EFICACIA DEL ESTADO COLOMBIANO PARA LA JUDICIALIZACIÓN DE LOS DELITOS POR MEDIOS INFORMÁTICOS.[1]

José Daniel Escudero Patiño.[2]

María Camila León Gómez.[3]

Paulina Metaute Gil.[4]

RESUMEN

La tecnología ha facilitado el manejo del mundo cibernético, sin embargo, ha traído grandes riesgos en lo concerniente a la protección de los datos y la información, atentados informáticos y múltiples infracciones que versan directamente sobre el cibercrimen. En este estudio, se describe la evolución normativa en materia de delitos informáticos y su gestión en el proceso penal en el marco del sistema jurídico colombiano; destacando la relevancia de la Ley 1273 del 2009 donde se creó el nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-, ley que es vital para la persecución de delitos informáticos en el Estado colombiano.

Por la incidencia social, política y económica de los ciberdelitos, se hace un recuento de los procesos por medio de los cuales la ciudadanía puede tener acceso a la justicia.

En Colombia, existen diferentes procedimientos para que la ciudadanía puede denunciar, igualmente, se han dispuesto instituciones encargadas de investigar, judicializar y tratar los

[1] Artículo de revisión bibliográfica para optar por el título de abogado en la Universidad Luis Amigó. Asesora metodológica: Laura Victoria Cárdenas Rojas – Asesor temático: Dany Steven Gómez Agudelo.

[2] Estudiante de Derecho y Ciencias Políticas de Noveno semestre de la Universidad Católica Luis Amigó, Email: jose.escuderopa@amigo.edu.co. Código ORCID: https://orcid.org/0000-0002-1859-0868https://orcid.org/0000-0002-1859-0868

[3] Estudiante de Derecho y Ciencias Políticas de Noveno semestre de la Universidad Católica Luis Amigó, Email: maria.leonom@amigo.edu.co. Código ORCID: https://orcid.org/0000-0002-5253-6822

[4] Estudiante de Derecho y Ciencias Políticas de Noveno semestre de la Universidad Católica Luis Amigó, Email: paulina.metautegi@amigo.edu.co. Código ORCID: https://orcid.org/0000-0002-6570-2789

delitos informáticos. Sin embargo, el país debe seguir fortaleciendo estos mecanismos para combatir eficazmente el cibercrimen.

PALABRAS CLAVES: Delitos informáticos; denuncia; entorno jurídico; judicialización; Ley 1273 del 2009; medios informáticos.

ABSTRACT

The technology has facilitated the management of the cybernetic world, however, it has brought great risks in terms of data and information protection, computer attacks and multiple infractions that deal directly with cybercrime. In this study, the normative evolution in the matter of computer crimes and its management in the criminal process in the framework of the Colombian legal system is described; highlighting the relevance of Law 1273 of 2009 where the new protected legal asset was created -called "of the protection of information and data"-, a law that is vital for the prosecution of computer crimes in the Colombian State.

Given the social, political and economic impact of cybercrime, an account is taken of the processes through which citizens can have access to justice.

In Colombia, there are different procedures for citizens to report, and institutions have been set up to investigate, prosecute and deal with computer crimes. However, the country must continue to strengthen these mechanisms to effectively combat cybercrime.

KEYWORDS: Computer crime; computer media; denunciation; legal environment; judicialization; Law 1273 of 2009.

INTRODUCCIÓN

El mundo cibernético juega un papel de gran importancia en la sociedad, esto de cara a que la red y nuevas tecnologías que crecen cada día de forma exponencial, han permitido que la población mundial, en su vida cotidiana implemente de una forma habitual el uso de medios tecnológicos conectados a la red de internet para realizar todo tipo de actividades, donde se tiene acceso a infinidad de datos e información con solo dar un click.

Constantemente las instituciones, empresas, entidades, mercados y personas usan la era digital como una llave que abre las puertas al mundo virtual, convirtiéndose en una herramienta fundamental para el almacenamiento de datos o información y las comunicaciones, que impulsan grandes cambios en el mundo actual.

> Con cada vez mayor frecuencia y mayor impacto, los dispositivos de almacenamiento y procesamiento de información llámense servidores, estaciones de trabajo o simplemente PC son vulnerados en sus elementos más sensibles, dejando expuestos no sólo múltiples y significativos datos de distinto valor (financiero, crediticio, estratégico, productivo…), sino los mismos patrimonios reales de personas y organizaciones y, aún más, su dignidad, su honra y su vida. (Ojeda, Rincón, & otros, 2010, pp. 43).

Con el crecimiento de las TIC[5], de forma más frecuente el mundo se encuentra expuesto a diferentes vulneraciones que se llevan a cabo a través del uso inadecuado de medios informáticos, obteniendo como resultado el progresivo aumento de la ciberdelincuencia, denotando la necesidad de regularlo.

En América Latina como lo relata el informe presentado por la OEA en su Reporte de Ciberseguridad, se identifica como un centro propicio para fraude cibernético[6], donde más de las tres cuartas partes de los países analizados en dicho informe carecen de los planes de ciberseguridad necesarios, contando con una infraestructura débil e ineficaz para hacer frente a los delitos cibernéticos. (2020).

---

[5] Tecnologías de la Información y las Comunicaciones (TIC): Las Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Congreso de la República, 2009).

[6] El fraude cibernético e informático se refiere al fraude realizado a través del uso de una computadora o del Internet. La piratería informática (hacking) es una forma común de fraude: el delincuente usa herramientas tecnológicas sofisticadas para acceder a distancia a una computadora con información confidencial. Otra forma de fraude involucra la intercepción de una transmisión electrónica. (Cornell Law School, S.F.).

En Colombia, los incidentes cibernéticos tuvieron un incremento del 54% en los años 2019-2020, en comparación con el año 2018, según registros de las autoridades. Además, de los 28.827 casos reportados, 15.948 fueron denunciados como infracciones a la Ley 1273 de 2009, que tipifica los delitos informáticos en Colombia. (TicTac & CCIT, 2019).

Es por ello, que en la codificación penal en Colombia plasmada en la Ley 599 del 24 de julio del 2000, sufre una modificación el 07 de enero del año 2009 bajo la Ley 1273, donde se crea y se adiciona el bien jurídico[7] tutelado de la "Protección de la Información y de los Datos", esta ley supone la creación de herramientas más eficaces para garantizar la protección de estos bienes jurídicos tutelados, pero, ¿es el Estado colombiano eficiente para la judicialización de los delitos cometidos por medios informáticos?

Dado lo anterior, el objetivo general se establece en analizar la eficacia que tiene el Estado colombiano en la judicialización de los delitos por medios informáticos, con dos objetivos específicos que son describir la evolución legislativa para la consagración de los delitos informáticos en Colombia, e identificar la gestión de los delitos informáticos en el proceso penal, que se desarrollarán en dos capítulos y que ayudarán a responder la pregunta de investigación planteada.

Este trabajo de investigación es de carácter cualitativo, debido a que ahonda en la comprensión de los delitos informáticos y su aplicación en el campo jurídico, se utilizó el método hermenéutico en razón de que la técnica de recolección de datos seleccionada es la observación y la revisión documental, en la cual se sistematizó y se analizaron los datos para lograr información confiable y objetiva; se pretende estudiar la normatividad en el Estado Colombiano sobre los delitos informáticos y el cibercrimen, teniendo en cuenta la gestión que se les da, con la finalidad de efectuar un análisis de la eficacia que tiene el país para la judicialización de estos delitos.

[7] El bien jurídico, puede entenderse como una condición necesaria, o socialmente concebida como necesaria o útil, para el desarrollo de la vida de las personas y de la sociedad. Sin embargo, solo existe en tanto en cuanto se crea una norma para protegerlo, normalmente estableciendo una sanción para las conductas que puedan vulnerarlo. Cuando no existe dicha norma, el bien carece de carácter jurídico. Por tanto, el bien jurídico es, en todo caso, un bien que goza de protección legal. Aunque toda norma protege un bien considerado digno de protección por el legislador, el bien jurídico goza de mayor relevancia en el ámbito del derecho penal. (Conceptos jurídicos, S.F.).

Igualmente, es clara la importancia de la tecnología en la actualidad debido al constante uso de esta en la vida cotidiana de las personas e intuiciones, de ahí la necesidad de regular mediante el derecho las conductas que pongan en riesgo la seguridad de la información que se encuentre en medios tecnológicos, en virtud de esto, y con el apoyo de las fuentes del derecho, el estudio efectuado es de carácter dogmático jurídico, por que realiza un recuento de la evolución legislativa de Colombia en materia de delitos informáticos, del mismo modo el Estado debe ser eficiente a la hora de regular este tipo conductas para lograr su fin último que en sí, es la justicia y el orden. Esto obedece a que actualmente la información relacionada con el tema de estudio es de gran importancia debido al avance de la tecnología en la época actual y futura.

