# Ciberdelincuencia en Colombia, Retos y Desafíos Jurídicos en la Normatividad Colombiana[1]

**Mariana Bolívar Londoño**[2]

**Valeria Carvajal Ríos**[3]

**Resumen:** La ciberdelincuencia en Colombia se puede determinar por el desarrollo de diferentes delitos por medio de un sistema informático, trayendo consecuencias como la vulnerabilidad de la confidencialidad y la seguridad de la información, convirtiéndose en una actividad viable para los autores de este delito, gracias a que la evolución de la tecnología permite el anonimato, la ubicación remota y la obtención de grandes cantidades de dinero de forma sencilla. Se buscó entonces, evaluar cuales son las falencias y vacíos existentes en la normatividad colombiana que están abriendo espacio a la reincidencia y desarrollo de esta conducta delictual; se llevó a cabo un profundo análisis de las leyes y regulaciones sobré ciberdelincuencia, comparando así la normatividad colombiana con la normatividad internacional.

**Palabras clave:** ciberdelincuencia; sistema jurídico; seguridad; ciberdelitos.

**Abstract:** Cybercrime in Colombia can be determined by the development of different crimes through a computer system, bringing consequences such as the vulnerability of confidentiality and security of information, becoming a viable activity for the perpetrators of this crime, thanks to the fact that The evolution of technology allows anonymity, remote location and obtaining large amounts of money easily. It is sought, then, to evaluate what shortcomings and gaps exist in Colombian regulations that are opening space to the constant occurrence and

[1] Articulo para obtener el título de abogado. Asesora: Laura Victoria Cárdenas Rojas.

[2] Estudiante de Derecho de la Universidad Católica Luis Amigo, valeria.carvajalri@amigo.edu.co, 2024

[3] Estudiante de Derecho de la Universidad Católica Luis Amigo, mariana.bolivarlo@amigo.edu.co, 2024

development of this criminal behavior; An in-depth analysis of the laws and regulations on cybercrime was carried out, thus comparing Colombian regulations with international regulations.

**Keywords:** Cybercrime; legal system; security; cybercrime.

## Introducción

La ciberdelincuencia se puede entender como los delitos cometidos por medio de internet o plataformas digitales que vulneran la seguridad de empresas, usuarios e individuos de las diferentes aplicaciones, redes sociales o cargos laborales. Los delitos más comunes son el Hacking, phishing, el malware, el robo de identidad, entre otros tipos de ataques cibernéticos. Los delitos informáticos entonces cobran una mayor relevancia en nuestra actualidad y en nuestro país, por su alto incremento en los últimos años, lo que ha traído como consecuencia la afectación de individuos, empresas e instituciones. Los delincuentes, cada vez utilizan más variedad de estrategias para cometer crímenes mediante la web, entre estas técnicas, se destaca el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos.

Nuestro objetivo en esta investigación, se basa en determinar cuáles son los vacíos jurídicos de la ciberdelincuencia que son presentados en la normativa colombiana, con el fin de darle una respuesta de fondo a esta problemática que se desarrolla en Colombia; desarrollaremos entonces dos objetivos específicos los cuáles se definen en determinar las consecuencias jurídicas que se pueden generar a partir del vacío jurídico de la ciberdelincuencia y comparar la normativa internacional frente a las disposiciones que se tienen en materia de ciberdelincuencia.

Para nuestra investigación, elegimos la metodología cualitativa explicativa, gracias a que la ciberdelincuencia se conoce por su naturaleza confusa y en constante evolución como fenómeno digital. Al optar por un enfoque explicativo, buscamos ir más allá de la mera descripción de delitos cibernéticos, sino también explorar las complejas relaciones causales y factores subyacentes que contribuyen a la ciberdelincuencia. Esta metodología nos permite una inmersión profunda en evidenciar cual es la raíz de la comisión de estos delitos, la motivación y los comportamientos de los actores involucrados en la comisión del delito, así como la identificación de patrones. Se busca construir teorías explicativas sólidas, para ofrecer

perspectivas valiosas que no sólo describen, sino que también expliquen las dinámicas complejas del cibercrimen, informando así estrategias más efectivas de prevención y mitigación.

El problema jurídico de esta investigación radica en: ¿hallar cuales son los vacíos jurídicos de la ciberdelincuencia que se presentan en la normativa colombiana? Es de anotar que la rapidez con la que evolucionan las tácticas y técnicas de los ciberdelincuentes, conlleva a que se requiera una constante adaptación de la normatividad, para así lograr abordar las nuevas modalidades de consumación de delitos desarrollados por medio de la web. La ciberdelincuencia ha adquirido gran relevancia en el entorno colombiano y global; Actualmente, nuestra sociedad se encuentra cada vez más interconectada, dependiendo de la tecnología para realizar actividades cotidianas tanto a nivel personal como empresarial, generando como consecuencia, el aumento de la ciberdelincuencia como modalidad delictual, lo que representa una amenaza significativa para la seguridad de los individuos, las instituciones y el Estado. (Congreso de la República de Colombia, 2009).

La investigación propuesta aborda la gran necesidad de evaluar y comprender los posibles vacíos normativos en la legislación colombiana relacionados con los delitos cibernéticos. Dada la rápida evolución de las amenazas digitales y la complejidad de los actos delictivos en el ciberespacio, se evidencia la urgencia de examinar de manera exhaustiva la normativa actual para identificar posibles lagunas legales, justificándonos en la importancia de fortalecer el marco jurídico que regula la ciberseguridad, asegurando así una respuesta efectiva y proporcional a los desafíos emergentes, pretendiendo contribuir con este estudio , a la formulación de recomendaciones y propuestas de mejora que permitan cerrar posibles brechas legales, fortaleciendo la capacidad del sistema jurídico colombiano para hacer frente a las complejidades de la ciberdelincuencia y proteger de manera más efectiva los derechos y la seguridad de los ciudadanos en el entorno digital.

**Vacíos jurídicos de la ciberdelincuencia en la normativa colombiana**

La ciberdelincuencia, nace a partir del desarrollo acelerado de la internet, emergiendo del lado oscuro del mismo, describiendo de forma genérica los aspectos ilícitos cometidos en el ciberespacio (Pons, 2017, pág. 4) , siendo así , el conjunto de todas aquellas conductas criminales que para su realización necesitan implementar la tecnología, ya sea como método, medio o fin

(Gamba, 2019, pág. 21).También, es toda conducta ilícita que puede ser sancionada a la luz del derecho penal, por hacer uso indebido de la información y de cualquier medio informático empleados para su manejo, o de la tecnología electrónica o computarizada, en perjuicio de la libertad de las personas y organizaciones, o de su patrimonio, o propiedad como activos, o de su derecho a la vida, a la intimidad, al crédito y buen nombre (Camargo, pag.6)

En el panorama actual de la sociedad digital, la ciberdelincuencia se ha convertido en un desafío creciente y complejo. En el caso específico de Colombia, si bien ha habido esfuerzos significativos para abordar esta problemática, persisten vacíos jurídicos que dificultan la eficacia de la normativa vigente.

