cifras del aumento de la ciberdelincuencia tras la pandemia de COVID-19.



Fuente: elaboración propia de los autores, con datos de: Vita, L. (2020). *Los delitos cometidos por medios informáticos crecieron 83% por cuenta de la pandemia*. Recuperado de Asuntos Legales: https://www.asuntoslegales.com.co/consumidor/los-delitos-cometidos-por-medios-informaticos-crecieron-83-por-cuenta-de-la-pandemia-3099101

Dado este panorama, los delitos informáticos merecen ser un tema de especial atención por parte del Gobierno Nacional y el Congreso de la República, pues en el mundo actual las tecnologías van avanzando en un abrir y cerrar de ojos, las personas en segundos tienen acceso a información de toda índole por medio de buscadores de internet e inteligencia artificial que con solo ingresar una palabra

proveen de una gran cantidad de información para satisfacer la inagotable curiosidad humana; esto es un avance natural de la tecnología, pero puede generar algunas irregularidades en esta clase de medios en donde todas las personas sin limitación alguna tienen acceso, quienes no solo utilizan estos servicios de forma correcta sino que se encaminan a lo ilegal y afectar los bienes jurídicos de la colectividad (Bechara, Mosquera, & Ledezma, 2020) y, como se ha mencionado en repetidas ocasiones, parece que la pandemia llegó como una especie de catalizador de estos delitos, y constantemente le recuerda a la sociedad la poca importancia que se le ha dado a estas conductas.

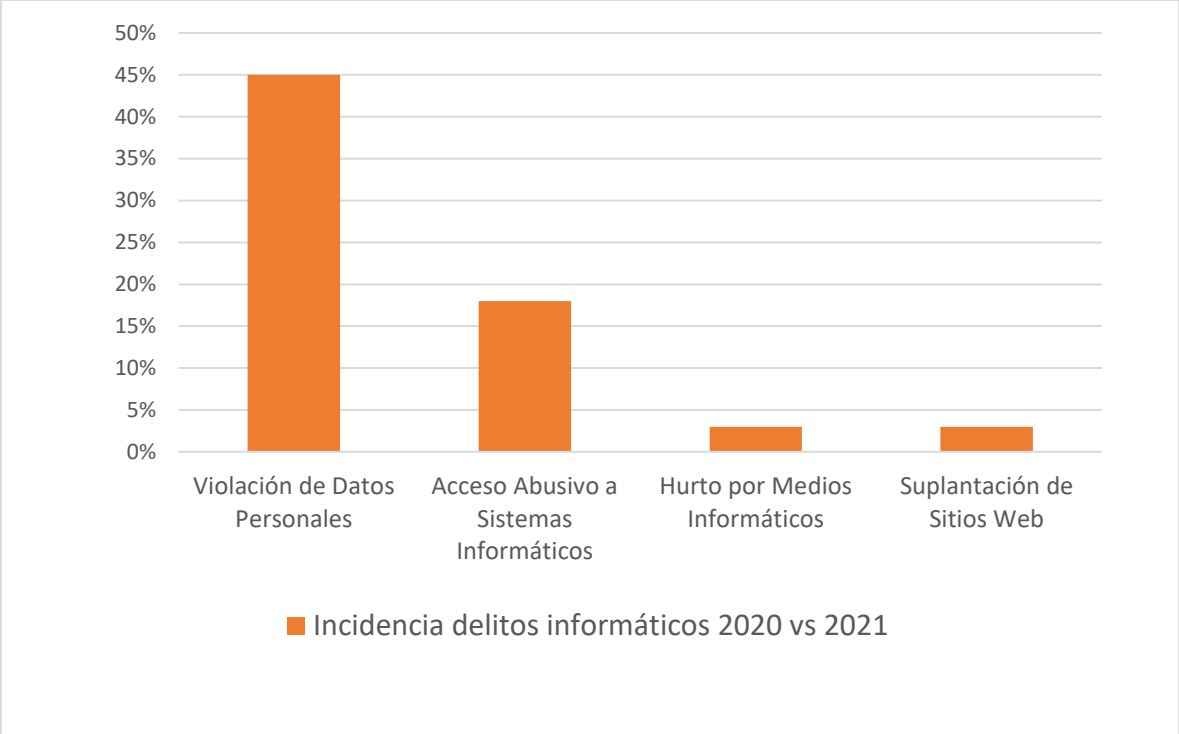
Y claro está, no es posible negar que, en un país donde los asesinatos, el narcotráfico, las estructuras de crimen organizado, la violencia intrafamiliar y de género están a la orden del día, es difícil exigirle a entidades como la Fiscalía General de la Nación que se vuelquen a atender casos en los que a una persona le llegó un correo electrónico de spam; sin embargo, Colombia no puede permitir que estas modalidades criminosas se tomen el país, pues como se ha referenciado, cada vez son más las funciones que tiene internet, y el omitir los controles legales a estas conductas punibles, podría poner en jaque miles de operaciones, que harían incluso tambalear a la estructura económica y social del Estado.