Este trabajo se desarrolla en dos capítulos que ayudarán a responder la pregunta de investigación planteada. En el primer capítulo podemos dar cuenta del desarrollo evolutivo de la normatividad existente en materia de delitos informáticos en Colombia, donde se evidencia el orden cronológico de dichos preceptos normativos para el establecimiento de los delitos informáticos en la actualidad; en el capítulo final, se disponen los trámites y los procesos llevados a cabo para la judicialización de delitos informáticos, donde se tienen en cuenta, los porcentajes, estadísticas, doctrina y jurisprudencia, para explicar de una forma más asertiva el desarrollo de dichos delitos en el proceso penal, con el propósito de alcanzar la respuesta al objetivo general de la investigación.

EVOLUCIÓN LEGISLATIVA PARA LA CONSAGRACIÓN DE LOS DELITOS INFORMÁTICOS EN COLOMBIA.

La creación del internet fue posible gracias a las redes de comunicación, la idea principal de dicha creación fue la de conectar varios ordenadores, para permitir la comunicación entre varios usuarios, teniendo como resultado, hoy en día, la creación de nuevos medios informáticos, permitiendo la conexión de millones de usuarios en todo el mundo de forma frecuente y cotidiana.

En enero del 2018, el DANE realizó un informe donde presentó las estadísticas de la situación digital de Colombia durante ese año. Dichas cifras permitieron concluir que alrededor de un 52,7% de la población tiene acceso a internet.

> En 2018, el 52,7% de los hogares poseía conexión a Internet para el total nacional; 63,1% para las cabeceras y 16,2% en centros poblados y rural disperso. La conexión a Internet fijo registró mayor proporción de hogares para el total nacional (40,5%) y cabecera (50,8%), respecto a la conexión a Internet móvil. (DANE, 2018).

Con lo anterior, se ha evidenciado el crecimiento considerable de las personas que acceden a internet en Colombia y de los avances tecnológicos, con ello se encuentra un panorama donde las Tecnologías de la Información y de las Comunicaciones (TIC) cada vez permean mayor parte de las actividades que desarrollan los colombianos hoy en día, que, entre otras cosas, implica el riesgo exponencial de sufrir ataques cibernéticos contra su información, sistemas, e incluso, de su integridad.

Es por ello, que se hace necesario definir en primera instancia, ¿Qué son los delitos informáticos?

El derecho no debe ser ajeno a la realidad social prexistente, debido a esto, se deben sancionar las conductas malintencionadas o maliciosas que se realizan por medios informáticos. El instrumento utilizado para ello es la creación de los delitos informáticos que están destinados a la protección de los bien jurídico tutelado de "protección de información y de los datos".

> Julio Téllez-Valdés (2003), en su libro Derecho Informático, enfoca el delito informático desde el punto de vista típico y atípico y lo define como "actitud contraria a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)".
>
> Se podría definir el delito informático como toda acción u omisión culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor, aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la ley, que se realiza en el entorno informático y está sancionado con una pena. (Flores Salgado, L. 2015. Pg. 132).

Desde un momento histórico en Colombia la primera ley que se expidió en relación con los delitos informáticos, fue la Ley 44 de 1993 sobre los Derechos de Autor[8], que conjuntamente y de forma anterior, el Decreto 1360 de 1989 el cual reglamentó la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor, donde se podría inferir como la primera normatividad encargada de sancionar penalmente las conductas que atentan contra los derechos de autor, pero en este caso ligado, a lo concerniente a un delito informático por reproducción no autorizada de software.

Esto sirvió como base para que en el año 2000 el Código Penal Colombiano implementara una modificación adicionando el Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor.

El Código Penal colombiano (Ley 599 de 2000) en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones.

Este título cuenta con nueve capítulos en los que se busca proteger el bien jurídico tutelado antes mencionado, en el capítulo VII, desde el artículo 192 hasta el 197, se presupone la violación a la intimidad, reserva e interceptación de comunicaciones, relacionándose con pequeños rasgos a los delitos informáticos, estos derechos de intimidad y comunicación se encuentran unidos sin posibilidad de ser separados, la Corte Constitucional ha expresado:

> El libre ejercicio del derecho a comunicarse se afecta, hasta el extremo de hacerlo inútil, cuando el contenido de la comunicación carece de la necesaria espontaneidad, por el temor a la injerencia extraña o a la exposición pública del mensaje o del intercambio de expresiones, lo que implica, obviamente, vulneración del derecho, también fundamental, a la intimidad. (Corte Constitucional, Sentencia C-626, 1996).

En Colombia, la Constitución Política establece en el artículo 15 lo siguiente: "La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley." (Asamblea Nacional Constituyente, 1991).

[8] El derecho de autor es la rama de la propiedad intelectual que reconoce, en cabeza de los autores, ciertas prerrogativas morales l y patrimoniales sobre sus obras artísticas y literarias que sean originales, y susceptibles de ser divulgadas o reproducidas por cualquier medio. Se considera creación intelectual aquella que es resultado del desarrollo del intelecto humano de su autor, persona natural quien crea la obra. (Universidad Nacional de Colombia. S.F.).

Quiere decir entonces que solo se pueden intervenir las comunicaciones si se cumplen con unas estipulaciones preexistentes. En materia penal, solo la fiscalía puede ordenar una restricción al derecho de la intimidad por medio de interceptación de las comunicaciones como lo establece el código penal:

> El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación, así como del procesamiento de la misma. Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación (Ley 906, 2004, art. 235).

El juez de control de garantías debe hacer un control previo[9] cuando hay limitaciones a los derechos fundamentales, restricción a la libertad personal, irrupción al domicilio, privacidad y a la intimidad de las personas, exceptuando las violaciones a la intimidad que se encuentran en el artículo 250 de la Constitución Política, donde el control de legalidad[10] realizado se llevaría a cabo de forma posterior[11].

> Resulta claro que aquello que se encuentre dentro del artículo 250 de la Constitución no requiere autorización judicial previa –solo orden de fiscal -, mientras que, para todos los demás procedimientos restrictivos de los derechos fundamentales, el Juez de Garantías ejerce un control previo de todas las diligencias de investigación penal que limitan los derechos fundamentales. (Gómez Agudelo, 2020).

[9] Control previo: Es de tipo preventivo, ya que se verifica antes de la realización del acto. El Juez de Garantías ejerce un control previo de todas las diligencias de investigación penal que limitan los derechos fundamentales. (Corte Constitucional, 2018).

[10] Control de legalidad: Aplica para la prueba mínima para asegurar al que se refiere el artículo 392 en los eventos en que procede la detención preventiva (L. 600/2000, art. 357), está relacionado, por lo tanto, (i) con la suficiencia de la prueba a la luz del cumplimiento del requisito probatorio establecido en el artículo 356, así como, (ii) con la necesidad constitucional de la medida, de conformidad con los fines legítimos que establece el artículo 355 según la doctrina constitucional sentada por esta corporación en la Sentencia C-774 de 2001. (Congreso de Colombia, 2000).

[11] Control posterior: Se da ante el juez de control de garantías y tiene por objeto verificar que la interceptación de comunicaciones como procedimiento de investigación, no haya sido extralimitado en cuanto a su práctica, ni arbitrario en cuanto a su desarrollo. (Barñol, M. 2014. Pg. 54).

En el artículo 197 y 195 del Código penal del 2000, también se tipifica la utilización ilícita de redes de comunicaciones y acceso abusivo a un sistema informático, en el primer caso se presenta un tipo penal de mera conducta, es necesario que se posea equipos de redes de comunicación o de cualquier medio electrónico[12] adaptado para emitir o recibir señales ilícitas, el segundo caso en cambio fue derogado por el artículo 4 de la Ley 1273 del 5 de enero 2009, creándose el artículo 269A del Código Penal, el cual describe de igual forma pero con aumento en la pena el acceso abusivo a un sistema informático.

En el artículo 196 del Código penal, se tipificó la violación ilícita de comunicaciones o correspondencia de carácter oficial, imponiendo una pena de prisión de tres a seis años, el delito hace alusión a la interceptación de las comunicaciones privadas y oficiales, además, con aumento hasta de una tercera parte cuando la correspondencia está destinada o remitida a los organismos de seguridad del Estado.

Fue la Ley 679 de 2001, que estableció el Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con niños menores de edad.