Camargo Buitrago, en su artículo regulación en Colombia de los delitos informáticos, nos dice que:

> Es fundamental, ver cómo una gran problemática los ciberdelitos, gracias a que día a día, esta modalidad de delinquir, aumenta de manera desmesurada. Según datos de la Dirección de Investigación Criminal e Interpol, desde el 2015 hasta este año 2019, en Colombia se han recibido 31.498 denuncias por delitos informáticos que abarcan desde el robo de data hasta la suplantación de una persona. Y no es para menos, en el país el internet se ha democratizado hasta tal punto que el 64% de los hogares y el 68% de las empresas tienen acceso a la red, y en los últimos ocho años se ha presentado un incremento del 70%, según información del Portal Oficial de Estadísticas del Sector TIC**.**

Los sujetos activos del cibercrimen son variados y operan en un entorno digital, aprovechando la complejidad y las conectividades públicas de la red. Entre estos autores, tenemos a los hackers, quienes poseen habilidades técnicas avanzadas que buscan vulnerabilidades en sistemas para explotarlas. En su mayoría, los sujetos activos que cometen este tipo de delitos, tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso informático, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. (Acuario Del Pino, 2010, pág.15)

Como lo indica Urueña centeno (2015) en su informe Ciberataques, la mayor amenaza actual:

> el ciber atacante se siente seguro, ya que no se expone físicamente a su víctima ni mucho menos a la posible intervención de las fuerzas de seguridad, dado que su acción delictiva se realiza *a distancia*; sensación de cómoda impunidad, al saber que hay lagunas legislativas a nivel internacional, por lo que muchos de los delitos cometidos no *se castigan*.

El derecho y la justicia se adaptan y evolucionan a la par con la sociedad. Las transformaciones sociales han venido propulsando los cambios jurídicos y, por supuesto, han ido incorporando instrumentos y protagonistas, además de modular algunos principios de la justicia. (Bustamante, Henao y Ramírez, 2023, pág.10)

En Colombia, a pesar de los avances en la concienciación sobre la ciberseguridad, persiste una brecha en la comprensión general de las amenazas digitales y las mejores prácticas para prevenirlas. La educación en informática se asienta en el manejo de Computadores y programas básicos de uso familiar y comercial no contemplando la seguridad informática como factor fundamental de prevenir y evitar los daños causados por la delincuencia (Serrano, 2014, pág. 9).

Tenemos que, el gran vacío que surge en Colombia, asienta sus raíces desde esta problemática, si no se comienza a educar adecuadamente a la sociedad desde las escuelas y las universidades, más adelante será más complicado que desarrollen buenas técnicas de prevención y combate frente a estos delitos. (Jiménez, 2022)

A medida que el uso de internet se ha extendido, ha aumentado el riesgo de su uso inadecuado. Los delincuentes cibernéticos viajan por el mundo virtual y realizan incursiones fraudulentas cada vez más frecuentes y variadas. Para hacer frente a esta gran problemática, varios países han dispuesto un sistema judicial especializado que permite procesarlos y castigarlos. A ese grupo de países se unió Colombia en 2009. (Ojeda, Rincón, Arias & Daza, 2010, pág.5).

Este tipo de delitos, comienzan a evidenciarse en Colombia cuando la Legislación incluye en su normatividad los delitos informáticos y establece penas por su ocurrencia, siendo el primer país que penaliza los delitos informáticos bajo el auxilio de la Ley 1273 de 2009 (Serrano,2014, pág. 9). Esta ley fue promulgada con el objetivo de abordar los crecientes desafíos legales vinculados a la ciberdelincuencia y proteger la integridad y seguridad de la información en el entorno digital.

Andrés Parra en su texto: **“**informáticos y marco normativo en Colombia”; escrito en el 2019, plantea la siguiente idea:

> El congreso de la república, ha gestado diferentes proyectos de Ley; unos tan efectivos que han rendido los mejores frutos en prevención y castigo a los ciber criminales y otros proyectos de Ley que a pesar de tener las modificaciones o decretos reglamentarios no han surgido ningún efecto positivo para el estado, es más, son proyectos de Ley tan vacíos que solo han permitido que el delincuente evade los controles jurídicos y procesales a los que han sido sometidos y por este caso no han tenido otro remedio más que el de derogarlos en el transcurrir del tiempo y por ende se genera la sensación de pérdida de tiempo valioso en crear e instaurar normas en algo tan importante como lo es la preservación de la información.

En Colombia, la implementación de tecnologías informáticas ofrece un aspecto tanto positivo, como negativo; Ha traído grandes beneficios, pero también ha logrado abrir las puertas a conductas antisociales y delictivas. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales (Acuña, Villa, 2018, pág.21)

En el país por desconocimiento de los fiscales o jueces, muchos delitos informáticos están siendo juzgados como delitos clásicos, y ubican al delito informático como una circunstancia de agravación que se usa para aumentar la pena. (Díaz, 2010, pág.12). El tratar los delitos informáticos como simples agravantes, en lugar de categorizarlos específicamente como ciberdelitos, puede crear una falta de claridad y especificidad en la legislación. Esto puede dificultar la identificación y persecución efectiva de las conductas delictivas específicas relacionadas con el ámbito digital.

Con lo anterior, hemos logrado evidenciar, que la ley en Colombia no satisface los requerimientos de seguridad informática, permitiendo que se creen vacíos que le dan paso a los ciberdelincuentes para mantener su actuar delictivo, existe un vacío en seguridad inmenso donde sólo se tratan los casos que más suenan a escala nacional e internacional (Serrano,2014, pág. 11). Además de que existe una enorme falta de divulgación, promoción y aplicación de la normatividad, también hace falta énfasis en la capacitación sobre la normatividad y cómo emplearla; se establece que en Colombia no existen expertos jurídicos en temas informáticos, dejando así la interpretación de la norma al libre albedrío (Serrano, 2014, Pág. 13). Esto puede llevar a interpretaciones erróneas, decisiones judiciales consistentes y dificultades en la aplicación efectiva de la legislación.