Ahora, si bien queda claro que los delitos cometidos por medios informáticos se dispararon por cuenta del aislamiento, es importante señalar que no sucedió lo mismo con la tasa de esclarecimiento de estos. De hecho, ocurrió lo contrario, pues las cifras muestran que, con corte al 17 de noviembre de 2020, se habían realizado 135 capturas por estos delitos. Esta cifra, en comparación con las 231 capturas realizadas en el mismo periodo de 2019, representa una caída de 42%. Lo anterior obedece a dos factores, que no solo se presentaron en Colombia sino también a nivel global, en primer lugar, la pandemia ocasionó traumatismos en muchos sectores, entre ellos el judicial y el carcelario, lo que ha generado una dilatación en el desarrollo de actividades en contra de los cibercriminales. En segundo lugar, la complejidad en la investigación de los delitos informáticos, ya que el anonimato es

un factor que en muchos casos está presente a favor de los cibercriminales, (Vita, 2020 citando a Ramírez, 2020).

Para el periodo 2021-2022, las cifras obtenidas tampoco son alentadoras, de hecho, los reportes de las autoridades competentes han evidenciado que la práctica criminosa se está afianzando con fuerza en el país, encontrando cada vez más víctimas y burlando las estrategias de seguridad existentes, por lo cual se obtienen cifras como las siguientes:

Figura 3. Incidencia de delitos informáticos de 2020 a 2021:



Fuente: elaboración propia de los autores, con datos de: Equipo TicTac (2022). *Tendencias del Cibercrimen 2021-2022*. Recuperado de TicTac: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

La pregunta por las causas de estos hecho puede tener muchas visiones, sin embargo, (Cortés, Ballén, & Duque, 2015) explican que existe una amplia ignorancia de la población con respecto a estas conductas, y la posibilidad que tienen de llevarlas ante el Estado, para que brinde una solución jurídica a este hecho, lo que significa que las personas rara vez denunciarán un hecho delictivo de carácter

informático, por otro lado, se evidencia, conforme a las investigaciones consultadas, que entidades como la Fiscalía General de la Nación o el Cuerpo Técnico de Investigación, no cuentan con suficiente personal encargado de la investigación de este tipo de conductas penales, así como un desconocimiento y falta de capacitación generalizado por parte de la Rama Judicial, de la naturaleza de estos hechos y las posibilidades jurídicas de enfrentarlos; todo esto crea una cadena de eslabones o errores, que permite la proliferación activa de los cibercrímenes en el país.

Cuando se mencionan las consecuencias, ya en este artículo se ha esbozado qué puede ocurrir en un espacio donde los delitos informáticos son ignorados –incluso tolerados-, y es que, es evidente que en el país existe una importante disparidad entre los delitos ocurridos, denunciados y efectivamente justiciados, así, el informe de Norton -importante empresa multinacional de seguridad informática- en el año 2012 calcula que en Colombia hay unas 9,7 millones de personas víctimas de delitos informáticos, y que tuvieron pérdidas financieras directas por un monto de 79.180 millones de pesos (Norton, 2012).

Por cada segundo, 18 adultos son víctimas de un delito informático lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial. Lo anterior, con pérdidas totales de 197 dólares por víctima en el mundo. En los últimos doce meses, aproximadamente 556 millones de adultos en todo el mundo fueron víctimas de los delitos informáticos, más que la población completa de la Unión Europea. Esta cifra representa el 46% de los adultos que se conectan a la red y que han sido víctimas de delitos informáticos en los últimos doce meses, a la par con los resultados del año 2011 (45%) (Norton, 2012).

Ahora, en años más recientes, el informe de amenazas globales de Fortinet, ha indicado que, en 2022, en América Latina existieron más de 360.000 millones de intentos de ciberataques en el segundo semestre de aquel año, de estos, en el caso de Colombia, el país recibió 20.000 millones de intentos de ciberataques en 2022, lo cual representa un crecimiento del 80% frente a 2021, así mismo, de acuerdo con el Informe Global de Brecha de Habilidades en Ciberseguridad de 2023, la cantidad

de organizaciones que experimentaron cinco o más infracciones aumentó en un 53 por ciento de 2021 a 2022 (Lesmes, 2023).