Esta ley se implementó en el año 2001 para regular la comisión de delitos a través de las telecomunicaciones y en especial todo lo que tuviere lugar a delitos con menores de edad, todo ello se llevaría a cabo por medio de expertos en redes globales de información, por otra parte el objetivo por parte del gobierno nacional fue implementar un control preventivo, para evitar la pornografía infantil con fines de explotación infantil, de este modo adoptando medidas, para que las prácticas ilícitas o ilegales que se dieran por medios informáticos tuvieran prohibiciones expresas tales como publicar imágenes, documentos, videos, archivos o cualquier material que implicara exponer actividades sexuales con menores de edad.

Además, dentro de esta misma ley se contempló algunos deberes para todos los habitantes del territorio colombiano en lo concerniente a denunciar cualquier actividad de la que se tuviese conocimiento en la cual se divulgara o promocionara contenido pornográfico con menores de edad.

[12] El medio electrónico es un mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones, incluyendo cualesquiera redes de comunicación abiertas o restringidas como internet, telefonía fija y móvil u otras. (Real Academia Española, S.F.).

De manera que el Gobierno Nacional creó una línea de atención vía telefónica y electrónica la cual serviría para denunciar el uso de redes globales que se utilizarían para la comisión de delitos con menores de edad y con lo cual estas denuncias serian de carácter penal, además, a raíz de estas denuncias como lo establece el artículo 8 de la Ley 679 del 2001, no solo se sancionaría los proveedores o servidores administrativos, sino que también todo usuario que sea responsable de denunciar dichas acciones y no lo hagan o difundan material con contenido pornográfico.

Es por ello, que, para lograr una mayor protección en el intercambio de datos y pornografía infantil, el 21 de julio de 2009, se sancionó la Ley 1336, "por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual, con niños, niñas y adolescentes".

Adicionalmente, el Congreso de la República de Colombia, el 05 de enero de 2009 promulgó la Ley 1273, se hace una modificación al Código Penal colombiano, que crea un nuevo bien jurídico tutelado, denominado "de la protección de la información y de los datos". Ley que fue promulgada bajo antecedentes internacionales como el convenio de Budapest y la decisión Marco 222 que suscribió el Consejo de Europa en el año 2005.

Dada la gravedad de los delitos informáticos, en el año 2001 la comunidad internacional decidió firmar el Convenio de Budapest, sobre la ciberdelincuencia o cibercriminalidad, este convenio entró en vigencia en el año 2004. Siendo el primer instrumento internacional de este tipo.

Por consiguiente, el 23 de febrero del año 2005 el Consejo de Europa suscribió la decisión Marco 222 sobre los ataques al sistema de información, como lo establece el artículo 2 de dicha decisión:

> Acceso ilegal a los sistemas de información 1. Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad. 2. Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad. (Consejo de la Unión Europea, 2005, p.3).

De igual forma, en su artículo 4, desarrolla la Intromisión Ilegal en los datos: Los Estados que conforman el consejo de la Unión Europea deben adoptar las medidas correspondientes para que las personas con la intención de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sean sancionadas penalmente.

Se prevé el aumento de las amenazas que traen las redes del ciberespacio y su incorrecta utilización por las cuales se generan diversos riesgos que directamente afectan la seguridad de los sistemas informáticos. Es menester del Estado, desarrollar políticas públicas que garanticen la protección de la sociedad, estas se deben salvaguardar por medio del ámbito procesal penal.

> Por su parte, el 11 de septiembre de 2013, Colombia fue invitada por el Consejo de Europa a adherirse al Convenio de Budapest, gracias a las gestiones del Gobierno nacional encaminadas a contar con instrumentos jurídicos y de cooperación internacional para enfrentar de forma efectiva el delito cibernético. El término establecido para formalizar la adhesión es de 5 años por lo que solo hasta el año 2018 Colombia tiene la posibilidad de aceptar dicha invitación. (Gaceta del Congreso de Colombia, 2017).

Con la promulgación que realiza el Congreso de la República de Colombia de la Ley 1273 del 2009, se logran incorporar los lineamientos del Convenio de Budapest celebrado en el año 2001. Con el aumento de las amenazas que traen las redes del ciberespacio, surge la necesidad de promulgar e incorporar leyes internas que sean concordantes con dicho convenio, debido a su importancia y estándares adoptados por diferentes ordenamientos jurídicos a nivel internacional.

Con la incorporación de la Ley 1273 del 2009, se crearon nuevos bienes jurídicos tutelados basados en lineamientos internacionales:

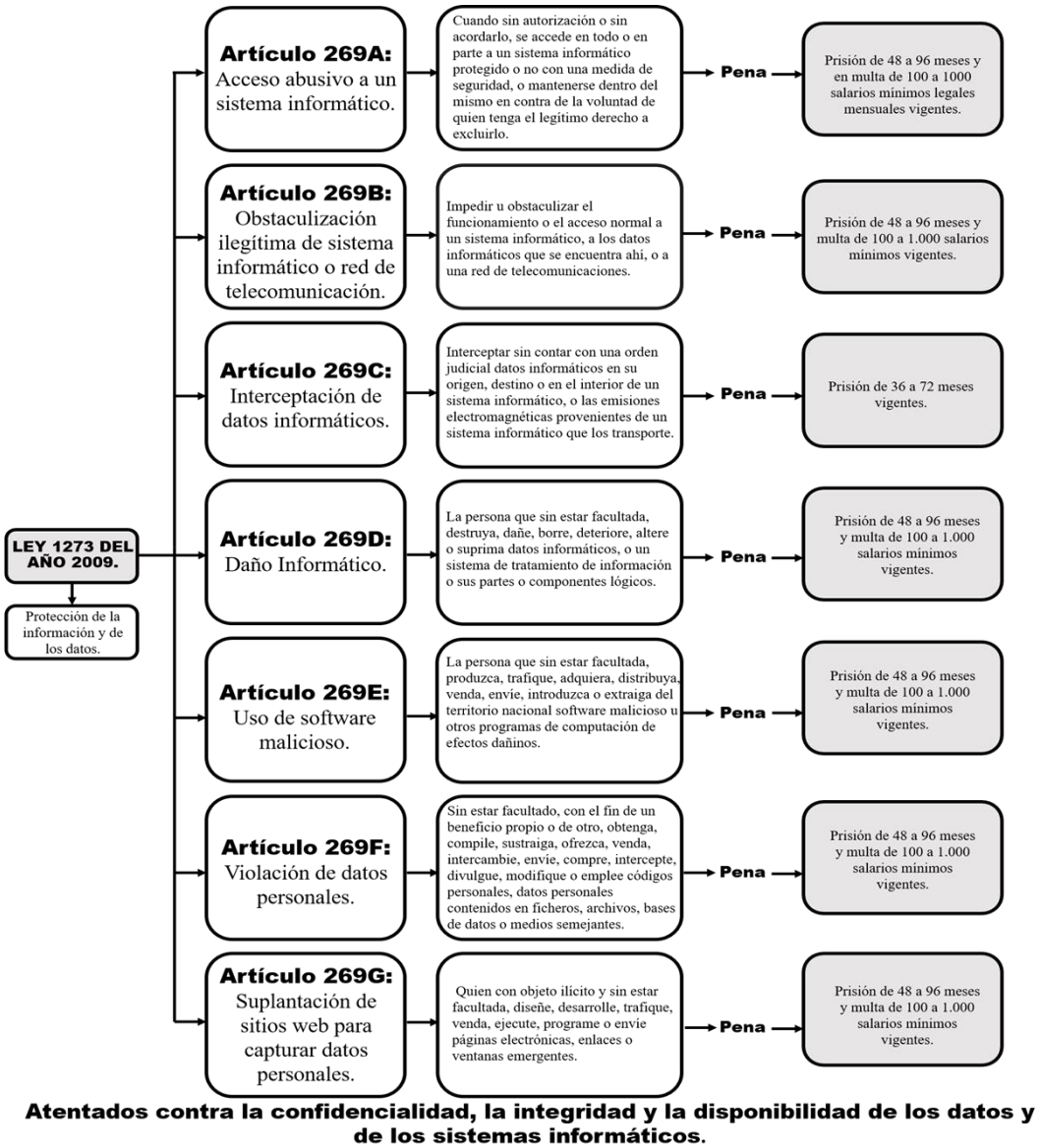

Figura 1. Legislación penal colombiana en cuanto a los delitos informáticos (Capítulo I de la Ley 1273 de 2009). Fuente: Construcción propia, con base en la Ley 1273 de 2009. Congreso de la República (2009).

La segunda gráfica da a conocer las “Circunstancias de agravación punitiva”, o aquellas conductas o situaciones que tiendan a agravar y aumentar la pena del delito (Artículo 269H Ley 1273 de 2009).