Ana María Pozo e Ingrid Pallarés, en su Estudio del marco normativo de protección de datos personales con objeto de prevenir la materialización de delitos informáticos que vulneran la dignidad humana. Análisis comparado entre Colombia y España nos dice que:

> En el año 2009, el Congreso de Colombia modificó el Código Penal, al crear un nuevo bien jurídico tutelado denominado “protección de la información y de los datos”; asimismo, preservó integralmente los sistemas que utilizan las Tecnologías de la Información y las Comunicaciones (TIC), a través de la Ley 1273 de 2009. Es decir, que el legislador incorporó, en el ordenamiento jurídico, elementos relacionados a las nuevas TIC, así como, con las nuevas figuras delictivas, con la intención de responder eficazmente a la criminalidad informática. Asimismo, mediante la Ley Estatutaria 1581 de 2012 reglamentada por los Decretos 1377 de 2013 y 1081 de 2015 se pretendió regular de forma integral la protección y tratamiento de datos personales. (Pag 13)

El Código Penal Colombiano, incluye delitos que pueden ser cometidos por medios informáticos, en este contexto se relacionan algunos como son; los delitos contra la intimidad, la usurpación y cesión de datos reservados de carácter personal, delitos contra el honor, calumnia e injuria, estafa, defraudaciones de fluido eléctrico e incluye de forma expresa la defraudación en telecomunicaciones siempre y cuando se utilice un mecanismo para la realización de la misma, o alterando maliciosamente las indicaciones o empleando medios clandestinos, delitos relativos a la propiedad intelectual (Cómo proteger las creaciones y proyectos desarrollados en una

empresa), delitos relativos a la propiedad industrial, delitos relativos al mercado y a los consumidores, publicidad engañosa cuando se hagan alegaciones falsas o manifiesten características inciertas sobre los mismos, causando un perjuicio grave y manifiesto a los consumidores (Fernández J, 2007).

La falta de una definición clara de ciertos delitos cibernéticos y la ausencia de penas proporcionadas y disuasorias también contribuyen a los vacíos jurídicos. Es esencial que la legislación colombiana aborde de manera precisa y exhaustiva los diferentes tipos de ciberdelincuencia, estableciendo sanciones proporcionales y actualizadas que reflejen la gravedad de los actos cometidos. (González M., 2017)

El vacío jurídico en torno a la ciberdelincuencia en Colombia representa una brecha preocupante que requiere de la búsqueda de soluciones. La ausencia de marcos legales y normativos para abordar la ciberdelincuencia deja a la sociedad vulnerable frente a las amenazas digitales en constante evolución. Para fortalecer la seguridad digital y proteger los derechos de los ciudadanos, es indispensable que las autoridades trabajen en la creación y actualización de leyes que se ajusten a la complejidad del panorama cibernético actual. La colaboración entre sectores público y privado también emerge como una necesidad crucial para garantizar un marco legal sólido que disuada eficazmente a los ciberdelincuentes y proteja los intereses digitales de la población colombiana. (Peña, 2016)

Finalmente, logramos evidenciar que estos vacíos, han llevado a Colombia a carecer de una óptima actualización en cuanto a legislación que hace frente a las amenazas cibernéticas que nos acarrean, adoleciendo totalmente de un buen apoyo de las entidades gubernamentales, enfrentando una necesidad de mejorar en cuanto a técnicas y alternativas para la persecución de los ciberdelincuentes, generando una gran importancia en obtener una fuerte colaboración internacional.

Como Estado, estos vacíos nos llevan a obtener una acumulación de problemáticas, que cada día se van volviendo más complicadas de resolver; se debe consolidar una legislación que sea ágil y actualizada, que nos brinde la oportunidad de poder generar estrategias de cooperación integral a nivel nacional e internacional, lo que nos traerá como beneficio el eficaz combate de la ciberdelincuencia.

**Consecuencias jurídicas del vacío normativo en la ciberdelincuencia en Colombia**

La ciberdelincuencia en Colombia se ha convertido en un desafío creciente en el desarrollo del entorno digital, generando grandes amenazas para la seguridad social. Un aspecto crítico que aumenta esta problemática, es el enorme vacío normativo que existe en la legislación colombiana relacionada con la ciberdelincuencia. Este vacío puede originar una serie de consecuencias jurídicas negativas que afectan la capacidad del sistema legal para abordar y prevenir eficazmente la consumación de delitos cibernéticos.

Las TIC interactivas se consideran un medio para facilitar las actividades delictivas antisociales que socavan la seguridad nacional y la aplicación de la ley y, por lo tanto, amenazan el tejido social de las sociedades capitalistas democráticas (Suarez, 2019, pág. 32).

Evidenciamos que una de las principales consecuencias que genera el vacío normativo en Colombia sobre ciberdelincuencia, es la Impunidad para los actores del delito**,** la carencia de mandatos legales frente a los crímenes desarrollados mediante dispositivos tecnológicos, deja un campo donde los ciberdelincuentes pueden actuar sin el temor a que esto genere para ellos perjuicios legales significativos. La falta de instrumentos jurídicos claros dificulta la identificación y seguimiento eficaz de los responsables, abriendo lugar a situaciones de impunidad.

Es necesario recalcar, que las personas dedicadas al cibercrimen, son personas con habilidades en el tema de la informática, a veces denominados piratas informáticos que navegan o roban ilegalmente información privada de una empresa o personas. En algunos casos, esta persona o grupo de individuos puede ser malicioso y destruir o dañar la computadora o los archivos de datos (Gamba, 2019, pág. 20)

La normatividad positiva, debe evolucionar y adaptarse al compás de la tecnología, día a día las tendencias y sistemas cambian, mejoran y evolucionan, entonces las leyes se van quedando obsoletas, Mitnick estadounidense que fue encarcelado durante 5 años por delitos informáticos, se dedica en la actualidad a burlar la seguridad de grandes empresas para después elaborar sistemas seguros, ya desde la legalidad. (Serrano, 2015, pág. 11)

De la misma manera, observamos que la otra de las consecuencias del vacío normativo es la inestabilidad legal, la confusión que existe en la implementación de la normativa crea un ambiente de inseguridad para las autoridades competentes y las víctimas de delitos cibernéticos. La interpretación y aplicación de las leyes existentes sobre la ciberdelincuencia son confusas, generando así, obstáculos para la implementación de la ley y en la defensa de los derechos de las víctimas, gracias a que es una modalidad muy actualizada, la cual no es de mayor entendimiento para los profesionales en derecho, legisladores y juristas, buscando así que estos adquieran nuevos conocimientos sobre la caracterización de las conductas informáticas ilícitas.(Cano, Diaz, Mendieta, Rivas, Sánchez, 2014, pag.23)

Es indispensable comprender, que la falta de normatividad, perjudica en gran medida a los juristas, evitando que ellos implementen de forma adecuada la normatividad, por culpa del gran vacío existente. Tiempo atrás, las viejas leyes no encajaban con los crímenes cometidos, las nuevas leyes no habían captado la realidad de lo que estaba sucediendo, y había pocos precedentes judiciales para buscar orientación (Gamba,2019, pág. 29). Bajo este suceso, se comenzaron a implementar nuevas normativas, pero estas continúan sin suplir lo necesario para un debido proceso.