En resumidas cuentas, el papel del Estado es clave para ponerle un freno a estos delincuentes, tanto desde la Administración de Justicia y la Investigación Criminal, como desde instituciones como el Ministerio de las TIC, para poder llevar a cabo la persecución criminal, y también importantes campañas de pedagogía y autocuidado de la población con respecto a los cibercriminales, y cómo impedir que realicen sus fechorías, o al menos disminuir los efectos dañinos de las mismas.

CAPÍTULO II. OTRAS CONDUCTAS DELICTIVAS INFORMÁTICAS EN EL PAÍS; LIMITANTES DE COLOMBIA EN LA MATERIA

Entendiendo así el papel que ha tenido la regulación en materia de delitos informáticos en la actualidad jurídica del país, es importante abrir la pregunta de si esta poca utilización tiene que ver, precisamente, con que la norma no alcanza a cubrir la enorme cantidad de conductas antijurídicas que pueden realizarse a través de las tecnologías, esta afirmación no es de poca monta, porque si se compara la literatura técnica y la legislación penal foránea se advierte de manera preocupante la falta de castigo para comportamientos que, sin duda alguna, ponen en peligro efectivo o lesionan la seguridad de la información y los sistemas informáticos, además de otros bienes jurídicos, dada la pluriofensividad de estos comportamientos criminales (Maya, 2018).

Nuestro país ha logrado avances en la materia, el legislador trató con la Ley 1273 de 2009, de reglamentar todo lo posible sobre los delitos informáticos para salvaguardar el bien jurídico tutelado “de la protección de la información y de los datos”. Esta norma está estructurada en dos capítulos, el primero de los cuales tipificó “los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y el segundo “los atentados informáticos y otras infracciones”. En ellos se incorporan, entre otros, los delitos de hurto por medios informáticos y semejantes y la “transferencia no consentida de activos”. En

el segundo capítulo encontramos las circunstancias de agravación punitiva, las cuales son aplicables a todos los tipos penales descritos en el Título VII de la Ley 599 de 2000.

Sin embargo, el poco conocimiento de la cultura informática es un factor crítico en el impacto de los delitos informáticos de la sociedad en general, pues los cambios constantes en este tipo de tecnologías conllevan mayores conocimientos en tecnologías de la información, las cuales asienten tener un marco de referencia admisible para el manejo de dichas situaciones. Además, debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de estos ya que, a nivel general, se tiene escasa experiencia en el manejo de esta área por parte de los juristas, y es por ello que los cambios normativos deben ser constantes.

Ahora el artículo 269I de la Ley 1273 consagra el delito de hurto por medios informáticos, con el fin de proteger el patrimonio económico de los ciudadanos, instituyendo que quien superando medidas de seguridad informáticas, ejecute la conducta señalada en el artículo 239 (hurto) maniobrando un procedimiento 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.

Hay que precisar que antes de la expedición de la Ley 1273 del 2009, el Código Penal en distintas normas hacía referencia a la descripción de conductas punibles ejecutadas utilizando medios informáticos, no explícitamente dentro de un título como tal, sino que estas se hallaban dispersas por varios de ellos; y el procedimiento penal que se concedía al mismo, era el de hurto simple (artículo 239); situación que cambio con la entrada en vigencia de esta nueva ley, pues en ella se consagra el tratamiento penal, como el de un hurto calificado, consagrado en el artículo 240 de la Ley 599 de 2000 (Bechara, Mosquera, & Ledezma, 2020).

Esta importante apreciación, permite entrever que en Colombia sí se han encaminado esfuerzos para luchar contra esta problemática, no obstante, el avance de la cultura digital es cada vez más alto y, como ocurre en muchas ocasiones en el derecho, la realidad termina superando la capacidad reguladora del mismo, pues

la norma termina teniéndose que ajustar, a veces con mucho afán, a la sociedad que está siendo aquejada por conductas criminosas, que, los legisladores de hace algunos años, nunca hubiesen podido prever; de hecho, los delitos informáticos usualmente son el ejemplo por excelencia en la academia para ilustrar esta situación.