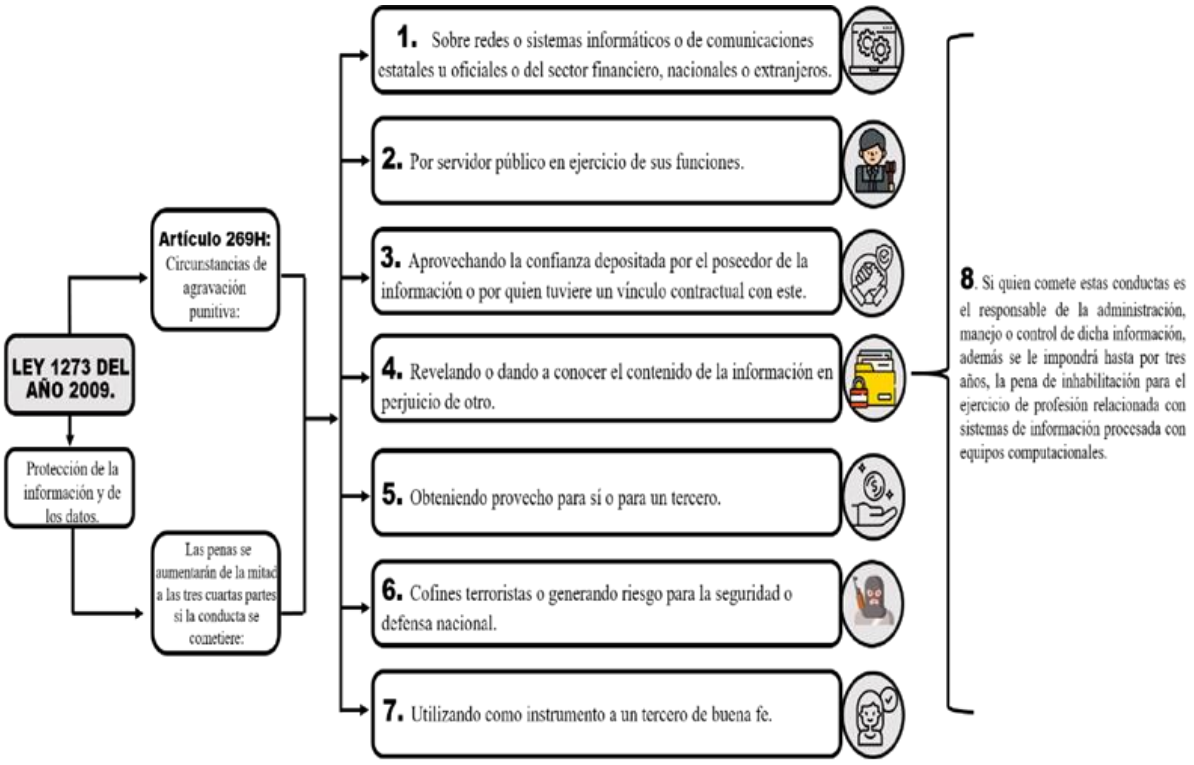

Figura 2. Legislación penal colombiana en cuanto a los delitos informáticos (Capítulo I de la Ley 1273 de 2009). Fuente: Construcción propia, con base en la Ley 1273 de 2009. Congreso de la República (2009).

La figura número tres expone “Los atentados informáticos y otras infracciones”; busca sancionar a las personas que pretendan poner en riesgo la preservación integralmente de los sistemas que utilicen las tecnologías de la información y las comunicaciones, en las disposiciones referidas en los artículos 269I “Hurto por medios informáticos y semejantes” y 269J “Transferencia no consentida de activos”, en donde es necesario para la ejecución del acto criminal el uso de recursos tecnológicos, por tal razón se encuentran contemplados en el segundo capítulo de la Ley 1273 de 2009.

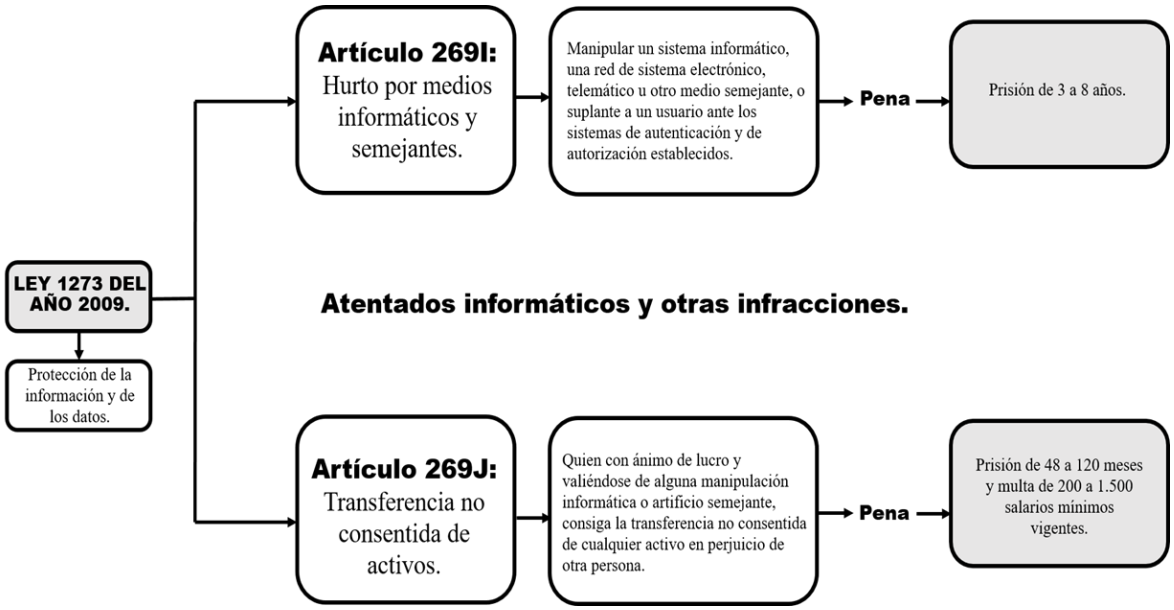

Figura 3. Legislación penal colombiana en cuanto a los delitos informáticos (Capítulo II de la Ley 1273 de 2009). Fuente: Construcción propia, con base en la Ley 1273 de 2009. Congreso de la República (2009).

Posteriormente, atendiendo la solicitud, la INTERPOL aceptó a Colombia como miembro de la Organización Mundial de la Policía, a través de la Ley 1670 del año 2013, el Congreso de la República aprueba el "Estatuto y Reglamento General de la Organización Internacional de Policía Criminal (INTERPOL)". De forma consiguiente, el Ministerio de Relaciones Exteriores en el año 2014 promulga el decreto 1066, por medio del cual se promulga el "Acuerdo de Cooperación Operativa y Estratégica entre la República de Colombia y la Oficina Europea de Policía (EUROPOL)".

Se debe hacer la claridad, que, desde el 28 de octubre de 1954, mediante comunicado emitido por la entonces Jefatura de Servicio de Inteligencia Colombiano (Departamento Administrativo adscrito a la Presidencia de la República), se solicita la adhesión de Colombia a la INTERPOL.

> Atendiendo la solicitud, Interpol aceptó a Colombia como miembro de la Organización, decisión que fue comunicada a los Países Miembros durante la Asamblea General de ese mismo año. Esta aceptación fue comunicada de manera oficial a Colombia mediante escrito del 5 de noviembre de 1954.
>
> El 11 de marzo de 1958, mediante Comunicación número 00521, la Jefatura del Servicio de Inteligencia Colombiano retiro la afiliación de Colombia a la entonces Comisión, en razón a

> que se desconocía cuál sería la organización que el nuevo Gobierno de ese entonces daría al Servicio de Inteligencia Colombiano. (Gaceta del Congreso, 2013. Pg. 10).

Es por ello, que se considera que Colombia ha formado parte de manera ininterrumpida en varias ocasiones de la Organización Internacional de Policía Criminal.

Al reconocer los tratados internacionales con la INTERPOL y EUROPOL, y con la promulgación realizada por el Congreso de la República de Ley Estatutaria 1581 de 2012, la cual establece como objeto en su artículo 1:

> La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (Ley 1581, 2012, art. 1).

También, en el año 2014 se crea el proyecto de Ley Estatutaria 1712, por medio de la cual se crea la Ley de transparencia y del derecho de acceso a la información pública nacional, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

> De conformidad con lo dispuesto en la Ley de Transparencia y del Derecho de Acceso a la Información Pública, cualquier persona podría acceder a la información pública de dos formas, la primera, acudiendo a la página web de los sujetos obligados quienes por disposición de los artículos 4° y 9° de la Ley 1712 de 2014 deben publicar proactivamente una información mínima obligatoria en los sistemas de información del Estado o en otras herramientas que lo sustituyan.
>
> La otra forma de acceder a la información pública es ejerciendo el derecho fundamental de acceso a la citada información mediante una solicitud dirigida al sujeto obligado, la cual deberá ser respondida de manera veraz y oportuna. Así las cosas, el sujeto obligado tiene el deber de publicar proactivamente la información pública en su condición de tal y, si la información que requiere la persona no se encuentra disponible por ejemplo en la página web del sujeto obligado, la persona podrá ejercer su derecho fundamental de acceso a la información pública mediante una solicitud o una petición de información pública. (Procuraduría General de la Nación, 2014. Pg. 1).

La cual fue revisada de forma integral mediante la Sentencia C-274 del año 2013, donde se evidencia que también configura los mecanismos de control ciudadano de la actividad estatal, con la finalidad de garantizar derechos constitucionales como el derecho al acceso y publicidad de la información pública:

> El proyecto de Ley Estatutaria “Por medio del cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional.”, fue revisado mediante la sentencia C-

> 274 de 2013, de acuerdo con lo establecido en los artículos 153 y 241-8 de la Constitución Política. (Corte Constitucional, 2013).

Estableciendo así, un marco básico para la protección de datos, su divulgación y denuncias por violaciones de seguridad. Dentro de estas leyes que son de índole ordinario, se detectan aquellas que regulan lo concerniente a la seguridad cibernética, explotación infantil a través de pornografía, comercio electrónico, bases de datos, incluyendo los referentes a los derechos de autor, etc.

GESTIÓN DE DELITOS INFÓRMATICOS EN EL PROCESO PENAL

En el derecho penal, como con las demás conductas punibles tipificadas, la comisión de estas supone la existencia de los dos sujetos principales, un sujeto activo y uno pasivo, sin distinción de personalidad natural. El titular del bien jurídico al cual se le ha ocasionado el daño antijurídico se conocerá como sujeto pasivo, por otro lado, el causante del daño o vulneración de derechos será conocido como sujeto activo.

En lo concerniente a delitos informáticos, el sujeto activo cuenta con habilidades de manejo, específicamente de sistemas informáticos.

Por la naturaleza de los delitos informáticos, el sujeto pasivo es quien resulta lesionado, puesto en peligro, con una vulneración de un derecho o bien jurídico tutelado. Al tratarse de delitos informáticos, en la posición de sujeto pasivo se puede encontrar personas tanto naturales o jurídicas, un grupo poblacional en específico, la sociedad en general, incluso, el Estado o la comunidad internacional.

En el caso colombiano, con respecto a los delitos informáticos, la reacción fue lenta y tardía, se evidencia en el balance realizado el 06 de febrero del año 2019, por parte de Comparitech, una plataforma especializada en el análisis de servicios tecnológicos. El estudio fue realizado entre 60 países, el primer puesto fue ocupado por Argelia, que es quien posee los peores índices de ciberseguridad, por el lado contrario, se encuentra Japón quien ocupó el último puesto, significando que posee los mejores sistemas y estándares para contrarrestar el cibercrimen; Colombia, ocupó el puesto número 39, lo cual lo posiciona en un rango medio en dicho estudio.

En Colombia por medio de los lineamientos de políticas para ciberseguridad y ciberdefensa CONPES 3701, se expuso cuáles son los organismos encargados de la seguridad digital del país. Entre estos se encuentran el Grupo de Respuesta a Emergencias Cibernéticas de Colombia –COLCERT-, el Centro Cibernético Policial –CCP- y el Comando Conjunto Cibernético CCOC.

La entidad COLCERT les presta apoyo a las demás entidades, asimismo su función está dirigida a ser: "Un coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa y tiene como misión la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional". (COLCERT, S.f.).

Mientras que el Comando Conjunto Cibernético: "Coordina, integra y conduce operaciones militares en el ciberespacio para la defensa de los intereses nacionales y de la infraestructura crítica cibernética nacional a fin de contribuir en el cumplimiento de la misión del Comando General de las Fuerzas Militares." (CCOC, 2017).

Y por último el Centro Cibernético Policial, es el encargado de: "Proteger, responder y divulgar a la ciudadanía todo lo relacionado con amenazas y delitos cibernéticos, orientado a resguardar la disponibilidad, integridad y confidencialidad de la información, que estará en cabeza de la Policía Nacional." (Guerrero, R, S.f.).

El Estado colombiano ha implementado diferentes estrategias para que los ciudadanos puedan acudir a la justicia con la finalidad de denunciar un delito informático, por tal razón, para realizar la respectiva denuncia en este tipo de casos, se puede acudir ante las autoridades competentes que son directamente la Fiscalía General de la Nación y la Policía Nacional de Colombia.

Las personas que hayan sido afectadas por alguna de estas conductas pueden ejecutar la correspondiente denuncia presencial en cualquier unidad de la fiscalía general de la Nación o a través del sistema de denuncia virtual *ADenunciar***,** que se encuentra habilitado las 24 horas del día, incluso, está establecida la línea 122 para comunicarse con el Centro de Contacto de la Fiscalía si se requiere.

"El 45% del total de denuncias por ciberdelitos en el país se hace a través de la aplicación *Adenunciar*. Desde julio de 2017 se han recibido un total 24.711 por ciberdelitos en esta plataforma virtual." (Centro Cibernético Policial, 2019-2020).

De forma articulada, desde el 30 de abril del año 2007, se crea el laboratorio de informática forense. Inicialmente empezó a funcionar en las instalaciones de la Seccional de investigación Judicial SIJIN-MEVAL en Medellín, Antioquia. Posteriormente en el año 2013, paso a ser parte de la oficina Regional de Investigación Criminal, ayudando a desarticular bandas delincuenciales y a la recuperación de información de los medios de almacenamiento digital y equipos electrónicos como terminales móviles.

> Desde su creación han sido realizados un total de 2.427 informes de laboratorio para las autoridades judiciales de la región por diferentes delitos, y un total de 241.838 gigabytes analizados.
>
> El laboratorio de informática forense participó en las investigaciones en casos de relevancia como la desarticulación de las pirámides DMG-DRFE, captadoras ilegales de dinero, los falsos recobros del Fosyga, el desfalco de la DIAN a través de empresas fachada para el recobro del IVA, la captura del cineasta español de películas pornográficas con menores de edad.

También, se instituyo el Centro Cibernético Policial –CCP- de la Policía Nacional, encargado de brindar apoyo, protección e información sobre los delitos cibernéticos.

> Todo lo que tenga que ver con el ambiente cibernético lo podemos manejar a través del CAI virtual, y allí se brinda la asesoría. Si es un tema que se debe escalar a la Fiscalía se orienta a la persona para que ponga la denuncia de manera adecuada. Algunas denuncias escalan a la Fiscalía mientras que los incidentes se solucionan en la misma atención que se realiza en el CAI virtual con una solución casi que de inmediato, explicó Rodrigo Acevedo, oficial del Centro Cibernético Policial. (Conexión Capital, 2020).

Esta entidad despliega actividades de prevención, investigación y judicialización de la cibercriminalidad en el país. Asimismo, la denuncia se puede presentar o formalizar a través de la página web www.ccp.gov.co del CAI Virtual por medio de un chat que se dispone para ello. Según el balance de cibercrimen realizado por el Centro Cibernético Policial en el año 2020: "Este centro ha atendido 11.950 incidentes y 7.862 correos gestionados durante el presente año".

De igual forma se estructura el balance sobre el desarrollo de las diligencias que realiza esta autoridad, así como la cantidad de delitos como hackeos de cuentas y de redes sociales,

accesos a sistemas informáticos, links que redireccionan a páginas fraudulentas, páginas que tengan características que puedan generar riesgos para los ciudadanos o especialmente para los niños, niñas y adolescentes, con base en la comisión de dichas conductas.

En las gráficas cuatro y cinco se muestra detalladamente un balance de cibercriminalidad realizado por el Centro Cibernético Policial en el año 2020, con el entendido de que el incremento en el uso del internet y las tecnologías de la información y las comunicaciones en la actualidad abren la puerta para que individuos con intereses maliciosos ataquen y violen la seguridad de los datos y de la información. Se expone en las gráficas los resultados de las operaciones que lleva a cabo el Centro Cibernético con la finalidad de contrarrestar la acción delictiva, así como la exhibición de las principales modalidades que se cometen a diario por estos medios.

Figura 4. Balance de Cibercrimen del año 2020. Fuente: Construcción propia, con base en el Balance de Cibercrimen del año 2020. Centro Cibernético Policial de la Policía Nacional (2020).

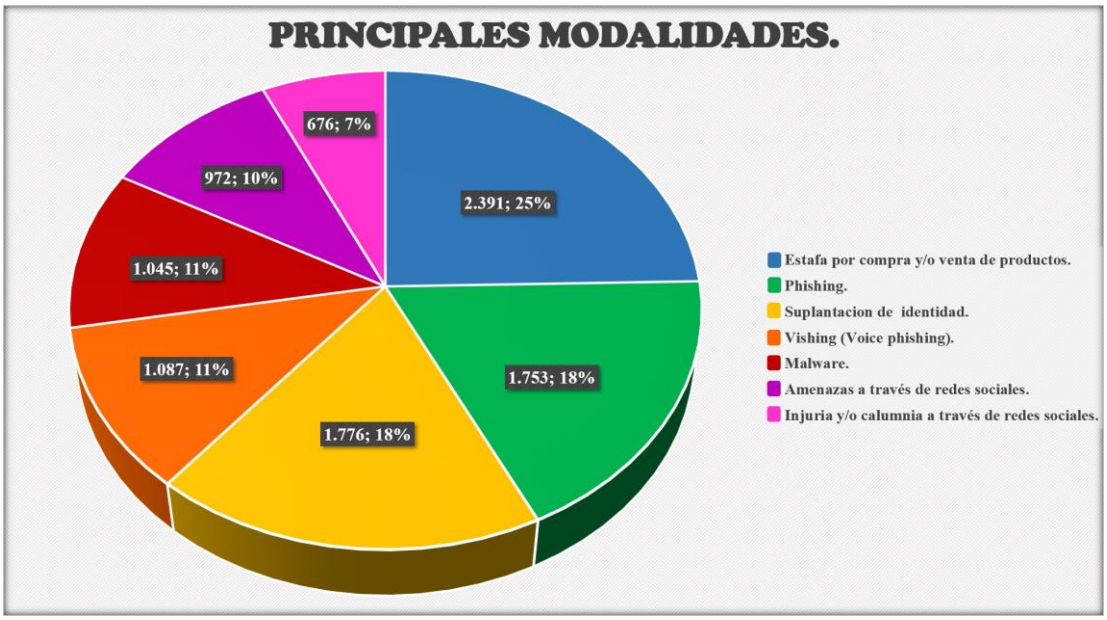

Figura 5. Balance de Cibercrimen del año 2020. Fuente: Creación propia, con base en el Balance de Cibercrimen del año 2020. Centro Cibernético Policial de la Policía Nacional (2020).

Según el centro cibernético de la policía nacional en el año 2019 se denunciaron 17.531 casos sobre delitos informáticos de estos 12.879 incidentes cibernéticos o sea el 43% de los casos puestos en conocimiento fueron gestionados sin que se estableciera una denuncia en la Fiscalía General de la Nación.

Otra herramienta fue proporcionada por MinTic que dispuso una nueva plataforma por la que ha dado la facilidad a las personas de denunciar delitos contra los menores de edad por internet, buscando prevenir este tipo de ataques, se crearon ‘En TIC Confío' y Te Protejo.

Hoy en día es cada vez más frecuente que los criminales utilicen los medios digitales para cometer conductas delictivas, por tal razón las autoridades han tipificado delitos como el ciberacoso, sexting, pornografía infantil y acceso carnal abusivo que pueden ser cometidos por ciberdelincuentes.

Por medio de este canal se informan los riesgos en los que pueden estar inmersos los niños, niñas y adolescentes del país, las denuncias presentadas son atendidas por la policía nacional de Colombia quienes harán la intervención pertinente.

Atreves de la página www.teprotejo.org, se llena el formulario y se identifica el delito.

La segunda estrategia 'En TIC Confío' presupone el uso responsable y seguro del Internet y otras herramientas digitales, con la ayuda de charlas-taller en las que se darán tips y recomendaciones para no caer en los delitos cibernéticos. Se debe ingresar a www.enticconfio.gov.co para diligenciar el formulario de contacto, en el enlace 'Solicitud de conferencias".

Por otra parte, con la Resolución 249 de febrero 19 de 2015, expedida por la Fiscalía General de la Nación, se busca que los Directores de Cuerpo Técnico de Investigación, CTI, y de la Dirección de Investigación Criminal, DIJÍN, de la Policía Nacional, trabajen de forma mancomunada por grupos de trabajo exclusivos para el desarrollo metodológico de las investigaciones a personas o grupos delincuenciales que estén cometiendo conductas punibles tipificadas como delitos informáticos o cibercrimen a través de medios informáticos como se estipula en su artículo 2:

> Integración del grupo de trabajo. El grupo de trabajo estará integrado por los siguientes servidores:
>
> • Un (1) Fiscal delegado ante jueces penales de circuito.
>
> • Un (1) Fiscal delegado ante los jueces penales del circuito especializado.
>
> • Un (1) Fiscal delegado ante los jueces penales del circuito especializado.
>
> • Un (1) Asistente de Fiscal I.
>
> • Un (1) Asistente de Fiscal II.
>
> • Un (1) secretario I.
>
> • Seis (6) investigadores de la Dirección Nacional del Cuerpo Técnico de Investigación adscritos a los siguientes grupos: tres (3) investigadores del grupo de delitos informáticos y dos (2) investigadores de la sección de análisis criminal.
>
> • Cinco (5) investigadores de la Dirección de investigación criminal e Interpol de la Policía Nacional adscritos al Centro cibernético policial. (Fiscalía General de la Nación, 2015).

Con la implementación de la Ley 1273 del 2009, surge una adaptación en el sistema judicial colombiano conteniendo los elementos de configuración de los delitos informáticos. Por consiguiente, se puede evidenciar a través de la Corte Suprema de Justicia la implementación de la Ley 1273 del 2009, donde se han proferido sentencias que versan sobre delitos informáticos y cibercrimen.

En el caso siguiente, se indica la sentencia de la sala de casación penal por un hurto realizado por medios informáticos y semejantes, donde el medio probatorio, se define como un bien material del delito, pues se considera que los datos e información manipulados con fines delictivos en el caso en cuestión, versa sobre un fin material, el cual es la obtención de dinero de forma ilícita por medios informáticos:

> En cuanto al objeto, la distinción doctrinal entre objeto jurídico y/o material de protección, obliga a determinar, en el caso concreto, que, si bien el delito se ubica dentro del título que protege la información y los datos, el bien material del delito no puede ser otro que la cosa mueble ajena que sufre un apoderamiento por parte de un extraño. Los datos, la información y su contenido solo son manipulados con el fin de obtener un provecho 18 económico por medio de la sustracción irregular de la cosa mueble ajena que se condensa en el dinero. (Corte Suprema de Justicia, 2015).

Se entrevé una aproximación, pues pasa de ser un bien intangible, a un bien con referencia material, que, en el ámbito probatorio, permite ser protegido en el ámbito jurídico. Es menester agregar que la actividad probatoria, en los casos donde el bien material es hurtado con fines de manipulación a través de medios informáticos con la finalidad de obtener el aprovechamiento económico, y que en este caso el medio probatorio se lleva a cabo mediante software que permiten rastrear de manera digital.

En referencia a las pruebas idóneas para determinar un delito informático la Corte Constitucional ha hecho hincapié en la importancia de contar con peritos informáticos para que se resuelva de una forma eficaz el juicio, adicionalmente, es preciso realizar un control judicial que asegure la legalidad formal y sustancial de la actuación, así como dar cumplimiento al deber de proteger los derechos fundamentales de quienes se encuentren en el proceso y por último es menester que exista una conservación correcta de la prueba.

El artículo 14 de la Ley 906 de 2004 sitúa el principio de reserva judicial para los sucesos en los que se ponga en riesgo una garantía fundamental dentro del proceso penal. Consagra lo siguiente:

> No podrán hacerse registros, allanamientos ni incautaciones en domicilio, residencia, o lugar de trabajo, sino en virtud de orden escrita del Fiscal General de la Nación o su delegado, con arreglo de las formalidades y motivos previamente definidos en este Código. Se entienden excluidas las situaciones de flagrancia y demás contempladas por la ley. (Congreso de la República, 2004).

En conformidad con lo expuesto la Corte Constitucional en la sentencia C-336 de 2007, reiterada en la C-131 de 2009, destaca cuál debe ser la actuación de los jueces para que se acate el debido proceso:

> 5. De tales previsiones constitucionales se concluye que fue voluntad del Constituyente: (i) radicar en cabeza de los jueces de control de garantías la adopción de las medidas necesarias para asegurar la comparecencia de los imputados al proceso penal; sólo excepcionalmente y previa regulación legal que incluya los límite (sic) y eventos en que procede, la Fiscalía podrá efectuar capturas; (ii) facultar directamente a la Fiscalía para adelantar registros, allanamientos, incautaciones e interceptación de comunicaciones, sometidos al control posterior del Juez de Control de Garantías; (iii) disponer que en todos los demás eventos en que, para el aseguramiento de los elementos materiales probatorios, se requiera medidas adicionales que impliquen afectación de derechos fundamentales deberá mediar autorización (es decir, control previo) por parte del Juez de Control de Garantías. (Corte Constitucional, 2007).

La sentencia C-336 del año 2007, explica que, en cuanto a los registros, allanamientos, incautaciones e interceptaciones de comunicaciones, la Fiscalía General de la Nación seria quien está facultada para hacer directamente este tipo de actividades, sometiendo la orden y lo hallado a la cadena de custodia y a un control integral posterior, las actuaciones restantes que consigan afectar derechos fundamentales deben contar con la autorización previa del Juez.

También, es clara la corte al precisar en la sentencia C-334 del 2010, la importancia de la protección a los datos que es fundamental para que no se viole el derecho a la intimidad de las personas: “La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley”. (Corte Constitucional, 2010).

Análogamente la sentencia dispone que estos allanamientos, registros, incautaciones e interceptación de comunicaciones, pueden violar o poner en peligro los derechos a la intimidad personal y familiar, afectar la honra y el buen nombre, así como los derechos reales y de propiedad con los que cuente el sujeto investigado de los bienes que posea.

Gracias a esta intromisión, si la Fiscalía y la Policía Judicial van a desarrollar alguna de estas actividades deben tener presente que solo pueden ejecutarlas si están relacionadas

directamente con bienes de los que es propietario o tenedor el indiciado o inculpado. Salvo los casos de flagrancia propuestos por el legislador.

Por último, la sentencia C-1092 de 2003, dicta las consecuencias de no cumplir con las medidas necesarias para la obtención de la prueba:

> Si encuentra que la Fiscalía ha vulnerado los derechos fundamentales y las garantías constitucionales, el juez a cargo del control no legitima la actuación de aquella y, lo que es más importante, los elementos de prueba recaudados se reputan inexistentes y no podrán ser luego admitidos como prueba, ni mucho menos valorados como tal. En consecuencia, no se podrá, a partir de esa actuación, llevar a cabo la promoción de una investigación penal, como tampoco podrá ser llevada ante el juez de conocimiento para efectos de la promoción de un juzgamiento; efectos estos armónicos con la previsión del artículo 29 superior, conforme al cual es nula de pleno derecho toda prueba obtenida con violación del debido proceso. (Corte Constitucional, 2003).

Resulta relevante el análisis de las sentencias anteriores para entender la implementación de los delitos informáticos en el sistema penal colombiano, pues más allá de la normatividad en la práctica, los delitos informáticos en el debido proceso en lo concerniente a pruebas, puede llegar a ser un reto para alcanzar el estatus de medio probatorio, y posteriormente la ejecución en el proceso judicial.

CONCLUSIONES

El desarrollo de la globalización y los alcances tecnológicos que existen en la actualidad han ocasionado una innumerable cantidad de ventajas que rodean la cotidianidad de toda la sociedad, al mismo tiempo, el tener acceso a tan vasta información almacenada ha generado cambios en los conductas colectivas, económicas y éticas de las personas lo que ha conllevado a la constitución de nuevos actos delictivos que ponen en peligro la seguridad de los datos y la información, así como también pueden vulnerar de diferentes formas, la vida y la integridad de la población.

Se encuentra evidenciado que históricamente en Colombia ha habido un desarrollo normativo por el cual el país se ha ido adaptando poco a poco a los cambios tecnológicos, esto de la mano de convenciones o antecedentes internacionales que han dado los primeros pasos para la judicialización y protección de delitos informáticos. En el Estado colombiano, desde la

promulgación de la Ley 1273 de 2009 y las adiciones realizadas en al Código Penal colombiano, donde se incorporaron nuevos tipos penales y la creación de ese nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-, norma que contribuyó a la creación de políticas y procedimientos de seguridad informática, así como las acciones penales en contra de quienes incurran en ciberdelitos.

Se han realizado diferentes esfuerzos, desde la implementación de la normatividad y diferentes canales o procedimientos para la persecución de los delitos informáticos, pero algunas de estas iniciativas siguen siendo abstractas para conseguir la judicialización de las personas u organizaciones delincuenciales que cometen este tipo ilícitos a partir del uso de dispositivos electrónicos y tecnológicos.

Es indispensable dejar claro que la corte hace mención a que es fundamental, la importancia sobre la protección a los datos y a la recopilación de los mismos, lo cual siempre se deberá hacer bajo lo reglamentado por la ley, sin importar qué dicha información sea recolectada por un ente público o privado, siempre se será primordial la protección de los derechos y la intimidad personal y familiar del sujeto investigado.

En Colombia, las cifras de las tendencias cibernéticas señalan que a través de los canales de atención establecidos por la Policía Nacional se registraron en el año 2019 un número total de casos de 28.827 y solo 57% fueron registrados como infracciones a la Ley 1273 del año 2009, además el 43% de los casos fueron gestionados sin que se instalara una denuncia ante la Fiscalía General de la Nacional.

Por consiguiente, es claro que casi aproximadamente la mitad de los casos presentados son descartados por no ser una infracción a la Ley 1273 del 2009, así como el 43% son gestionados sin la necesidad de desgastar el aparato judicial acudiente al principio de economía procesal, adicionalmente las personas acuden de forma proporcional a la denuncia física que cuenta con un 54,5% así como a las denuncias por medios virtuales con un porcentaje del 45.5%.

Aunque la adaptación para el desarrollo de estos procesos en línea, han sido lentos y aún la denuncia física cuenta con un porcentaje mayor de aceptación, se ha dado un gran avance en

la utilización de las herramientas tecnológicas, encima estos recursos brindan más comodidad y agilidad en la instauración de la denuncia.

Los resultados obtenidos de este trabajo de investigación establecieron la recurrencia de diferentes delitos cibernéticos en los cuales se evidencia que la normatividad colombiana, sí cuenta con mecanismos procesales para que los ciudadanos puedan acudir a denunciar ante las autoridades competentes. No cabe duda, que aún así, se debe seguir fortaleciendo estos instrumentos para alcanzar una mayor efectividad de la judicialización de estos delitos.

Además, desde el punto probatorio, la Corte Constitucional ha hecho hincapié en la importancia de contar con peritos especializados en delitos informáticos con el fin de asegurar la legalidad formal y sustancial para lograr dar cumplimiento al deber de proteger los derechos fundamentales de quienes en los procesos judiciales que versen sobre delitos informáticos para que se resuelva de forma eficaz el juicio para la conservación de la prueba electrónica. De esta necesidad, la Fiscalía General de la Nación, mediante la Resolución 249 de febrero 19 del 2015 buscó que los Directores de Cuerpo Técnico de Investigación, CTI, y de la Dirección de Investigación Criminal, DIJÍN, de la Policía Nacional, trabajen de forma mancomunada por grupos de trabajo exclusivos a la investigación de las conductas punibles tipificadas como delitos informáticos o cibercrimen a través de medios informáticos.

Por consiguiente, en lo concerniente a delitos informáticos, están justificados constitucionalmente por la necesidad de “garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución” para dar cumplimiento con la validez a un orden justo. A través de ello, el Estado deberá brindar una protección subsidiaria frente a ese bien jurídico tutelado -denominado "de la protección de la información y de los datos"- mediante la imposición de penas, cuando estima que es necesario acudir a este mecanismo para brindarles una protección eficaz. Sin embargo, este último instrumento debería ser útil y cumplir con dicha protección, pero por la reacción tardía y por los pocos procesos que terminan judicializados, no se logra cumplir con los instrumentos jurídicos y sanciones para dichas conductas delictivas.

Referencias

Asamblea Nacional Constituyente, Constitución Política de Colombia de 1991. Artículo 15. Bogotá: Presidencia de la República.

Barñol, M, (2014). Reconocimiento de las principales audiencias preliminares en el marco de la ley 906 de 2004. Tesis de grado. Universidad Católica de Colombia. https://repository.ucatolica.edu.co/bitstream/10983/1627/1/RECONOCIMIENTO%20DE%20LAS%20PRINCIPALES%20AUDIENCIAS%20PRELIMINARES%20EN%20EL%20MARCO%20DE%20LA%20LEY%20906%20DE%202004.pdf

CCOC, (2017). "Comando Conjunto Cibernético, Misión y Responsabilidad". https://www.ccoc.mil.co/quienes_somos_mision_responsabilidad

Centro Cibernético Policial, (2019-2020). Tendencias Cibercrimen Colombia 2019 - 2020. https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

COLCERT, (S.f.). "Grupo de respuesta de emergencias cibernéticas de Colombia". http://www.colcert.gov.co/

Colombia, Congreso de la República (2009). Ley 1336 de 2009, por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Diario Oficial No. 47.417, 21 de julio de 2009. http://www.ley/2009/ley_1336_2009.html.