La laguna normativa también genera consecuencias en cuanto a la ausencia de mecanismos claros para la recopilación de pruebas electrónicas. Esto presenta desafíos en la presentación de evidencia digital en procesos judiciales, evitando así, que los tribunales logren llevar a cabo investigaciones eficaces con resultados recuperables.

La limitación en la normatividad y en los métodos de recolección de pruebas es preocupante , gracias a que como afirmo Sutherland en 1943 "*El sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional*"; Lo que nos lleva a que la legislación vaya decreciendo y los delincuentes generando poco a poco nuevas estrategias de crimen cibernético.

Así mismo, la carencia de legislación específica puede resultar en una protección inadecuada de derechos fundamentales en cuanto a la víctima a la hora de implementar el uso de

la Web. La privacidad y la seguridad quedan sujetas a la vulnerabilidad, ya que no existen medidas claras para evitar que se genere la violación de estos derechos en la Web.

Tenemos como ejemplo de lo anteriormente mencionado, a los menores de edad, ellos son las personas más vulnerables a la hora de hablar de delitos cibernéticos, gracias a que estos poseen actualmente mayor accesibilidad a los aparatos tecnológicos desde edad temprana como resultado de normalizar el uso de estos dispositivos. Esto genera una gran problemática, debido a que los más pequeños son los más débiles y a quién más fácil pueden acceder los ciberdelincuentes.

El ciberbullyng, la pornografía, sextorsión, sexting y el grooming son tendencia en las redes sociales. Según el Centro Cibernético Policial (2017), “esta forma afecta principalmente al 75% de los niños, niñas y adolescentes, teniendo en cuenta que son más vulnerables al engaño y más vulnerables en el ciberespacio”. Asimismo, ha surgido otro fenómeno delictivo, el ciber espionaje, que afecta a todo lo concerniente. con la seguridad de la información teniendo esto una amplia gama de repercusiones en el sector económico (Ponal, 2017)

Esta problemática es una gran amenaza para nuestras futuras generaciones, resulta ser responsabilidad de las autoridades gubernamentales, comenzar a implementar medidas de seguridad más efectivas, que sean complicadas de vulnerar; Además, desarrollar mejores regulaciones, para así proteger a los niños de estas situaciones.

También tenemos que el carecer de una buena legislación sobre ciberdelitos, genera grandes desafíos a la hora de implementar la cooperación internacional para la búsqueda, investigación y persecución de ciberdelincuentes. Todo esto, gracias a que esto les genera desagrado a otros países, porque sienten que Colombia no les generaría un avance, sino que por el contrario sería un retroceso o una carga.

La falta de regulación por parte de las Entidades Estatales (Gobiernos), encargadas de elaborar las políticas públicas sobre este aspecto, impulsa a los ciberdelincuentes a transmitir virus a través de una serie de países utilizando sus servidores para realizar la transferencia de datos por canales que no cuentan con una buena seguridad del remitente al destinatario. (Fiscalía general del estado, 2011) Todos estos actos se realizan desde países en los que la legislación es

muy laxa, lo que permite por no contar con la cooperación internacional para mitigar este riesgo. Todos estos actos se realizan desde países en los que la legislación es muy laxa, lo que permite por no contar con la cooperación internacional para mitigar este riesgo. (López,2015, pág. 3)

De la misma manera, la ciberseguridad Nacional no se queda atrás frente a**l** vacío que evidenciamos en la legislación colombiana, gracias a que este puede llegar a generar el quebrantamiento de la capacidad del Estado para controlar las amenazas cibernéticas que se presentan a nivel nacional. En Colombia muchos delitos informáticos están siendo juzgados como delitos clásicos, y ubican al delito informático como una circunstancia de agravación que se usa para aumentar la pena. (Díaz, 2010, pag12).

En Colombia, la educación en informática se asienta en el manejo de Computadores y programas básicos de uso familiar y comercial no contemplando la seguridad informática como factor fundamental de prevenir y evitar los daños causados por la delincuencia (Serrano, 2015, pág. 9) las autoridades gubernamentales, las instituciones educativas y las empresas pueden desempeñar un papel importante en la promoción de la educación sobre seguridad cibernética, lo que incluye la implementación de políticas y regulaciones que fomenten la seguridad en línea

Por último, tenemos que esté vacío normativo, nos trae también afectación sobre la Incredulidad en los Sistemas Digitales, la falta de una buena estructura normativa frente a los ciberdelitos, crea en la sociedad, una gran desconfianza frente al uso de estos sistemas, lo que trae como consecuencia el retroceso económico social por la falta de uso y evolución de las nuevas tecnologías.

Evidenciamos la gran importancia que existe frente al desarrollo de una buena legislación sobre ciberdelitos, gracias a que esto genera para la sociedad, grandes, medianas y pequeñas consecuencias, que poco a poco, van evidenciando el crecimiento de nuestra sociedad y la gran caída económica que, a largo plazo, generaría para el país. La urgencia de abordar este vacío normativo es evidente para lograr fortalecer la capacidad del marco legal y proteger los derechos y la seguridad de la sociedad colombiana en la nueva era digital.

**Comparativa de la normativa internacional frente a las disposiciones que contiene la normativa Colombia en materia de ciberdelincuencia.**

La ciberdelincuencia se ha desarrollado como una preocupación global que trasciende las fronteras nacionales, gracias a que el Internet constituye uno de los principales impulsores de los cambios de muchas de las actividades desempeñadas por los ciudadanos, empresas, organizaciones y gobiernos en el actual mundo digital, convirtiéndoles en actores digitales cada vez más maduros e interactivos. (Osuna,2018,). Según la revista TyN ya hay cinco mil millones de usuarios de Internet en todo el mundo (TyN Magazine, 2022) lo que ha llevado a la promulgación de normativas a nivel internacional y nacional para abordar este problema en constante evolución. Es fundamental realizar una comparación entre las regulaciones internacionales y las leyes colombianas para evaluar sus similitudes, diferencias y eficacia en la lucha contra los delitos cibernéticos en este ámbito.