Dicho lo anterior, es posible notar que en Colombia la herramienta legislativa se ha quedado corta, y así, por ejemplo, un Juez Penal no podría condenar por ciberacoso o pishing, pues estaría prevaricando (Maya, 2018). Es necesario tener en cuenta que la Ley rectora del delito informático en Colombia -1273 de 2009-, está próxima a cumplir catorce años de vigencia y, como se dijo ya, la realidad tecnológica es mucho más rápida que cualquier Congreso o Parlamento, y por ello se observa que las herramientas de judicialización se van quedando rezagadas en el tiempo, con respecto a las conductas que aquejan el seno de la colectividad.

CONDUCTAS NO TIPIFICADAS DE MANERA AUTÓNOMA

Por esta razón, parece fundamental señalar que ya algunos autores han levantado su voz y formulado propuestas concretas de reforma del Código Penal, para dar cobertura a las diferentes conductas novedosas en materia de cibercriminalidad, especialmente, el doctor Ricardo Posada Maya, en "Conductas No Tipificadas de Manera Autónoma" (2018), se ocupa de señalar algunas como:

- *Uso, posesión o tráfico de contraseñas para computadores, redes o sistemas informáticos.*[1]
- *Ciberterrorismo*.[2]

[1] El Convenio de Budapest prevé en su artículo 6º (abuso de dispositivos), que se penalicen las conductas de producción, venta, importación, distribución u otras dirigidas a obtener una contraseña (de ordenador), un código de acceso o datos informáticos similares que le permitan al criminal realizar un delito posterior de acceso abusivo a un sistema informático, o delitos posteriores

[2] La difusión de información falsa con fines de generar "indignación" "descontento" y "estallidos sociales" ha generado una ola de violencia masiva en varios países del mundo, particularmente en América Latina, siendo una conducta clara de ciberterrorismo.

- *Robo, suplantación o usurpación de identidad informática.*[3]
- *Cyberstalking – Cyberbullying.*[4]
- *Phishing.*[5]
- *Uso de equipos para la invasión electrónica de la privacidad (Hacker-Tools)*[6] (Maya, 2018)

Visto lo anterior, es dable entender que, como se ha insinuado desde el inicio de este trabajo, la realidad de la tecnología sigue superando a la capacidad legislativa de los Estados, por ello es que aparecen estas conductas, muchas desconocidas o ignoradas por gran parte de la población pero que, sin duda, están afectando de forma importante a la sociedad en sí misma (Vita, 2020); es necesario entonces reconocer la existencia de estas y muchas otras más conductas que están poniendo

[3] Esta propuesta de tipo penal iría de la mano con la primera acá referenciada, y buscarían proteger información que se encuentra encriptada o interna en una base de datos, servidor o software, pero no existiría ya para castigar la obtención, uso y tráfico de contraseñas, sino acciones más orientadas a la estafa, como es, por ejemplo, la suplantación de una persona ante una entidad pública o privada para obtener datos que solo ella podría obtener, o la manipulación fraudulenta de todo tipo de servidores para tratar de reemplazar a una persona autorizada, con el fin de acceder ilícitamente a datos, dineros u otro tipo de beneficios.

[4] Desde hace muchos años que se acosa a las personas por estos medios, pues, así como internet representa una oportunidad para expresar ideas, propuestas y puntos de vista, lastimosamente también es usado para el matoneo; según cifras del CyberBullying Research Center (Estados Unidos), así lo ha experimentado el 28% de más de 20.000 adolescentes encuestados por el portal investigativo en colegios de los Estados Unidos entre 2007 y 2016. Esta cifra aumentó en los últimos años y llegó a 33.4% en 2016.

[5] En su fenomenología usual, los criminales denominados phisher se hacen pasar por empleados de empresas o de entidades bancarias de confianza, que hacen llamadas telefónicas, utilizan malware, envían mensajes de texto o correos electrónicos (smishing), aparentando entablar comunicaciones comerciales u oficiales electrónicas legítimas con el fin de engañar a las personas, ganarse su confianza y obtener su información personal o confidencial, por ejemplo: información detallada de la tarjeta de crédito o débito, u otras claves o contraseñas mediante el ingreso a páginas web que descargan códigos maliciosos.

[6] Se trataría, por ejemplo, del uso no autorizado de equipos rastreadores o de vigilancia, de invasión a las cámaras web de los equipos de comunicaciones, del uso de relojes con cámaras para la obtención de claves de cajeros, o la intrusión a los equipos celulares para obtener la ubicación de los sujetos que intervienen en comunicaciones privadas.

en riesgo los bienes jurídicos de la ciudadanía, para ajustar la legislación y dejarla más acorde al momento histórico que se está viviendo.