Conceptos jurídicos, (S.F.). "Bien jurídico, derecho penal". https://www.conceptosjuridicos.com/bien-juridico/

Conexión Capital, (2020). "Así funciona el CAI virtual del Centro Cibernético Policial". Bogotá, Colombia. https://conexioncapital.co/asi-funciona-el-cai-virtual-de-la-policia/

Congreso de Colombia, (2012) Por la cual se dictan disposiciones generales para la protección de datos personales. [Ley Estatutaria 1581 de 2012].

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981#:~:text=La%20presente%20ley%20tiene%20por,el%20art%C3%ADculo%2015%20de%20la

Congreso de Colombia, (24 de julio del 2000) Código penal colombiano. [Ley 599 del 2000]. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Congreso de la República de Colombia, (24 de julio 2000). Código de procedimiento penal. [Ley 600 de 2000]. http://www.secretariasenado.gov.co/senado/basedoc/ley_0600_2000.html

Congreso de la República (2001). Ley 679 de 2001, por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Diario Oficial No. 44.509, 4 de agosto de 2001. http://www.cntv.org.co/cntv_bop/basedoc/ley/2001/ley_0679_2001.html.

Congreso de la República, (05 de enero del 2009) "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"**.** [Ley 1273 del 2009]. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República, (05 de febrero de 1993). "por medio de la cual se modifica y se adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944". [Ley 44 de 1993].

Congreso de la República, (2009). "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones." [Ley 1341 del 2009]. http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

Congreso de la República, (2013). Por medio de la cual se aprueba el "Estatuto y Reglamento General de la Organización Internacional de Policía Criminal (Interpol)" [Ley 1670 del año 2013]. https://www.cancilleria.gov.co/sites/default/files/Normograma/docs/ley_1670_2013.htm

Congreso de la República, (2014). “Por medio de la cual se crea la Ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones”. http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201712%20DEL%2006%20DE%20MARZO%20DE%202014.pdf

Congreso de la Republica, (31 de agosto del 2004) “Por la cual se expide el Código de Procedimiento Penal.”. [Ley 906 De 2004]. http://www.secretariasenado.gov.co/senado/basedoc/ley_09060_204a.html

Consejo de la Unión Europea, (2001). Serie de tratados europeos. Convenio sobre la Ciberdelincuencia, Budapest: 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

Consejo de la Unión Europea, (2005). Decisión Marco 222. https://www.boe.es/doue/2005/069/L00067-00071.pdf

Cornell Law School, (S.F.). “Fraude Cibernético e Informático”. Wex Legal Dictionary. https://www.law.cornell.edu/wex/es/fraude_cibern%C3%A9tico_e_inform%C3%A1tico

Corte Constitucional, (2013). Sentencia C-274. [M.P. María Victoria Calle Correa]. https://www.corteconstitucional.gov.co/relatoria/2013/c-274-13.htm

Corte Constitucional, (2018). Sentencia C-014 del 2018. [M.P. Alberto Rojas Ríos]. https://www.corteconstitucional.gov.co/relatoria/2018/C-014-18.htm

Corte Constitucional, Sala Plena. (2003) Sentencia C-1092, 2003. [M.P. Álvaro Tafur Galvis]. https://www.corteconstitucional.gov.co/relatoria/2003/C-1092-03.htm

Corte Constitucional, Sala Plena. (2007) Sentencia C-336, 2007. [M.P. Jaime Córdoba Triviño]. https://www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm

Corte Constitucional, Sala Plena. (2009) Sentencia C-131, 2009. [M.P. Nilson Pinilla Pinilla]. https://www.corteconstitucional.gov.co/relatoria/2009/C-131-09.htm

Corte Constitucional, Sala Plena. (2010) Sentencia C-334, 2010. [M.P. Juan Carlos Henao Pérez]. https://www.corteconstitucional.gov.co/relatoria/2010/C-334-10.htm

Corte Constitucional. (21 de noviembre de 1996). Sentencia C-626. [M.P. José Gregorio Hernández Galindo]. https://www.corteconstitucional.gov.co/relatoria/1996/C-626-96.htm

Corte Suprema de Justicia, Sala de Casación Penal, (2015) Sentencia SP1245- 2015. [M.P. Eyder Patiño Cabrera] https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015.pdf

DANE, (2018). Boletín técnico, indicadores básicos de tenencia y uso de tecnologías de la información y comunicación – tic en hogares y personas de 5 y más años 2018. https://www.dane.gov.co/files/investigaciones/boletines/tic/bol_tic_hogares_2018.pdf

Fiscalía General de la Nación, (2015). Resolución 249 de 19 de febrero de 2015. Diario Oficial N°:49442 de marzo 3 De 2015.

Flores Salgado, L. (2015). Derecho informático. Grupo Editorial Patria. https://elibro.net/es/ereader/funlam/39404?page=149

Gaceta del Congreso de Colombia, (2013). Informe de ponencia para primer debate al proyecto de Ley número 42 de 2012 Senado. Imprenta Nacional. ISSN 0123 – 9066. http://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/Ponencias/2013/gaceta_186.pdf

Gaceta del Congreso de Colombia, (2017). Proyecto de Ley 58 de 2017 Senado. Imprenta Nacional. ISSN 0123 – 9066. https://www.camara.gov.co/sites/default/files/2018-06/gaceta%20403%20de%202018.pdf

Gómez Agudelo, (2020). Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano. Revista Ratio Juris, Vol. 15 N°30. UNAULA. ISSN 1794 – 6638. https://publicaciones.unaula.edu.co/index.php/ratiojuris/article/view/469/1046

González-Monguí, P. E. (2017). Delitos contra la libertad individual y otras garantías. Bogotá: Editorial Universidad Católica de Colombia.

Guerrero, R, (S.f.). "Documento CONPES3701 lineamientos de políticas para ciberseguridad y ciberdefensa". Seminario de investigación aplicada, Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00002648.pdf

Ministerio de Relaciones Exteriores de Colombia, (2014). Por medio del cual se promulga el "Acuerdo de Cooperación Operativa y Estratégica entre la República de Colombia y la Oficina Europea de Policía". [Decreto 1066 del 2014]. https://www.leyex.info/documents/leyes/Decreto1066de2014.pdf

MINTIC, (2016). "MinTic invita a denunciar el abuso a menores de edad en internet". https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/15041:MinTIC-invita-a-denunciar-los-abusos-contra-menores-de-edad-en-Internet

OEA, 2020. Ciberseguridad riesgos, avances y el camino a seguir en américa latina y el caribe. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Ojeda, Rincón, Arias, & Daza, (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Ed. Copyright Universidad Pontificia Javeriana.

Policía Nacional de Colombia, (2017). "10 años laboratorio de informática forense al servicio de la investigación". https://www.policia.gov.co/noticia/10-anos-laboratorio-informatica-forense-al-servicio-investigacion

Policía Nacional de Colombia, (2020). "Balance de cibercriminalidad Centro Cibernético Policial". https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

Presidente de la República, (23 de junio de 1989). "decreto único reglamentario". [Decreto 1360 de 1989].

Procuraduría general de la Nación, (2014). “Preguntas frecuentes de la Ley de transparencia y derecho del acceso a la información 1712 del 2014”. https://www.procuraduria.gov.co/portal/media/file/PREGUNTAS.pdf

Real Academia Española, S.F. “Diccionario Panhispánico del español jurídico”. https://dpej.rae.es/lema/medio-electr%C3%B3nico#:~:text=Tel.,fija%20y%20m%C3%B3vil%20u%20otras.

Rebecca, M, (2019). Comparitech Límite. Obtenido de https://www.comparitech.com/blog/vpnprivacy/cybersecurity-by-country/

Téllez-Valdés, Julio (2003). Derecho informático. 3a ed. México: McGraw Hill. https://dialnet.unirioja.es/servlet/articulo?codigo=5214446

TicTac & CCIT, (2019). Tendencias del Cibercrimen en Colombia 2019 – 2020. https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Universidad Nacional de Colombia, (S.F.). “Propiedad intelectual y derechos de autor”. SIUN, Sistema de Investigación UN. https://propiedadintelectual.unal.edu.co/acerca-de-pi/derechos-de-autor/