Barrios (2017) en su libro Ciberdelito: amenazas criminales del espacio, afirma que:

> El Internet se ha consolidado como pieza estructural de la Sociedad de la Información y desempeña un papel crucial en el desarrollo económico. La popularización de la Red a escala global ha permitido la creación del «ciberespacio virtual», tal y como lo concibiera el autor que acuñó tal término, William GIBSON, al haberse configurado de forma paralela al mundo físico un espacio comunicativo e interactivo que, especialmente en la última década del siglo XX, ha modificado las relaciones económicas, políticas, sociales y, muy especialmente, las personales. (Pag.2)

La amenaza de la ciberdelincuencia no se limita a Colombia, sino que es un tema que es abordado por gobiernos y empresas de todo el mundo. Para combatir estas amenazas cibernéticas cada vez mayores, los países pertenecientes a la unión europea han desarrollado sólidos programas de ciberseguridad y promulgado leyes destinadas a frenar la ciberdelincuencia y protegerse de los peligros digitales. (Fong, 2023)

A nivel mundial se presentan gran cantidad de delitos cibernéticos , entre ellos esta, el acoso escolar, intimidaciones, humillaciones, acoso sexual y agresiones psicológicas de forma constante con la intensión de someter a la víctima abusivamente; muchas veces no se sabe quién

es el responsable de este tipo de delitos ya que muchas personas crean perfiles falsos en Facebook y Twitter desde donde cometen estos ataques de forma anónima, por lo cual vemos y analizamos las mismas conductas dentro de los continentes, donde se sigue la misma línea de victimización. (Alvarado M., 2017)

Se evidencia que a nivel global los delincuentes se están aprovechando del desarrollo que está teniendo la web, para atacar a través de sus puntos débiles, las redes, infraestructuras y sistemas informáticos. La Interpol en su informe sobre Ciberdelincuencia, plantea que:

> El phishing, el ransomware y las violaciones de la seguridad de los datos son solo algunos ejemplos de las actuales ciber amenazas, eso sin contar que continuamente están surgiendo nuevos tipos de ciberdelitos. Los ciberdelincuentes son cada vez más ágiles y están mejor organizados, como demuestra la velocidad con que explotan las nuevas tecnologías, y el modo en que adaptan sus ataques y cooperan entre sí de forma novedosa.

La cooperación internacional para la lucha contra la ciberdelincuencia es imprescindible y se halla materializada en un conjunto de normas reguladoras de origen preferentemente convencional. El derecho interno tiende a facilitar la asistencia, de forma discrecional, atendiendo a principios de cortesía internacional o, más propiamente, de cooperación, utilizando con cierta frecuencia criterios de reciprocidad (Fernández y Sánchez, 2012).

Partiendo por Colombia, tenemos que al pasar de los años se ha tenido que adaptar al cambio constante en la sociedad y las nuevas modalidades de delinquir, lo que le ha llevado a generar cambios en las legislaciones de manera significativa en los últimos años, para así lograr enfrentar las amenazas emergentes que genera el cibercrimen. En este sentido, la Ley 1273 de 2009, también conocida como Ley de Ciberdelincuencia, es un pilar fundamental. Esta desarrolla delitos como acceso abusivo a sistemas informáticos, el daño informático y el fraude en medios electrónicos, creando disposiciones específicas para prevenir, investigar y sancionar esta tipología de conductas. La Ley 1581 de 2012 también regula la protección de datos personales, concediendo potestades al individuo para que pueda vigilar la información recolectada por una central de información y protegerse de un posible daño en su esfera íntima personal. (Ruíz, B,2016, Pag.4)

A continuación, evidenciamos como se desarrollan los tipos de ciberdelitos más destacados en la Ley 1273 del 2009:

**Ciberdelitos contenidos en la Ley 1273 de 2009**

| Clasificación de la protección | Delitos | Composición del punible según verbo rector y modalidad |
|---|---|---|
| **Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos** | Acceso abusivo a un sistema informático. | El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. |
| | Obstaculización ilegítima de sistema informático o red de telecomunicaciones. | El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones. |
| | Interceptación de datos informáticos. | El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte. |
| | Daño informático | El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos. |
| | Uso de *software* malicioso | El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos. |
| | Violación de datos personales | El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes. |
| | Suplantación de sitios *web* para capturar datos personales | El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes / El que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. |
| **De los atentados informáticos y otras infracciones** | Hurto por medios informáticos y semejantes | El que, superando medidas de seguridad informáticas, realice la conducta [hurto] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos. |
| | Transferencia no consentida de activos | El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave. |

Fuente: Mejía, Hurtado, Grisales, 2023, pág. 8.

Por otro lado, tenemos la Ley 1581 de 2012 se encarga de establecer los principios, deberes y derechos que las entidades públicas y privadas deben seguir al procesar la información confidencial de los ciudadanos colombianos. Esta ley tiene como objetivo proteger la privacidad y el control de la información personal de las personas y sancionar los incumplimientos que se lleven a cabo frente a esta.

En la sentencia T-176 del veinticinco (25) de marzo de dos mil catorce (2014), con ponencia del Magistrado Jorge Pretelt, se expone que:

> El reconocimiento del derecho fundamental autónomo al Habeas Data, busca la protección de los datos personales en un universo globalizado en el que el poder informático es creciente. Esta protección responde a la importancia que tales datos revisten para la garantía de otros derechos como la intimidad, el buen nombre, el libre desarrollo de la personalidad, entre otros. Sin embargo, el que exista una estrecha relación con tales derechos, no significa que no sea un derecho diferente, en tanto conlleva una serie de garantías diferenciables, cuya protección es directamente reclamable por medio de la acción de tutela, sin prejuicio del principio de subsidiariedad que rige la procedencia de la acción. (Corte Constitucional, 2014, p. 1).

Sin embargo, actualmente se encuentra necesario evaluar la idoneidad y eficacia de los distintos tipos penales existentes para combatir la delincuencia cibernética en Colombia. Resultando indispensable en la actualidad el recordar que los delitos informáticos incluidos en el título VII bis y modificados por la Ley 1273 del 2009 surgieron durante el año 2001, año en que se redactó la Convención de Budapest, que dio lugar a la Ley 1273 (Ámbito jurídico,2022, parr.2) lo que genera una desactualización en la normatividad, gracias a la constante evolución que se evidencia a través de los años de este tipo de modalidad delictual.

A nivel internacional, se han firmado acuerdos para establecer estándares compartidos y fomentar la colaboración entre naciones en la lucha contra la ciberdelincuencia, entre estos se encuentra la Convención de Budapest del Consejo de Europa, la cual es un recurso legal que aborda una amplia gama de delitos cibernéticos. El principal objetivo de este convenio es incrementar la cooperación internacional y generar marcos legales armónicos entre las naciones con el objetivo de hacer frente a los delitos informáticos y a la actividad criminal en internet.