Debe decirse, incluso, que la lista que se propuso líneas atrás es meramente enunciativa, y recoge los planteamientos de uno de los autores más autorizados en el tema en el país, sin embargo, esto no quiere decir que sean las únicas conductas criminosas que se están llevando a cabo actualmente en Colombia y el mundo, puesto que, a la par que avanzan las tecnologías, también avanza la criminalidad, como ejemplo de ello, recientemente se pudo conocer que en los Estados Unidos, delincuentes están haciendo uso de las herramientas de Inteligencia Artificial (AI) para grabar la voz de una persona y generar mensajes de pánico o urgencia, con fines de solicitar dinero de sus familiares (Avendaño, 2023), una modalidad de *Phishing "tío tío*"[7] potenciada altamente por el avance tecnológico.

Así pues, el panorama es amplio, pero ante la creciente amenaza cibercriminal, el Estado a través del ordenamiento jurídico, debe liderar la avanzada por la protección de los bienes jurídicos de sus ciudadanos, previniendo los riesgos, conociendo las causas y anticipándose a las consecuencias de la proliferación masiva de estas conductas, garantizando un desarrollo tecnológico seguro para toda la colectividad en general.

CAPÍTULO III. NECESIDAD DE ACTUALIZACIÓN NORMATIVA EN EL PAÍS: COLOMBIA COMO PARAÍSO DEL CIBERCRIMEN

En el mundo actual es frecuente escuchar la expresión "Paraíso Fiscal", esta hace referencia a un territorio que ofrece a individuos y empresas extranjeras poca o ninguna carga tributaria en un entorno estable política y económicamente, además,

[7] Refiere a una modalidad del delito de Phishing, en la cual el cibercriminal se contacta con una persona, y se hace pasar por un familiar, especialmente por un sobrino, y le explica que se le ha presentado una urgencia, ha tenido un accidente o algo similar, solicitándole el envío de un dinero a una determinada cuenta para sacarlo de algún apuro.

esto lo suelen combinar con que proporcionan poca o ninguna información financiera a las autoridades fiscales extranjeras (BBC News Mundo, 2021).

En ese orden, un paraíso fiscal ofrece un sistema legal flexible y que se esfuerza por proteger la privacidad de sus inversores con el fin de dificultar las eventuales investigaciones que se realicen en los países originarios de las inversiones allí asentadas; dicho de otra forma, los paraísos fiscales tienen sistemas regulatorios débiles a fin de facilitar el ocultamiento de riqueza por parte de los no residentes, como medida para incentivar la migración del capital a sus territorios.

Los paraísos fiscales no son ilegales, puesto que son territorios independientes que soberanamente han implementado una legislación fiscal favorable para los extranjeros que allí se instalen o inviertan; la ilegalidad surge del extranjero que invierte allí con respecto a la legislación de su país de origen (BBC News Mundo, 2021). Así, por ejemplo, no es ilegal que un colombiano tenga inversiones en un paraíso fiscal, pero sí sería ilegal que ese colombiano oculte su patrimonio en el paraíso fiscal, es decir, que no declare en Colombia que tiene patrimonio allí.

Dicho lo anterior, es posible considerar de forma análoga la existencia de países que puedan llegar a verse como “Paraísos criminales”, los cuales serían aquellos que ofrecen a individuos y grupos al margen de la ley poca o ninguna legislación penal en cierto tipo de delitos, combinado con una estructura judicial deficiente que permita la ejecución continuada y estable de ciertas conductas punibles, particularmente, de los conocidos como delitos informáticos.

Nuevamente, la existencia de una regulación jurídica deficiente, o incluso la inexistencia de esta para ciertos delitos, resulta ser, a fin de cuentas, una expresión soberana de cualquier Estado, así, es muy fácil ver cómo cada nación legisla únicamente según sus necesidades actuales y apremiantes, el problema real está en que, en el siglo XXI, pocos son los asuntos que se quedan dentro de la órbita interna de cada país, ya que la globalización ha hecho de las suyas, y un evento, por aislado que parezca, puede acabar teniendo efectos impensables al otro lado del globo.

Con esto en mente, resulta necesario considerar la situación actual de Colombia con respecto a los delitos informáticos, así, a lo largo de este trabajo se ha observado que en el país existe una regulación –la Ley 1273 de 2009-, también existe una norma procesal –la Ley 906 de 2004-, y que existen numerosas preocupaciones desde la academia por atajar esta problemática, sin embargo, la regulación vigente se ha evidenciado como desactualizada y ajena a la realidad de Colombia y el mundo (Bechara, Mosquera, & Ledezma, 2020), por su parte, la legislación procesal también ha mostrado grandes falencias, especialmente desde el ente investigador y la administración de justicia, quienes han visto el delito informático como uno de baja importancia, que no requiere mayor atención (Cortés, Ballén, & Duque, 2015), situaciones que, si se comparan, resultan siendo idénticas a lo que sucede a nivel tributario con los denominados Paraísos Fiscales, así, Colombia podría estar comenzando a convertirse en un Paraíso Criminal para ciberdelincuentes.

De hecho, para el año 2022, Colombia fue el segundo país de América Latina que más ciberataques tuvo, según reveló el informe de seguridad de IBM, que es el anual X-Force Threat Intelligence Index; en esa línea, sobre los sectores más afectados, el comercio minorista y mayorista fueron los más atacados, también, finanzas y seguros fue el segundo sector más atacado en 2022 con el 24% de los casos, seguido por energía y manufactura, ambos con un 20% (Lesmes, Colombia, el segundo país de América Latina con más ciberataques en 2022, 2023).

Entonces, es claro entrever que los ataques cibernéticos en Colombia están en aumento, por ello, las empresas e incluso la Administración Pública necesitan más y mejores estrategias, donde no se trate solamente de saber cómo reaccionar a un ciberataque sino cómo prevenirlo, y entender que, desde el Presidente de una compañía, hasta los colaboradores de áreas no relacionadas con tecnología, deben ser el filtro número uno para blindar a la organización; y ni qué decir de las personas naturales, que resultan siendo las principales víctimas de este tipo de delincuentes.

En Colombia los ciberdelincuentes explotan las conversaciones por correo electrónico, la tasa de intentos mensuales a nivel mundial aumentó 100% y en la

región, el secuestro de conversaciones de e-mail representó el 11% de los ataques; en el caso de la extorsión, se volvió el método preferido de los ciberdelincuentes que atacan principalmente a los sectores, empresas y regiones más vulnerables usando esquemas de extorsión y aplicando una alta presión psicológica para forzar a las víctimas a pagar (Lesmes, Colombia, el segundo país de América Latina con más ciberataques en 2022, 2023).

Por ello es que (Lesmes, 2023 citando a Robles, 2023) ha dicho que:

> *Colombia se ha convertido en un país atractivo para los ciberatacantes porque hay empresas con un alto volumen de usuarios, y justamente ellos van tras los datos, que hoy en día valen muchísimo. Cuidar nuestros datos personales es vital, pero a su vez, se necesita que las empresas inviertan en herramientas con tecnologías como Inteligencia Artificial.*

Siendo así, la situación actual se ve preocupante en muchos aspectos, pero el más grave, sin duda, es que a pesar del aumento de estas conductas, no se está viendo una respuesta ágil y suficiente por parte del Estado, al contrario, la evidencia estudiada enseña que es poca la preocupación que despierta en las autoridades estos delitos, por tanto, no sería de extrañar que las mismas continuaran aumentando exponencialmente en el país, consiguiendo un número mayor de víctimas e incluso, convirtiendo a Colombia en una especie de centro de operaciones para grupos organizados al margen de la ley que aprovechen la situación actual de regulación deficiente, para ejecutar sus crímenes incluso en otras naciones, sabiendo que, con toda probabilidad, sus acciones quedarán en la impunidad.

Por ello, y ya desde la perspectiva puntual de Colombia, se puede afirmar que existe la necesidad de un esfuerzo articulado entre la Administración Pública, la Rama Legislativa y la población civil, para tipificar, denunciar, investigar y sancionar un espectro mayor de las conductas delictivas realizadas por medios informáticos, lo cual requiere, sin duda, una modernización de la Fiscalía General de la Nación y la Policía Nacional, para que dejen de considerar a los delitos informáticos como

delitos de poca relevancia, y comiencen a darles la importancia que han adquirido y adquirirán en los tiempos venideros.

Como ya se ha dicho previamente, las tecnologías son necesarias para el desarrollo del país, y el Estado se encuentra en la obligación de promoverlas, facilitarlas y acercarlas a la población, pero en el mismo sentido, tampoco es posible permitir que el avance de los sistemas informáticos se traduzca en lesiones a los bienes jurídicos protegidos por la legislación, así, todas las Ramas del Poder Público deben dirigir sus esfuerzos a producir una normativa eficaz, eficiente, actualizada y consciente de la realidad contemporánea, que permita obtener un avance ordenado y legal de la tecnología, disminuyendo al máximo posible los riesgos derivados de ella.