(Cancilleria, 2022, párr.1) Este convenio, hasta la fecha, ha sido ratificado por 65 países, entre ellos Chile, Perú y Colombia, mientras que México mantiene un estatus de "observador" (Elizalde, Flores y Castro, 2021, Pag.5)

Colombia al ratificar el tratado de Budapest, requería una política pública criminal más completa, así como corregir las deficiencias de la Ley 1273/2009, la cual busco establecer la idea de protección de datos y sistemas de información (Karisma,2018) , pero que finalmente se quedó corta y no ahondo lo suficiente en el tema , como para cubrir todas las formas de crimen ideadas por los ciberdelincuentes, lo que llevo al estado a buscar otras alternativas , entre ellas la ratificación del convenio, buscando con este dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos. (Corte constitucional de Colombia, 2019, Sentencia c-224)

El convenio de Budapest (2001), nos habla en su capítulo III art 23 sobre cómo debe llevarse a cabo la cooperación internacional entre los estados firmantes del acuerdo, exponiéndonos lo siguiente:

> Las Partes cooperarán entre sí en la mayor medida posible de conformidad con las disposiciones del presente Capítulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

Tenemos entonces que, en casos que suponen el uso ilícito de las redes de comunicación, el convenio permite investigar y judicializar estos crímenes para que tanto Colombia, como los demás países que pertenecen al convenio no se conviertan en un paraíso donde los ciberdelincuentes extiendan sus redes. (Cancillería,2017)

Entre los países sudamericanos que han ratificado el convenio de Budapest (CBC) hemos destacado Colombia, Perú y chile, gracias a que son países con similitudes en su legislación y aplicabilidad de la misma, logrando así, analizar de qué manera desarrollan y compaginan este

convenio con sus leyes actuales o posteriores sobre ciberdelincuencia. (Mejía, Hurtado, Grisales, 2023, pág. 10)

Ignacio flores, en su artículo sobre la prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia (2015), desarrolla que:

> la aparición de supuestos de litispendencia internacional y de los consiguientes conflictos de jurisdicción en la persecución y castigo de la ciberdelincuencia, es más que previsible ante la falta de una autoridad internacional jurisdiccional, y de normas eficaces de armonización sustantiva y procesal —señaladamente de normas que fijen la competencia territorial internacional— capaces de contribuir a la determinación de la jurisdicción nacional idónea en caso de tramitación de procedimientos paralelos por parte de diferentes jurisdicciones.(Pag.9)

Adicionalmente, internacionalmente se han desarrollado políticas en temas de ciberseguridad y ciberdefensa, se han implementado nuevas capacidades tecnológicas y se han activado organismos para la creación de estas funciones, tal y como se evidencia en la siguiente tabla:

**Acciones tomadas para afrontar la Ciberdefensa a nivel de países**

| PAÍS | ACCIÓN NORMATIVA |
|---|---|
| Alemania | En febrero de 2011, el gobierno alemán lanzó su estrategia de Seguridad Cibernética. En abril de 2011 el Ministerio del Interior puso en marcha el Centro Nacional de Ciberdefensa. |
| Australia | Creó el Centro de Operaciones Cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio. |
| Canadá | El Departamento de Seguridad Pública implementó el Centro Canadiense de Respuesta a Incidentes Cibernéticos (CCIRC), y en octubre de 2010 adoptó la Estrategia Canadiense de Seguridad Cibernética. |

| | |
|---|---|
| Estados Unidos | Creó un Centro de Ciber-Comando Unificado que depende de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), DHS: National Cyber Security División, US-CERT: United States Computer Emergency Readiness Team y la oficina de Seguridad Cibernética de la Casa Blanca. En mayo de 2011 fue adoptada la Estrategia Internacional para el Ciberespacio. |
| Estonia | En 2008 creó conjuntamente con otros países de Europa, la OTAN y EE.UU. el Centro Internacional de Análisis de Ciberamenazas. En este mismo año es adoptada una Estrategia de Seguridad Cibernética. |
| Francia | Creó la Agencia de Seguridad para las Redes e Información (ANSSI), que vigila las redes informáticas gubernamentales y privadas con el fin de defenderlas de ataques cibernéticos. En febrero de 2011 que adoptada una Estrategia de Defensa y Seguridad de los Sistemas de Información. |

Fuente: Tomado de CONPES 84, (2004)

También evidenciamos otras normativas internacionales encargadas de combatir la ciberdelincuencia, son promulgadas por organismos como la Organización de Cooperación y Desarrollo Económico OCDE, la cual busco generar una regulación para que las legislaciones de los países miembros de la misma, no carecieran de medidas que erradicaran la delincuencia informática. Se encargo de crear una Comisión encargada de desarrollar un informe donde se plasmarán los principales problemas sobre la delincuencia informática y las dificultades técnicas para su erradicación.

Jesús Gamba (2019), en su artículo el delito informático en el marco jurídico colombiano y el derecho comparado: caso de la transferencia no consentida de activos, desarrolla la siguiente idea:

La interdependencia de los países dentro de la comunidad internacional también ha producido algunos referentes de organismos como las Naciones Unidas y los diferentes protocolos, donde se han analizado la necesidad de establecer convenios para combatir la ciberdelincuencia mediante la incorporación de las legislaciones internas, los lineamientos orientados a la prevención de las conductas delictivas. (pág. 61)

Entre los estados, se van sucediendo colaboraciones y entrecruzamiento de información para la investigación criminal provista a los órganos judiciales sin distinción de nacionalidad por parte de las prestadoras de servicios en internet (ESP) y de las prestadoras del servicio de internet (ISP). (Deluca y Del Carril, 2017). Gracias a que la ciberdelincuencia posee un carácter trasnacional por la implementación del internet, se hace necesaria la creación de tratados de extradición o acuerdos de ayuda mutua entre los países, permitiendo así, fijar mecanismos más eficaces para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar adecuadamente la incidencia de la criminalidad informática. (Ramírez, Aguilera,2009)

Aunque las regulaciones internacionales y colombianas tienen el mismo objetivo de combatir la ciberdelincuencia, hay algunas distinciones significativas. Por ejemplo, las leyes internacionales suelen ser más extensas y abordar una mayor variedad de delitos cibernéticos, mientras que las leyes colombianas se enfocan en delitos específicos y en la protección de datos personales.

Bruna Martins (2022) En su libro “Convenio de Budapest sobre la Ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México” nos plantea que:

> Debido a las diferencias en las leyes nacionales y los procedimientos legales, la cooperación entre países puede ser un desafío a nivel internacional. En Colombia, la aplicación efectiva de las leyes puede encontrar dificultades debido a la capacidad institucional y la disponibilidad de recursos. La elaboración de políticas públicas para temas relacionados a cibercrímenes ha favorecido perspectivas relacionadas con la defensa y seguridad cibernética, buscando facilitar el uso de la información en los procesos judiciales y prevenir o anticipar la consumación de crímenes cibernéticos. (Pág. 28)

Actualmente los recursos que son brindados para el combate del ciberdelito en Colombia siguen teniendo falencias, sin embargo, como país se siguen buscando y generando alternativas para el óptimo enfrentamiento frente a estos delitos, la adhesión al convenio de Budapest fue un gran salto que dio Colombia frente a esta lucha, sin embargo, como nos lo exponen en su estudio

comparativo Mejía, Hurtado, Grisales. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones:

> la normativa colombiana aún tiene un camino abierto y que debe reconocer las falencias para realmente instituir los ciberdelitos según sus modalidades pluriofensivas y sus manifestaciones de orden particular. No basta con tener una adhesión al convenio de Budapest para efecto de lucha transnacional contra el cibercrimen, antes bien, deben proveerse los mecanismos y herramientas legales para que la persecución de los precitados punibles tenga el sentido que aquel instrumento busca. (Pág. 14)

Tanto las regulaciones a nivel global como las que se aplican en Colombia constituyen avances significativos en la lucha contra la ciberdelincuencia, aunque ambas tienen sus propias particularidades y retos. Para hacer frente a este desafío global y proteger la seguridad y la privacidad en el mundo digital, se requiere una colaboración continua entre países y una aplicación efectiva de las leyes a nivel nacional.

## Conclusiones

A raíz de esta investigación, hemos evidenciado la constante complejidad y desarrollo que se ha venido generado a través de los años frente a la ciberdelincuencia en Colombia, generando así la adaptación de los delincuentes a los avances en las nuevas tecnologías y las estrategias para vulnerar su seguridad. Se evidencian enormes desafíos para las entidades encargadas de hacer frente a este tipo de delitos, en cuanto a la detección, prevención y persecución de los mismos, lo que resalta la necesidad de una normatividad actualizada y eficiente.

Logramos la identificación de grandes brechas en la normatividad colombiana frente a los ciberdelitos; identificando así, desafíos jurídicos para los ciudadanos, como lo serian la falta de claridad en las definiciones, el vago progreso existente en las leyes para hacer frente a estos delitos , la limitada capacidad para llevar acabo un buen abordaje frente a los aspectos internacionales y transfronterizos y también con el contar con capacidades que permitan alinear el desarrollo tecnológico con las políticas existentes para la gestión de riesgos en ciberseguridad( Asobancaria, 2019, pág. 87).  Lo que nos lleva a resaltar la necesidad que afronta el país, para

realizar reformas legales que logren combatir de manera eficaz la constante evolución que tiene este tipo de modelos delictuales.

Evidenciamos que la desactualización de la normatividad colombiana en materia de ciberdelincuencia, resulta ser un desafío significativo en la protección de la seguridad digital del país. La Ley 1273 de 2009, aunque fue un gran paso a la evolución en su momento, actualmente no logra abarcar la complejidad y diversidad de los ciberdelitos, dejando vacíos legales que pueden ser usados en beneficio de los delincuentes. La rápida evolución tecnológica demanda una revisión y actualización constante de las leyes para así lograr garantizar una respuesta efectiva frente a amenazas que se presentan en la actualidad, como el ransomware, el phishing avanzado y los ataques a infraestructuras críticas. Asimismo, es crucial fortalecer la cooperación internacional y proporcionar formación continua a las autoridades encargadas de la ciberseguridad.

Finalmente, hemos concluido que la carencia de un óptimo marco normativo, conlleva a que se generen gran variedad de obstáculos para el eficaz combate frente a los ciberdelitos, además, esto crea un impacto negativo en cuanto a la confianza de los ciudadanos sobre su seguridad digital y en cómo se previenen este tipo de vulneraciones. La conclusión subraya la urgencia de medidas legislativas y de políticas públicas que fortalezcan la respuesta del país ante la ciberdelincuencia, protegiendo así la integridad de la sociedad y la infraestructura digital.

**Bibliografía**

Acuario, S. (2023). Delitos Informáticos: Generalidades. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

Acuña, Villa. (2018). estado actual del cibercrimen en Colombia con respecto a Latinoamérica. https://repository.unad.edu.co/bitstream/handle/10596/25619/%20%09lfacunal.pdf?sequence=1&isAllowed=y

Alvarado, M. (2017). Aspectos legales al utilizar las principales redes sociales en Colombia.https://www.redalyc.org/journal/5177/517752177019/html/#:~:text=En%20la%20l

egislaci%C3%B3n%20colombiana%20existen,la%20Informaci%C3%B3n%20y%20los%20Datos.

Ámbito jurídico. (2022). Los desafíos del delito informático. https://www-ambitojuridico-com.luisamigo.proxybk.com/noticias/especiales/penal/los-desafios-del-delito-informatico

Asobancaria. (2019). *Desafíos del riesgo cibernético en el sector financiero para Colombia y américa latina*. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Barrios. (2017). Ciberdelito: amenazas criminales del espacio.https://www.moisesbarrio.es/pdf/libro_ciberdelitos.pdf

Budapest. (2001). Convenio sobre la Ciberdelincuencia. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Bustamante, Henao y Ramírez. (2023). https://mail.google.com/mail/u/1/#search/dany.gomezag%40amigo.edu.co/FMfcgzGwHLpZdSNvFTwcMjHknPQGXSvd?projector=1&messagePartId=0.1

Camargo, L. (s.f) Regulación en Colombia de los delitos informáticos. https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/5727/Articulo%20regulaci%C3%B3n%20delitos%20informaticos%20en%20Colombia.pdf?sequence=

Cancillería. (2017). Gobierno radicó Proyecto de Ley para adherirse al Convenio sobre la ciberdelincuencia (Convención de Budapest). https://www.cancilleria.gov.co/newsroom/news/gobierno-radico-proyecto-ley-adherirse-convenio-ciberdelincuencia-convencion-budapest

Cano, Diaz, Mendieta, Rivas, Sánchez. (2014). Aporte internacional frente a los delitos informáticos en Colombia y su ejecución por parte de las autoridades competentes. https://repository.unilibre.edu.co/bitstream/handle/10901/7695/CanoCuervoAlejandra2014.pdf?sequence=1&isAllowed=y

Código de Procedimiento Penal Colombiano (CPP - Ley 906 de 2004. 31 de agosto de 2004.).

Congreso de la República de Colombia. (2009). Ley 1273 del 2009.

Corte constitucional. (2019). Sentencia C-224/19.

Corte constitucional. (2014). Sentencia T- 176/14.