CONCLUSIONES

En definitiva, la regulación de los delitos informáticos en Colombia, representada por la Ley 1273 de 2009 que creó el Título VII Bis del Código Penal, sigue siendo una norma de vital importancia en el contexto actual de la cibercriminalidad en Colombia, sin embargo, el avance actual de las tecnologías hace que su vigencia y eficacia sea replanteada, puesto que la norma en vigor no alcanza a cubrir todo el espectro de la actividad punible en esta materia que se da en el país.

En ese mismo sentido, es clave para el análisis entender que el mundo cada vez se desplaza más hacia una digitalización absoluta y, por ello, los ordenamientos jurídicos deben estar listos para prevenir actividades que puedan alterar el orden y el derecho de las personas, que se ejecuten a través de estos medios, prueba de ellos fue la pandemia de COVID-19, ya que las medidas orientadas a su mitigación obligaron a aumentar en gran medida el uso de las herramientas digitales en todo el mundo, aumentándose, de forma subsiguiente, la cibercriminalidad.

Así pues, es claro también que deben dirigirse esfuerzos eficaces y céleres por parte de la Administración Pública, que bien podrían también tomar la forma de campañas de pedagogía y acompañamiento a la población -en especial a sujetos de especial

protección, como los adultos mayores y los menores de edad-, para concientizarlos acerca de estas modalidades delictivas, para que estén alerta y eviten ser víctimas de los criminales que se valen de la tecnología para llevar a cabo sus fechorías.

Por su parte, es necesario que desde el Gobierno Nacional se lideren todo tipo de actuaciones encaminadas al abordaje intersectorial de esta problemática, basada en las investigaciones, la organización de foros, congresos, simposios, el reclutamiento de comités de expertos, entre otros, para analizar las posibilidades de reforma al Código Penal, actualización jurisprudencial de tipos penales, revisión de los tipos existentes, entre otras acciones que permitirían dotar de mayor vigencia a la ley penal, para así poder dar cumplimiento real a las necesidades de una población cada vez más acosada por el delito tecnológico.

Finalmente, no debe dejarse de lado que la población civil también está llamada a hacer parte de esta tarea y es que, desde su posición, se encuentra también llamada a estar atenta a estas modalidades de delitos, apoyarse en redes comunitarias para denunciar la aparición de nuevas conductas, disminuir el envío masivo de noticias faltas a través de las redes, procurar la búsqueda de información real y confiable y difundir información cierta y clara acerca de cómo prevenir el ataque criminal informático; sin abandonar nunca, claro está, el deber de denunciar que acompaña siempre a todo ciudadano y que será crucial en esta lucha fundamental en el siglo XII, una que, en realidad, apenas acaba de comenzar.

REFERENCIAS

Aránguez, T. (2016). *¿Qué es el método hermenéutico?* Recuperado el 09 de Septiembre de 2023, de La Galería de los Perplejos: https://arjai.es/2016/08/24/que-es-el-metodo-hermeneutico/

Avendaño, P. (08 de Marzo de 2023). Ciberestafadores utilizarían IA para imitar las voces de familiares y robar. *El Tiempo*. Recuperado el 06 de Septiembre de

2023, de https://www.eltiempo.com/mundo/eeuu-y-canada/ciberestafadores-utilizarian-ia-para-imitar-las-voces-de-familiares-y-robar-748381

BBC News Mundo. (4 de Octubre de 2021). *Pandora Papers: qué son los paraísos fiscales y cuándo es ilegal usarlos*. Recuperado el 01 de Octubre de 2023, de BBC News Mundo: https://www.bbc.com/mundo/noticias-58794908

Bechara, Y. Y., Mosquera, A. Y., & Ledezma, E. E. (2020). *Análisis Jurídico de la Ley 1273 de 2009 y el surgimiento y expansión del Delito de Hurto y Semejantes por Medios Informáticos.* Recuperado el 10 de Septiembre de 2023, de Universidad Cooperativa de Colombia: https://repository.ucc.edu.co/bitstream/20.500.12494/36449/7/2020_delito_hurto_informatico.pdf

Constitución Política de Colombia. (1991). Recuperado el 05 de Septiembre de 2023, de http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Cortés, R., Ballén, J., & Duque, J. (Diciembre de 2015). La persecución judicial contra los delitos informáticos en el Distrito Judicial de Villavicencio. *Derecho, Comunicaciones y Nuevas Tecnologías - Universidad de los Andes*. Recuperado el 25 de Septiembre de 2023

Duque, González, Cossio, & Martínez. (2018). *Investigación en el saber jurídico.* Recuperado el 09 de Septiembre de 2023, de Universidad de Antioquia: https://unilibros.co/gpd-investigacion-en-el-saber-juridico.html

Equipo TicTac. (2022). *Tendencias del Cibercrimen 2021-2022.* Recuperado el 18 de Septiembre de 2023, de TicTac: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

García, L. (11 de Mayo de 2020). *Deutsche Welle*. Recuperado el 01 de Octubre de 2023, de https://www.dw.com/es/c%C3%B3mo-aprovechan-los-ciberdelincuentes-la-crisis-del-coronavirus/a-53393723

Lesmes, L. (10 de Abril de 2023). *Colombia recibió 20.000 millones de ciberataques en 2022.* Recuperado el 18 de Septiembre de 2023, de El Tiempo: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberseguridad-en-colombia-datos-sobre-ciberataques-en-el-pais-757651

Lesmes, L. (1 de Marzo de 2023). *Colombia, el segundo país de América Latina con más ciberataques en 2022*. Recuperado el 05 de Septiembre de 2023, de El Tiempo: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-el-segundo-pais-con-mas-ciberataques-en-2022-746276

López, J. M. (11 de Septiembre de 2023). *Ciberataques subieron 65% siendo los bancos e industriales sus blancos más comunes.* Recuperado el 19 de Septiembre de 2023, de La República: https://www.larepublica.co/empresas/reporte-ciberseguridad-2023-a-empresas-y-sectores-3701737

Maldonado, R. (2016). *El Método Hermenéutico en la Investigación Cualitativa.* Recuperado el 09 de Septiembre de 2023, de Universidad de Concepción: https://www.researchgate.net/publication/301796372_EL_METODO_HERMENEUTICO_EN_LA_INVESTIGACION_CUALITATIVA

Maya, R. (2018). La Diferencia entre Delitos Informáticos y Cibercrímenes. En R. Maya, *Los cibercrímenes: un nuevo paradigma de criminalidad.* Bogotá D.C.: Editorial Ibáñez. Recuperado el 13 de Septiembre de 2023, de https://vlex.cesproxy.elogim.com/#/search/jurisdiction:CO/Los+cibercr%C3%ADmenes%3A+un+nuevo+paradigma+de+criminalidad/WW/vid/777443729

Norton. (2012). *Norton Cybercrime Report 2012.* Recuperado el 01 de Septiembre de 2023, de Norton: https://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Novoa, P. (29 de Septiembre de 2021). *La información: llegó la hora de tratarla como activo empresarial.* Recuperado el 01 de Septiembre de 2023, de Ámbito Jurídico: https://www.ambitojuridico.com/noticias/ambito-del-lector/la-informacion-llego-la-hora-de-tratarla-como-activo-empresarial

Ospina, M. R., & Sanabria, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, 199-217. Recuperado el 13 de Septiembre de 2023, de https://dialnet.cesproxy.elogim.com/servlet/articulo?codigo=7667839

Revista Semana - Tecnología. (08 de Abril de 2020). Delitos informáticos aumentaron en Colombia durante la cuarentena. *Revista Semana*. Recuperado el 01 de Septiembre de 2023, de https://www.semana.com/on-line/tecnologia/articulo/delitos-informaticos-aumentaron-en-colombia-durante-la-cuarentena/662686/

Sutton, A. (2016). *La pregunta de investigación en los estudios cualitativos.* Recuperado el 09 de Octubre de 2023, de Investigación en Educación Médica: https://doi.org/10.1016/j.riem.2015.08.008

Varón, G. (16 de Abril de 2008). *Congreso de la República de Colombia*. Recuperado el 23 de Septiembre de 2023, de http://leyes.senado.gov.co/proyectos/index.php/proyectos-ley/periodo-legislativo-2006-2010/2007-2008/article/283-por-medio-de-la-cual-se-modifica-el-codigo-penal-se-crea-un-nuevo-bien-juridico-tutelado-denominado-de-la-proteccion-de-la-informacion-y-de-lo

Vita, L. (09 de Diciembre de 2020). *Los delitos cometidos por medios informáticos crecieron 83% por cuenta de la pandemia*. Recuperado el 05 de Octubre de 2023, de Asuntos Legales: https://www.asuntoslegales.com.co/consumidor/los-delitos-cometidos-por-medios-informaticos-crecieron-83-por-cuenta-de-la-pandemia-3099101