Del Pino, S. (2010) Delitos informáticos generalidades. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

Deluca, S y Del Carril, E. (2017). Cooperación internacional en materia penal en el MERCOSUR: el cibercrimen. Revista de la Secretaría del Tribunal Permanente de Revisión. https://doi.org/10.16890/rstpr.a5.n10.p13

Díaz, G. (2010) El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el convenio de Budapest. En: Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR.

Díaz, G. (2010). Aniversario en Colombia del nuevo delito de violación de datos personales. Primer año de vigencia de la Ley de Delitos Informáticos., p. 175

Elizalde, Flores y Castro. (2021). Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho comparado. https://iuscomitialis.uaemex.mx/article/view/17320/12891

Fernández, J. & Sánchez, S. (2012). Diplomado en Derecho de los Negocios In- ternacionales. Fundación Global, Democracia y Desarrollo (Funglode) y Universidad Complutense de Madrid

Fernández, J. (2007) Respuesta penal frente a fraudes cometidos en internet: Estafa, estafa informática y los nudos de la red, UNED. Revista de Derecho Penal y Criminología, 19 (2), pp. 210-230.2

Fiscalía General del Estado (2011) sobre el fiscal de sala de criminalidad informática y las secciones de criminalidad informática de las fiscalías. [En línea]. Madrid, 2011. [Consulta: 23 marzo 2017].

Flores, I. (2015). prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia. https://www.pensamientopenal.com.ar/system/files/2016/01/doctrina42833.pdf

Fong, J. (2023). Informe global sobre ciberdelincuencia: países con mayor riesgo en 2023. https://seon.io/es/recursos/informe-global-sobre-ciberdelincuencia-que-paises-corren-mayor-riesgo/

Gamba, J. (2019). El delito informático en el marco jurídico colombiano y el derecho comparado: caso de la transferencia no consentida de activos. https://bdigital.uexternado.edu.co/server/api/core/bitstreams/2e7e30f3-4a1f-45f6-b59a-dae6012b7210/content

González, M. (2017) La cibercriminalidad como instrumento para la expansión y empoderamiento del crimen organizado, Grupo de estudios en seguridad internacional, Universidad de Granada, pp. 13-45.

INTERPOL. (s, f). Ciber amenazas relacionadas con la COVID-19. https://www.interpol.int/es/Delitos/Ciberdelincuencia/Ciberamenazas-relacionadas-con-la-COVID-19#:~:text=En%20los%20sitios%20web%20y,sus%20ordenadores%20o%20dispositivos%20m%C3%B3viles.

Interpol. (s. f.). La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad. https://www.interpol.int/es/Delitos/Ciberdelincuencia

Jiménez (2022), Ciberdelincuencia: evolución y relación con la actual situación de pandemia. nuevas modalidades y nuevas problemáticas, Universidad de Salamanca.

Karisma. (2018). Convenio de Budapest: Aplicación en Colombia frente a los derechos humanos. minuta_karisma.pdf (derechosdigitales.org)

Ley 1273. (2009). *Congreso de la República*.

Ley 1581. (2012). *Congreso de la Republica*.

López, E. (2015) Ciberseguridad de Gobierno. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2811/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Martins, B. (2022). Convenio de Budapest sobre la Ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México. https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf)

Mejía, Hurtado, Grisales. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo.Dialnet-LeyDeDelitosInformaticosColombianaElConvenioDeBuda-8920556 (5).pdf

Ministerio de Hacienda y Crédito Público (2004), Conpes Social. Ajuste a la destinación de la participación de propósito general 2004 al fonpet, Bogotá D.C

Min Tic (2021). Gobierno radicó Proyecto de Ley para adherirse al Convenio de Budapest contra la ciberdelincuencia. (https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/56315:Gobierno-radico-Proyecto-de-Ley-para-adherirse-al-Convenio-de-Budapest-contra-la-ciberdelincuencia).

Ojeda, Rincón, Arias & Daza. (2010) Delitos Informáticos y entorno jurídico vigente en Colombia, Cuadernos De Contabilidad, 11(28), pp 20-53. Recuperado a partir de https://revistas.javeriana.edu.co/i ndex.php/cuacont/article/view/3176.

Organización para la Cooperación y el Desarrollo Económicos (OCDE). https://www.oecd.org/espanol/

Osuna, J. (2018) Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea. Revista de Estudios en Seguridad Internacional. http://dx.doi.org/10.18847/1.7.7

Parra, A.(2019).DELITOS INFORMÁTICOS Y MARCO NORMATIVO EN COLOMBIA.https://repository.unad.edu.co/bitstream/handle/10596/28115/%20%09jparraca.pdf?sequence=1&isAllowed=y.

Peña, D (2016). Llegó la hora de tomar en serio los delitos informáticos Llegó la hora de tomar en serio a los Delitos Informáticos - PM Abogados

Plan nacional de desarrollo de Colombia. (2018). https://colaboracion.dnp.gov.co/CDTI/Agenda%20Semanal/AGENDA%20LEGISLATIVA%20DEL%2025%20AL%2029%20DE%20JUNIO%20-2018.pdf.

Policía Nacional, (2021). Tendencias cibercrimen Colombia 2019-2020. CAI Virtual de la Policía Nacional de Colombia. https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_ -_2020_0.pdf

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. Revista Latinoamericana de Estudios de Seguridad. https://revistas.flacsoandes.edu.ec/urvio/article/view/2563/1608

Pozo, Pallares. (2022). Estudio del marco normativo de protección de datos personales con objeto de prevenir la materialización de delitos informáticos que vulneran la dignidad humana. Análisis comparado entre Colombia y España. https://repository.usta.edu.co/bitstream/handle/11634/48392/2022PallaresIngrid.pdf?sequence=9.

Ramírez, E y Aguilera, A. (2009). Los delitos informáticos. tratamiento internacional. https://www.eumed.net/rev/cccss/04/rbar2.htm

Ruíz, B. (2016). Regulación en materia de protección de datos personales o habeas data en Colombia a través de la Ley 1581 de 2012: examen histórico y crítico sobre su ineficacia ante las administradoras de bases de datos, portales de Internet y motores de búsquedas. http://hdl.handle.net/10983/13794

Serrano, E. (2014). La práctica de delitos informáticos en Colombia. https://repository.unimilitar.edu.co/bitstream/handle/10654/13452/Ensayo%20%20Edison%20Serrano%20EAS.pdf?sequence=1&isAllowed=y

*TyN Magazine*. (2022). *Cinco mil millones de personas utilizan Internet en todo el mundo.* https://tynmagazine.com/cinco-mil-millones-de-personas-utilizan-internet-en-todo-el-mundo/

Urueña Centeno, Francisco Javier. 2015.Ciberataques, la mayor amenaza actual. http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf