# EL IMPACTO TRANSFORMADOR DE LOS CIBERDELITOS EN EL SISTEMA PENAL COLOMBIANO.

JUAN FELIPE CARTAGENA TREJOS.

LAURA MARCELA HERNANDEZ JIMENEZ.

**RESUMEN**.

El presente artículo aborda el tratamiento jurisprudencial de los ciberdelitos en el sistema penal colombiano desde una perspectiva integral y en constante evolución, teniendo en consideración los ciberdelitos como conductas punibles en el ciberespacio que atentan contra los bienes jurídicos de los cibernautas. Con el crecimiento exponencial del uso del internet y la expansión del ciberespacio, los Estados se han visto en la necesidad de establecer tratados internacionales, normas y leyes para regular la convivencia en la realidad virtual y proteger a los cibernautas y su información personal.

En Colombia, se ha implementado un marco normativo extenso para proteger a los cibernautas y su interacción en el ciberespacio, incluyendo el derecho de *hábeas data*, el cual salvaguarda la privacidad y la protección de los datos personales de los usuarios. Entre los delitos informáticos que se abordan, se encuentra el acceso abusivo a sistemas informáticos, regulado por la Ley 1273 de 2009, delito que se configura cuando alguien accede a un sistema informático sin autorización o, incluso teniendo el permiso del titular, se mantiene dentro del mismo excediendo las facultades otorgadas.

En tal sentido, yace aquí la importancia de establecer normas específicas para combatir los delitos informáticos, y se refuerza mediante la ratificación por parte de Colombia del Convenio sobre la Ciberdelincuencia, adoptado en Budapest en 2001, convenio

que tiene como objetivo fortalecer las relaciones internacionales entre Estados para enfrentar la ciberdelincuencia y proteger los derechos de los cibernautas en el entorno digital al ajustarse a los fines esenciales del Estado al garantizar, proteger y prevenir los ataques y violaciones de derechos que pueden sufrir los usuarios del ciberespacio, convirtiéndose este en una herramienta fundamental para la cooperación internacional en la lucha contra los delitos informáticos.

Se tratarán temas como la relevancia de la ciberseguridad en la prevención de la ciberdelincuencia. La rápida evolución tecnológica y la sofisticación de los ataques cibernéticos hacen indispensable el desarrollo de medidas de seguridad eficaces para proteger a los cibernautas y sus datos personales. La cooperación internacional se presenta como un aspecto crucial en este ámbito, ya que los delitos informáticos trascienden las fronteras nacionales y requieren una respuesta coordinada y conjunta entre los Estados.

El presente artículo presenta información relevante sobre la ciberdelincuencia y los delitos informáticos en Colombia, así como el marco legal que ha sido establecido para prevenir y combatir este tipo de delitos. Aunado a esto, se destaca la importancia de la Ley 1273 de 2009, que ha sido un hito significativo en la lucha contra la ciberdelincuencia en el país porque subraya la necesidad de continuar fortaleciendo las políticas de ciberseguridad y la cooperación internacional para enfrentar de manera efectiva esta problemática que afecta a nivel mundial. La implementación de políticas públicas de seguridad informática y programas de concientización se sugiere como una forma de prevenir y combatir eficazmente los delitos informáticos, garantizando así la seguridad y los derechos de los ciudadanos en el entorno digital. La lucha contra los delitos informáticos requiere un enfoque multifacético y colaborativo para salvaguardar la integridad del ciberespacio y proteger a los usuarios de las amenazas que puedan surgir en el ámbito digital.

***Palabras Claves:*** Ciberdelito, Ciberespacio, internet y Derechos Humanos de Cuarta generación.

**ABSTRACT**.

This article addresses the jurisprudential treatment of cybercrimes in the Colombian penal system from a comprehensive and constantly evolving perspective, considering cybercrimes as punishable behaviors in cyberspace that threaten the legal interests of internet users. With the exponential growth of internet usage and the expansion of cyberspace, states have found it necessary to establish international treaties, norms, and laws to regulate coexistence in virtual reality and protect internet users and their personal information.

In Colombia, an extensive regulatory framework has been implemented to protect internet users and their interactions in cyberspace, including the right to habeas data, which safeguards privacy and the protection of users' personal data. Among the addressed computer crimes is abusive access to computer systems, regulated by Law 1273 of 2009, a crime that occurs when someone accesses a computer system without authorization or, even with the owner's permission, remains within it exceeding the granted faculties.

In this sense, it becomes essential to establish specific norms to combat computer crimes, reinforced by Colombia's ratification of the Budapest Convention on Cybercrime adopted in 2001. This convention aims to strengthen international relations between states to combat cybercrime and protect the rights of internet users in the digital environment, aligning with the essential purposes of the state to guarantee, protect, and prevent attacks and violations of rights that cyber users may suffer, becoming a fundamental tool for international cooperation in the fight against computer crimes.

The article will address topics such as the relevance of cybersecurity in preventing cybercrime. The rapid technological evolution and sophistication of cyber-attacks make the development of effective security measures indispensable to protect internet users and their

personal data. International cooperation presents itself as a crucial aspect in this field since computer crimes transcend national borders and require a coordinated and joint response between states.

The present article provides relevant information about cybercrime and computer crimes in Colombia, as well as the legal framework established to prevent and combat this type of offense. In addition to this, the importance of Law 1273 of 2009 is highlighted, which has been a significant milestone in the fight against cybercrime in the country, and the need to continue strengthening cybersecurity policies and international cooperation to effectively address this issue that affects worldwide.

The implementation of public policies on information security and awareness programs is suggested to prevent and effectively combat computer crimes, ensuring the security and rights of citizens in the digital environment. The fight against computer crimes requires a multifaceted and collaborative approach to safeguard the integrity of cyberspace and protect users from threats that may arise in the digital sphere.

***Key Word:*** Cybercrime, Cyberspace, Internet, and Human Right fourth generation.

**INTRODUCCIÓN.**

En la era contemporánea, el exponencial avance tecnológico ha dado lugar a la expansión de la delincuencia informática o ciberdelitos, los cuales han surgido como un fenómeno complejo y multifacético que desafía la integridad del sistema penal tradicional. Estos delitos cibernéticos abarcan una amplia gama de actividades ilícitas que tienen lugar en el ámbito digital, incluyendo el robo de información, el fraude financiero, la distribución de contenido ilegal, el ciberacoso y el sabotaje cibernético, entre otros. Su naturaleza transnacional, carácter sofisticado y la relativa facilidad para el anonimato han provocado un aumento significativo en la cantidad y complejidad de los delitos informáticos.

Este nuevo paradigma de delincuencia ha impactado de manera notable tanto en el ámbito individual como en el colectivo, generando consecuencias económicas, sociales y políticas que trascienden fronteras y desafían los marcos normativos y operativos del sistema penal. Los ciberdelincuentes han demostrado una capacidad sin precedentes para traspasar barreras geográficas y jurisdiccionales, lo que ha dificultado enormemente su persecución y sanción por parte de las autoridades tradicionales.

Ante esta realidad, los sistemas penales a nivel global se han visto obligados a emprender transformaciones sustanciales para afrontar eficazmente el creciente desafío de los ciberdelitos. En este sentido, los legisladores han tenido que promulgar nuevas leyes y reformar las existentes para adecuarlas a la realidad digital y abordar los distintos aspectos y manifestaciones de estos delitos. Se ha buscado así establecer un marco jurídico que contemple la singularidad del ciberespacio, garantizando la protección de los derechos y la seguridad de los ciudadanos en el entorno virtual.

Además, los órganos encargados de aplicar la ley han tenido que enfrentar el reto de adquirir habilidades técnicas y conocimientos especializados en el campo de la ciberseguridad, a fin de investigar y rastrear eficazmente las actividades delictivas llevadas a cabo a través de la red. La colaboración entre fuerzas policiales y expertos en tecnología de la información se ha convertido en un componente crucial para el éxito en la lucha contra los ciberdelincuentes, ya que estos actúan con frecuencia de manera anónima y sofisticada, desafiando la capacidad de las fuerzas tradicionales de aplicación de la ley para combatirlos.

En el ámbito internacional, la cooperación y coordinación entre países se ha vuelto esencial para enfrentar el fenómeno transnacional de los ciberdelitos. Los delincuentes digitales operan a menudo desde ubicaciones geográficas remotas, traspasando fronteras sin dificultad y evadiendo así la persecución de las autoridades nacionales. Por ello, el intercambio de información y evidencia entre Estados se ha erigido como una estrategia clave

para mejorar la eficiencia y efectividad de las investigaciones y enjuiciamientos relacionados con ciberdelitos.

Es así como los ciberdelitos han emergido como una fuente de transformación del sistema penal en la era digital. Su complejidad y alcance han puesto de manifiesto la necesidad de reformas legislativas, capacidades tecnológicas y cooperación internacional para abordar eficazmente esta forma de delincuencia. La protección de los ciudadanos, empresas e instituciones en el ciberespacio se convierte en un reto ineludible para los sistemas de justicia penal, demandando una respuesta proactiva y adaptable frente a una realidad delictiva en constante evolución.

## 1. El Tratamiento Jurisprudencial en Torno a la Regulación de los Ciberdelitos en el Sistema Penal Colombiano.

Para iniciar con el desarrollo del capítulo es necesario hacer un breve recuento histórico y conceptual sobre los ciberdelitos en el ordenamiento jurídico Colombiano, ya que su trascendencia para el mundo moderno se deriva de los derechos de cuarta generación o derechos de la tecnología, lo que originó nuevas modalidades delictivas. Por este motivo, se puede afirmar que el concepto de ciberdelito deviene de las conductas punibles desplegadas en el ciberespacio que atenta contra los bienes jurídicos tutelables de los cibernautas.

El ciberespacio ha transformado la manera como los seres humanos interactúan y el internet es el medio para que ello sea posible, sin embargo, la ciencia jurídica no ha sido la excepción frente a los cambios que produjo la integración del internet a las formas de comunicación del *Hombre* ya sea frente a factores económicos, sociales o políticos, lo cual condujo a los Estados a proferir tratados internacionales, normas y leyes, con la finalidad de regular el ejercicio del derecho de los cibernautas para perpetuar la convivencia en la realidad virtual.

En el caso de Colombia existen un marco normativo extenso que busca la protección

de los cibernautas y su interacción en el ciberespacio, así como la información personal que se encuentra en cabeza de las entidades de privadas y estatales, es un derecho conocido como habeas data regulado por la Ley 1266 de 2008 y  Ley 1581 del 2012, su protección se encuentra amparado en la Constitución Política de Colombia,

Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. (Constitución Política de Colombia [C.P.],1991,art.15)

A partir de la cita anterior se puede afirmar que es una derecho fundamental, sujeto al amparo constitucional Acción de tutela, regulada por el Artículo 86 y fundando en el Artículo 85 de la Carta Política, en el evento en que la vulneración transgrede de la órbita constitucional y se configure un ciberdelito fundado en la ley 1273 del 2009, también conocida como el bien jurídico *de la protección de la información y de los datos* configurando la acción en objeto de conocimiento del sistema penal, puesto que son conductas que se agrupan en el delito de acceso abusivo a sistemas informáticos, frente a su regulación la Corte Suprema de Justicia (2002) señaló que los elementos normativos que configuran la conducta punible son:

> i) Sujeto activo no calificado, por no necesitar de una condición especial para quien accede a un sistema informático “sin autorización”, o que, teniéndola, decide conscientemente mantenerse conectado; ii) Sujeto pasivo, persona natural o jurídica titular del sistema informático, iii) Lesionar varios bienes jurídicos tutelados, entre ellos, la información, los datos y la intimidad. En ese sentido, ha sido reconocido como un tipo penal pluriofensivo, iv) Solo admite el dolo en el actuar del ciberdelincuente; v) Es un delito de mera conducta, por cuanto, la sola intromisión en

> una red informática, en las condiciones establecidas en el tipo penal, afecta el bien jurídico tutelado; vi) Contempla dos verbos rectores, acceder o mantener. (Corte Suprema de Justicia, Sala de Casación Penal, SP592, 2022).

Es evidente que la Corte Suprema de Justicia marcó una línea jurisprudencial frente a la sanciones impuestas al tenor de la ley 1273 del 2009 puesto que, en la sentencia señalan que el delito *Acceso Abusivo a Sistemas Informáticos* se agrupan en conductas de mero acceso, lo que significa que son acciones desplegadas por el sujeto activo que nacen a la vida jurídica con la mera permanencia en la red de datos, ya que, solo se necesita la introducción ilegítima sin previa autorización del titular de la cuenta, por este motivo, el delito se refleja en la perpetración de la password[1], que abre paso en los sistemas informáticos.

De conformidad con el apartado anterior, se puede precisar que la conducta punible se entiende como intrusismo informático, es cuando una personas o varias acceden ilegalmente a una plataforma de base de datos, la ilegalidad de dicha conducta se configura porque no se encuentran autorizados a penetrar la red, sin embargo, la Corte expuso que el ingrediente normativo que deben exigir los jueces y probar los fiscales es que "el sujeto activo de la acción a) acceda en el sistema informático sin autorización, o, b) aun cuando, teniendo el permiso del titular legítimo del derecho, se mantiene dentro del mismo, excediendo las facultades otorgadas" (Corte Suprema de Justicia, Sala de Casación Penal, SP592, 2022).

Aunque la ley 1273 del 2009 se encuentra en vigencia hace 14 años, es un delito que no se presentaba con frecuencia, puesto el sujeto activo puede ser cualquier ciudadano con el ánimo de perpetrar en sistemas de información, el titular de la acción cuenta con las cualidades y habilidades de navegación en medios digitales, que le permite acceder o

[1] Es una palabra de origen inglés, la cual hace referencia a contraseña o clave de acceso.

mantener en plataformas digitales generando afectaciones propietario de su cuenta o información, se puede afirmar que es un delito que nace a la vida jurídica a partir de las nuevas necesidades derivadas de las telecomunicaciones, por este motivo los Estados en el mundo optaron por firmar tratados con el fin de proteger la convivencia en de los cibernautas.

Colombia ratificó en el orden interno el convenio sobre la ciberdelincuencia adoptado el 23 de noviembre de 2001, en Budapest con la finalidad de fortalecer las relaciones internacionales entre Estados y enfrentar la problemática con un organismo jurídico que equipare la ilicitud de las conductas desplegadas en el ciberespacio o base de datos, dado que, los actores delincuencias pueden cometer el hecho ilícito desde cualquier parte del mundo, puesto que la acción es susceptible a las redes de comunicación, por ello resulta imprescindible la colaboración judicial entre Estados, para que la ciudadanía sea orientada frente a la prevención de los ciberdelincuentes y los sistemas penales puedan establecer un alto a la conducta ilícita en materia cibernética.

Cabe señalar que el Convenio sobre la ciberdelincuencia se ajusta a los fines de esenciales del Estado[2] pues con este se busca garantizar, proteger y prevenir a los cibernautas de los diferentes ataques y violaciones de derechos que pueden sufrir por los ciberdelincuentes, por ello el ministerio de justicia y derecho en sentencia C-224 del 2019 expuso que:

> El Convenio sobre la Ciberdelincuencia defiende fines constitucionalmente válidos y su ratificación busca materializar los lineamientos de política pública relacionados con la ciberseguridad, la ciberdefensa y la prevención de la cibercriminalidad adoptadas a través de los documentos CONPES 301 de 2011 y 3854 de 2016, en los que se precisa la necesidad de contar con estrategias complementarias,

[2] Los fines esenciales se encuentran regulados por el Artículo 2 de la Constitución Política de Colombia el cual consagra las obligaciones que tiene Colombia como Estado Social de Derecho de garantizar a todos sus habitantes.

> procedimentales y de cooperación internacional, entre otras, dirigidas a articular esfuerzos y consolidar una política de protección común en temas de escala y afectación global. (Corte Constitucional, Sala Plena de la Corte, C-224/19).

De la cita anterior se puede precisar que, el Convenio sobre la Ciberdelincuencia ratificado por Colombia se alinea con los objetivos esenciales del Estado, teniendo como finalidad garantizar, proteger y prevenir a los cibernautas de los diversos ataques y violaciones de derechos que puedan sufrir por parte de los ciberdelincuentes.

La ratificación de este convenio busca materializar los lineamientos de política pública relacionados con la ciberseguridad, ciberdefensa y prevención de la cibercriminalidad, los cuales han sido previamente adoptados a través de documentos oficiales como el CONPES 301 de 2011 y el CONPES 3854 de 2016.

En síntesis, la normatividad colombiana ha buscado proteger a los ciudadanos y su interacción en el ciberespacio, especialmente en lo que respecta a la protección de la información personal. La Ley 1581 del 2012, que regula el *habeas data,* ha sido fundamental en este aspecto, amparando el derecho fundamental a la intimidad y la protección de los datos. Así las cosas, la regulación de los ciberdelitos en el sistema penal colombiano ha sido un proceso dinámico y necesario para proteger a los ciudadanos frente a los nuevos desafíos tecnológicos; la definición y enjuiciamiento de los delitos informáticos han evolucionado gracias a la labor de la Corte Suprema de Justicia, y la cooperación internacional desempeña un papel clave en la prevención y enfrentamiento de esta problemática. No obstante, la protección de los cibernautas y la preservación de la seguridad en el ciberespacio son objetivos fundamentales en el marco de la evolución de los derechos de cuarta generación en la era digital.

## 2. La Prevención de la Ciberdelincuencia de Conformidad con la Ley 1273 de 2009.

En la actualidad, el delito de acceso abusivo a sistemas informáticos representa una de las amenazas más significativas a nivel mundial; el rápido avance de la tecnología ha permitido que la comisión de este delito sea altamente rentable, lo que ha generado serias preocupaciones en diferentes países. Para hacer frente a esta problemática, varias naciones han suscrito el "Convenio sobre la ciberdelincuencia" del Consejo de Europa firmado en noviembre de 2001 en Budapest, con el propósito de brindar orientación a los Estados en relación a las nuevas conductas delictivas que se llevan a cabo en el ciberespacio. El Convenio introduce una clasificación de los delitos informáticos, los cuales se organizan en los siguientes grupos: (Convenio sobre cibercriminalidad, 2001)

1. Un primer grupo engloba los Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, que incluyen:

- Acceso no autorizado a sistemas informáticos.
- Interceptación indebida de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Uso abusivo de dispositivos para facilitar la comisión de delitos.
- Algunos ejemplos dentro de este grupo son el robo de identidad, la conexión a redes no autorizadas y la utilización de spyware y keylogger.

2. Un segundo grupo se centra en los delitos de falsificación informática, que incluyen:

- Manipulación de datos informáticos mediante la introducción, eliminación o supresión de información.
- Fraude informático mediante la alteración, eliminación o manipulación de datos informáticos, o la interferencia en sistemas informáticos.
- Eliminación fraudulenta de datos o corrupción de archivos.

Algunos ejemplos de delitos en esta categoría incluyen la alteración de registros electrónicos,

el fraude en línea y la manipulación de información financiera.

3. En el tercer grupo se encuentran los delitos cuyo enfoque se centra en el contenido y se pueden clasificar de la siguiente manera:

- Producción, oferta, difusión o adquisición de material de pornografía infantil a través de sistemas informáticos, así como la posesión de dicho material en un sistema informático o medio de almacenamiento de datos.
- Delitos relacionados con violaciones de derechos de propiedad intelectual y otros derechos afines.

En Colombia, se aprobó el 5 de enero de 2009 una legislación denominada "Ley de protección de la información y los datos". Esta ley introduce modificaciones al Código Penal y establece un nuevo marco legal con el propósito de sancionar cualquier conducta ilícita relacionada con la comisión de delitos informáticos en el país. Su objetivo primordial es penalizar las acciones punibles que surgen del acceso a una base de datos o plataforma digital, cuando dicho acceso resulta en la violación de derechos fundamentales como la integridad personal, la intimidad o el habeas data.

La promulgación de la Ley 1273 de 2009 marcó un hito significativo en el fortalecimiento del marco jurídico en la lucha contra los delitos informáticos en Colombia. Toda vez que la ley se creó para abordar una nueva forma de delincuencia que había surgido en el país, debido a un vacío normativo en cuanto a la regulación de esta conducta, por lo tanto, era imperativo proporcionar las herramientas necesarias a los jueces y fiscales para hacer frente a estos delitos, así como encontrar una forma más adecuada de tipificarlos, ya que estas conductas tienen impacto más allá de los medios convencionales o tradicionales conocidos. Además, todas estas medidas están vinculadas al bienestar colectivo, porque desde su aparición, la tecnología ha experimentado un gran auge en la vida de las personas.

A pesar de los esfuerzos legislativos, Colombia ha experimentado un crecimiento

exponencial en la incidencia del delito de acceso abusivo a sistemas informáticos desde mediados del 2020 hasta la actualidad, tal como ha sido registrado por la Fiscalía General de la Nación. Esta preocupante tendencia pone de manifiesto la necesidad de adoptar medidas más efectivas para prevenir, investigar y sancionar este tipo de delitos, así como de fortalecer la cooperación nacional e internacional en la lucha contra la ciberdelincuencia.

La Ley 1237 de 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"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"* está disposición legal, se estructura en dos capítulos, el primero de los cuales aborda las medidas para salvaguardar la confidencialidad, integridad y disponibilidad de la información. El segundo capítulo se refiere a otras infracciones y ataques informáticos. La introducción de este marco legal ha llevado a la tipificación de los delitos informáticos en Colombia de la siguiente manera:

- Acceso ilícito a un sistema informático (modificación del Código Penal).
- Obstaculización indebida de sistemas informáticos o redes de telecomunicaciones.
- Intercepción de datos informáticos.
- Daño a sistemas informáticos.
- Uso de software malicioso.
- Hurto mediante medios informáticos y similares.
- Violación de datos personales.
- Suplantación de sitios web para la captura de datos personales.
- Transferencia no autorizada de activos.

La introducción de estos delitos informáticos en la legislación colombiana ha permitido una mayor protección y sanción de conductas ilegales en el ámbito digital, adaptándose a los avances tecnológicos y garantizando la seguridad de la información y los

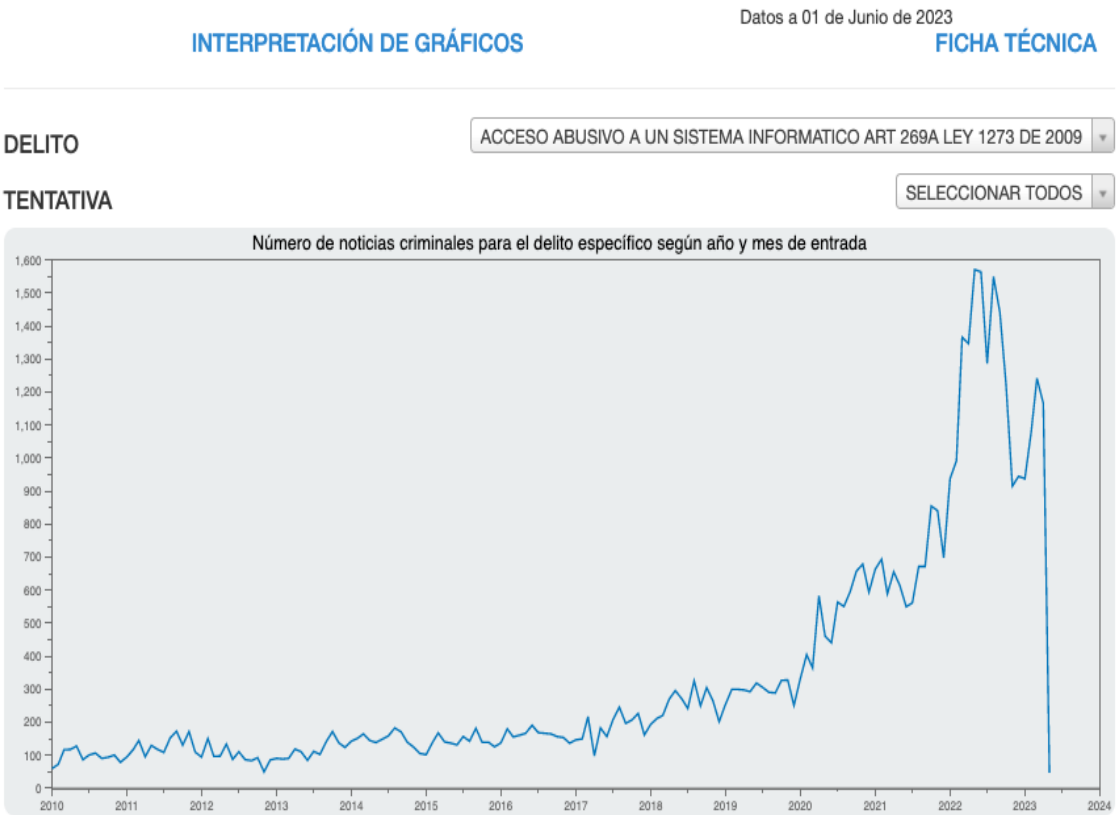
derechos de las personas en el ciberespacio.

En la actualidad el delito de acceso abusivo a sistemas informáticos representa una de las más grandes amenazas en el mundo, ya que el avance tecnológico ha permitido que el ejercicio del delito sea rentable, por este motivo diferentes países a nivel mundial han firmado el Convenio sobre la ciberdelincuencia en Budapest con la finalidad de orientar a los Estados ante las nuevas conductas criminales que se despliegan en el Ciberespacio.

La Ley 1273 del 2009 fue expedida para hacerle frente a la nueva necesidad legal derivada de la cibercriminalidad con el objetivo de sancionar las conductas punibles que originan en acceder a una base de datos o plataforma digital que conduce a la violación del derecho a la integridad, intimidad o Habeas data, no obstante Colombia ha presentado un crecimiento exponencial desde mediados del 2020 hasta la actualidad como lo refleja la Fiscalía General de la Nación.

Gráfico 1.

*Estadística de la Fiscalía General de la Nación del índice de Denuncias por el delito de Acceso Abusivo a un Sistema Informático.*



*Nota: la gráfica muestra la interpretación del número de denuncias realizadas entre el año 2010 y el 1 de junio del 2023 en el Territorio Colombiano.*

La gráfica anterior evidencia un aumento significativo en la cibercriminalidad desde el inicio de la pandemia en 2020, como se refleja en el lado izquierdo de la gráfica, donde se observa el número de denuncias realizadas. Al inicio de 2020, las denuncias oscilaban entre 200 y 300, mientras que hasta el 1 de junio de 2023, se ha registrado un aumento a un rango de 1,100 y 1,200 denuncias. A partir del análisis previo, se puede concluir que el período de confinamiento ha sido un factor determinante en el incremento de denuncias por delitos informáticos.

A la luz de lo expuesto anteriormente, resulta relevante plantear ¿cómo la implementación de la Ley 1273 de 2009 contribuye a la prevención del ciberdelito en el sistema penal colombiano?. En este contexto, es pertinente mencionar las reflexiones del autor Sánchez Castillo (2017), quien destaca que la política criminal de un Estado no debe limitarse únicamente a la imposición de sanciones, sino que también debe incluir medidas de prevención del delito. Estas medidas preventivas se llevan a cabo a través de políticas públicas que buscan generar conciencia en la ciudadanía para evitar convertirse en víctimas de conductas ilícitas. El autor realiza un análisis específico de la Ley 1273 de 2009, la cual contempla los siguientes aspectos:

> La ley colombiana 1273, a pesar de haber sido creada para dar un tratamiento de carácter jurídico frente al flagelo de ciberdelincuencia sufrido actualmente, no es suficiente, ya que desde el año 2013 ha ido creciendo en todo el territorio nacional, por cuanto se debe pensarse en estrategias que fortalezcan el bien jurídico y a su vez integre las medidas que deben adoptarse en cuanto a seguridad informática se refiere,

> con el fin de reducir, prevenir o mitigar el daño causado por esta problemática. (Sánchez Castillo, 2017, p.103)

Aunque la norma está orientada a la sanción penal y se limita al prohibicionismo, es posible implementar políticas públicas en materia de seguridad informática en todo el territorio colombiano brindando capacitaciones a las entidades públicas y privadas en materia de ciberseguridad, en este mismo sentido se puede creer diferentes programas de concientización desde los programas educativos en el cual se exponga los delitos informáticos y cómo prevenir ser víctima de ellos. Es innegable debatir que el constante avance de las tecnologías de la información ha llevado, además de numerosos beneficios para la sociedad, a la proliferación de los delitos informáticos. La delincuencia informática se fundamenta en la comisión de delitos utilizando la tecnología, a través de redes telemáticas y la interconexión de computadoras, aunque no son los únicos medios utilizados.

No obstante, el artículo 269I del código penal colombiano establece disposiciones sobre el delito de *Hurto por medios informáticos y semejantes:*

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

El artículo en cuestión aborda el tema del daño por medios informáticos y situaciones similares. Esta disposición legal tiene como objetivo regular y sancionar los actos de daño realizados a través del uso de medios informáticos, garantizando así la protección de los sistemas informáticos y las redes electrónicas. Además, busca salvaguardar el patrimonio económico de los ciudadanos.

En dicho artículo se establecen las penas para aquellos individuos que, al superar las

medidas de seguridad informática, cometan el delito de daño por medios informáticos y similares. Especifica que aquellos que, mediante la manipulación de procedimientos informáticos, redes de sistemas electrónicos, telemáticos u otros medios similares, o mediante la suplantación de un usuario ante los sistemas de autenticación y autorización establecidos, incurran en la conducta descrita en el artículo 239, serán penalizados de acuerdo con lo estipulado en el artículo 240 de la Ley 599 del 2000, Código Penal Colombiano.

De conformidad, con el acápite anterior es pertinente traer a colación el articulo 14 de la ley 599 del 2000 toda vez que desarrolla la territorialidad como un factor esencial para la imputación de la conducta punible, ya que es el espacio en el cual se ejecuta el delito. En materia de delitos informáticos, donde el lugar de los hechos es el ciberespacio conocido como un espacio intangible por medio del cual se produce las redes de la comunicación como un canal directo para la remisión de datos informáticos que se materializan por medios de equipos, programas y plataformas digitales; la IP también conocido como protocolo de internet es trascendental para la imputación del delito, ya que por medio de esta se conoce la ubicación del equipo utilizado para el despliegue de la conducta ilícita, lo que permite que el sistema penal colombiano pueda sancionar al sujeto por los hechos cometidos en el territorio colombiano pese a no ser un espacio físico sino digital pero objeto de la jurisdicción del estado colombiano.

Para concluir, la Ley 1273 de 2009 en Colombia aborda la prevención de los delitos informáticos y ha sido un hito significativo en la lucha contra esta forma de delincuencia. Se creó para sancionar conductas ilegales relacionadas con el acceso no autorizado a sistemas informáticos y la violación de derechos fundamentales. Esta ley se basa en el "Convenio sobre la ciberdelincuencia" del Consejo de Europa, el cual clasifica los delitos informáticos en grupos.

A pesar de los esfuerzos legislativos, la incidencia de los delitos informáticos ha

aumentado en Colombia. Se requieren medidas más efectivas, como políticas públicas de seguridad informática y programas de concientización, para prevenir y combatir la ciberdelincuencia de manera más efectiva. La ley ha introducido modificaciones al Código Penal y tipifica delitos como el acceso ilícito a sistemas informáticos, el daño a sistemas, la violación de datos personales y la suplantación de identidad en línea. Su implementación ha fortalecido el marco jurídico para proteger los derechos de las personas en el entorno digital.

### 3. Prevención del Ciberdelito en Países como República Dominicana y Panamá.

En el contexto actual, los ciberdelitos representan una preocupación creciente a nivel mundial, lo que ha llevado a cada país a implementar medidas para abordar esta problemática y proteger a sus ciudadanos en el entorno digital. Este capítulo se enfoca en comparar la Ley 1273 de 2009 en Colombia con la regulación legal de los delitos informáticos en países como Panamá y República Dominicana.

La Ley 1273 de 2009 en Colombia es una legislación que regula los delitos informáticos y establece sanciones para estas conductas, reconociendo la importancia de proteger la información y los datos personales como bienes jurídicos tutelados. Sin embargo, es crucial examinar cómo otros países abordan esta problemática.

En el caso de Panamá, el país ha ratificado el Convenio sobre la Ciberdelincuencia adoptado en Budapest en 2001, lo que ha presentado desafíos en términos de implementación y establecimiento de estándares legales claros para la investigación y persecución de los delitos informáticos.

Por otro lado, en República Dominicana, se promulgó la Ley 53-07 sobre Delitos y Crímenes de Alta Tecnología en 2019. No obstante, esta ley ha generado controversia debido a las restricciones que impone a la libertad de expresión, especialmente en relación con la

eliminación de contenido discriminatorio por parte de los proveedores de servicios.

En este capítulo, se analizan las similitudes y diferencias entre estas legislaciones, así como los desafíos que enfrentan en su implementación. Se examinan las sanciones establecidas para los delitos informáticos y se discuten las implicaciones de estas leyes en la protección de los derechos de los ciudadanos y la seguridad en el entorno digital.

Mediante esta comparación, se busca obtener una visión más amplia de cómo diferentes países abordan la regulación del ciberdelito y cómo se pueden aprender de las experiencias de cada uno para fortalecer la protección en el ámbito digital.

Según el estudio de derecho comparado realizado por Mejía, M., Hurtado, S. V., y Grisales, A, titulado "Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo" (2023), la mayoría de los países de la región tienen leyes que regulan los delitos informáticos y establecen sanciones para estas conductas, reconociendo la importancia de proteger la información y los datos personales como bienes jurídicos tutelados. Aunque existen diferencias significativas entre las diferentes legislaciones, todas ellas buscan proteger la seguridad y privacidad de la información en línea y garantizar la responsabilidad penal de aquellos que cometen delitos informáticos.

Es importante destacar que cada país tiene su propia legislación específica y sanciones para los delitos informáticos. En el caso de la República Dominicana, se promulgó la Ley 53-07 sobre Delitos y Crímenes de Alta Tecnología en 2019, que establece sanciones y la creación de una unidad especializada en delitos informáticos, al igual que en Colombia y Panamá.

A pesar de que los tres países reconocen la importancia de proteger la privacidad y seguridad de los datos personales en el entorno digital, cada legislación tiene disposiciones que buscan salvaguardar la información personal de los ciudadanos y establecen regulaciones para su manejo adecuado. En última instancia, este análisis comparativo permitirá identificar

enfoques exitosos y áreas de mejora en la lucha contra los ciberdelitos, promoviendo un mayor fortalecimiento en la protección de la ciberseguridad y los derechos de los usuarios en el contexto global de la era digital.

### *3.1.* Enfoque de cada Legislación.

***Colombia:*** Con la Ley 1273 de 2009 se modifica el Código Penal, y se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

La Ley 1273 define una amplia gama de conductas delictivas relacionadas con sistemas y datos informáticos. Entre los delitos contemplados se incluyen el acceso no autorizado a sistemas, la manipulación de datos, el sabotaje informático, la falsificación informática, el hurto por medios electrónicos, el daño informático y la violación de datos personales, entre otros. Es así como la ley prevé medidas para la protección y seguridad de la información almacenada en sistemas informáticos, tanto en entidades públicas como privadas, estas deben implementar políticas de seguridad informática que establezcan los lineamientos, normas y procedimientos para garantizar la protección de la información almacenada en sistemas informáticos. Estas políticas deben contemplar aspectos como la protección de datos personales, el acceso autorizado a la información, la confidencialidad de los datos y las medidas de prevención de intrusiones y ataques informáticos.

Las entidades deben adoptar medidas técnicas adecuadas para proteger los sistemas informáticos y la información almacenada en ellos. Esto incluye el uso de sistemas de protección contra virus, malware y otras amenazas informáticas, así como la utilización de mecanismos de cifrado y autenticación para asegurar la confidencialidad de los datos. Esto implica tener mecanismos para identificar y reportar cualquier evento que ponga en riesgo la seguridad de la información, así como la implementación de planes de contingencia para

hacer frente a situaciones de emergencia informática.

Las entidades deben mantener registros de las actividades realizadas en sistemas informáticos, así como de las medidas de seguridad implementadas. Esto permite tener un seguimiento de posibles incidentes y facilita las labores de investigación en caso de que se produzcan delitos informáticos

La ley establece la obligación de colaborar con las autoridades competentes en la investigación y persecución de delitos informáticos. Las entidades deben proporcionar la información necesaria para llevar a cabo las diligencias judiciales y facilitar la identificación y captura de los responsables de los delitos.

***República Dominicana:*** La legislación de República Dominicana en materia de ciberdelitos se encuentra en desarrollo, la legislación abarca una amplia gama de conductas delictivas relacionadas con el uso inadecuado de tecnologías de la información y la comunicación. Estos delitos comprenden el acceso no autorizado a sistemas informáticos, la falsificación informática, la distribución de programas maliciosos, el sabotaje informático, el fraude electrónico, entre otros.

Además, la Ley 53-07 establece medidas con el fin de proteger y salvaguardar la información almacenada en sistemas informáticos. Una de estas medidas cruciales es la creación de la Unidad Especializada de Investigación de Delitos Tecnológicos. Esta unidad tiene como propósito investigar y perseguir los delitos de alta tecnología en el país, respondiendo así a la necesidad de contar con un equipo de expertos altamente capacitados en el ámbito de la ciberseguridad y las tecnologías de la información, capaces de enfrentar los desafíos que plantea el crecimiento de la ciberdelincuencia.

La Unidad está integrada por profesionales especializados en delitos informáticos, informática forense, análisis de sistemas y otras áreas afines a la tecnología. Su misión principal es indagar los delitos que involucran el uso de tecnologías de la información y la

comunicación, incluyendo el acceso no autorizado a sistemas, la distribución de programas maliciosos y el fraude electrónico, entre otros.

Por otra parte, la ley establece la responsabilidad de los proveedores de servicios de Internet y telecomunicaciones en colaborar con las autoridades durante la investigación de delitos informáticos. Esta colaboración es fundamental para abordar eficazmente la ciberdelincuencia y garantizar la seguridad y confiabilidad de los servicios de comunicación en línea.

***Panamá:*** Aunque en Panamá no se cuenta con una legislación específica destinada a abordar exclusivamente los delitos informáticos o de alta tecnología, como sí ocurre en otros países como Colombia o República Dominicana, el país dispone de otras leyes y disposiciones legales aplicables a casos relacionados con delitos informáticos, protección de datos y ciberseguridad. Entre las leyes relevantes en este contexto, se destacan las siguientes:

Ley 81 de 2019 de Protección de Datos Personales: Esta legislación regula el tratamiento, uso y salvaguarda de los datos personales en el territorio panameño. En ella se estipulan los derechos y obligaciones de los titulares de datos y de los responsables que manejan esta información. Además, se establecen las medidas de seguridad que deben implementarse para proteger los datos personales frente al acceso no autorizado y la divulgación indebida.

El Código Penal incluye disposiciones que pueden aplicarse a los delitos informáticos, tales como la falsificación informática, el acceso no autorizado a sistemas, el daño a datos informáticos, el sabotaje informático, entre otros. Aunque no existe una sección exclusivamente dedicada a los delitos informáticos, las acciones ilícitas vinculadas con el uso inapropiado de tecnologías de la información pueden ser perseguidas y sancionadas bajo las disposiciones generales de este código.

Ley 82 de 2019 de Delitos Contra el Orden Económico: Esta ley establece el marco

legal para la prevención y represión de delitos económicos, como el fraude, la estafa y otros delitos financieros. En el contexto digital, estas disposiciones pueden aplicarse a delitos económicos cometidos a través de medios electrónicos o informáticos.

Es relevante mencionar que estas tres legislaciones han adoptado las directrices del convenio de cibercriminalidad de Budapest, el cual es un tratado internacional que tiene como objetivo aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional. Algunos de los aspectos más importantes del Convenio son los siguientes:

- **A.** La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectadas al área de los delitos informáticos.
- **B.** El Convenio se complementa con un Protocolo Adicional que realiza cualquier publicación de la propaganda racista y xenófoba a través de redes informáticas como una ofensa criminal.
- **C.** El terrorismo cibernético también se estudia en el marco del Convenio.
- **D.** A principios de 2023, se han adherido y ratificado el Convenio 68 países de diversas partes del mundo.

En conclusión, Colombia, Panamá y República Dominicana han promulgado leyes para abordar los delitos informáticos. Colombia cuenta con una ley específica que tipifica los delitos informáticos y establece sanciones, mientras que Panamá ha ratificado el Convenio de Budapest y enfrenta desafíos en su implementación. Por su parte, la legislación en República Dominicana ha sido objeto de controversia debido a las restricciones a la libertad de expresión. A pesar de las diferencias en la legislación, es importante destacar que estos países están tomando medidas para combatir los delitos informáticos y proteger a la sociedad frente a estos delitos. Es necesario seguir trabajando en la armonización de las leyes nacionales y la

cooperación internacional en la lucha contra los delitos informáticos, y el convenio de ciberdelincuencia es una guía importante para lograr este objetivo.

## CONCLUSIÓN

En la era moderna, el surgimiento y la expansión de los ciberdelitos han llevado a una transformación sin precedentes del sistema penal en todo el mundo. Estos delitos informáticos, que abarcan desde el robo de información hasta el ciberacoso y el sabotaje cibernético, han evolucionado rápidamente en paralelo con los avances tecnológicos y la creciente conectividad digital. Esta revolución tecnológica ha planteado desafíos significativos para el sistema penal tradicional, que se ha visto obligado a adaptarse para enfrentar las complejas amenazas que emergen en el ciberespacio.

La naturaleza transnacional de los ciberdelitos ha generado problemas en términos de jurisdicción y cooperación entre países. Los delincuentes digitales pueden operar desde cualquier lugar del mundo, utilizando técnicas de ocultación y anonimato para eludir la identificación y persecución por parte de las autoridades tradicionales. Como resultado, la colaboración internacional se ha convertido en un elemento fundamental para enfrentar estos desafíos, exigiendo la adopción de acuerdos y convenciones internacionales para combatir los ciberdelitos de manera efectiva.

Las sanciones han sido uno de los pilares clave para abordar los ciberdelitos y ha llevado al desarrollo de leyes específicas que regulan estas conductas en muchos países. Estas normas buscan establecer un marco legal claro para investigar, procesar y sancionar a los delincuentes informáticos, así como proteger los derechos de las víctimas y la seguridad en línea de los ciudadanos. La protección de la información y los datos personales se ha convertido en un bien jurídico tutelado en numerosas jurisdicciones, reflejando la importancia de salvaguardar la privacidad y la integridad digital.

No obstante, la implementación efectiva de estas leyes y la lucha contra los

ciberdelitos han enfrentado obstáculos significativos. La naturaleza dinámica y evolutiva de la tecnología digital ha dificultado la adecuación de las regulaciones a los nuevos desafíos y tácticas utilizadas por los delincuentes informáticos. Además, la falta de conocimientos especializados en ciberseguridad y recursos tecnológicos adecuados en las fuerzas policiales y el sistema judicial ha planteado desafíos adicionales para la investigación y persecución de los ciberdelitos.

En este contexto, la educación y la sensibilización se han vuelto fundamentales para prevenir los ciberdelitos y mejorar la seguridad en línea. La concienciación sobre las amenazas cibernéticas y la promoción de las mejores prácticas de ciberseguridad son aspectos cruciales para empoderar a los usuarios y empresas en el entorno digital.

El análisis comparativo entre diferentes legislaciones y enfoques adoptados por distintos países ha brindado la oportunidad de identificar enfoques exitosos y áreas de mejora en la lucha contra los ciberdelitos. Esta comparación ha permitido entender cómo diversos sistemas penales abordan los delitos informáticos y cómo se pueden aprender de las experiencias de cada uno para fortalecer la protección en el ámbito digital.

En última instancia, la lucha contra los ciberdelitos es un desafío en constante evolución que requiere un enfoque multidisciplinario y colaborativo. La cooperación entre países, la implementación de regulaciones efectivas, el fortalecimiento de capacidades tecnológicas y la concienciación pública son pilares clave para enfrentar este fenómeno transformador del sistema penal. Sólo mediante esfuerzos conjuntos y una voluntad colectiva de adaptarse al cambiante panorama digital, se podrán proteger los derechos y la seguridad de las personas en la era de la tecnología y la interconexión global.

**REFERENCIAS BIBLIOGRÁFICAS**

Arzuaga, T., Guevara, L. (2013). "La Ley 1273 de 2009 y los delitos informáticos". Biblioteca Digital USB. Recuperado de: https://bibliotecadigital.usb.edu.co/server/api/core/bitstreams/a8221e41-9ade-468d-953d-6b74e3346e52/content

Constitución Política de Colombia [C.P.]. (1991). (2.ª ed.). Legis

Congreso de la República de Colombia. (24 de Julio de 2000). Código Penal [Ley 599 de 2000]. DO: 44.097

Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia. Recuperado el 11 de julio de 2023 de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

Congreso de la República de Colombia. (5 de enero de 2009). Se modifica el código penal y se crea el bien jurídico tutelable de la protección de la información y de los datos [ Ley 1273 del 2009] DO: 47.223.

Corte Constitucional, Sala Plena de la Corte ( 22 de mayo del 2019). Sentencia C-224 del 2019 [M.P: Pardo Schlesinger, C.]

Corte Constitucional , Sala Plena de la Corte. (12 de septiembre de 2019). Sentencia SU-420 del 2019. [M.P: Reyes Cuartas, J.F.].

Corte Constitucional. (2019, 22 de mayo) Sentencia C-224/19. (Cristina Pardo, M.P). Recuperado de: https://www.corteconstitucional.gov.co/relatoria/2019/C-224-19.htm

Cadena, A. (2021). Crecimiento del ciber fraude en Colombia durante la

pandemia por COVID-19. Recuperado de: https://repository.unimilitar.edu.co/bitstream/handle/10654/38839/CadenaAlvaradoAnaMaria2021.pdf?sequence=1&isAllowed=y#:~:text=Se%20lleg%C3%B3%20a%20la%20conclusi%C3%B3n,para%20el%202019%20y%202020.

Centro criptológico Nacional. (2022). Ciberamenazas y Tendencias: Análisis de las ciberamenazas nacionales e internacionales de su evolución y tendencias futuras (edición 2022). Ministerio de Defensa. Gobierno de España. Recuperado de: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6786-ccn-cert-ia-24-22-

Corte Suprema de Justicia, Sala de Casación Penal. ( 2 de marzo del 2022). Sentencia SP592 [M.P: Corredor, Beltrán, D.E.]. Recuperado de: https://www.fiscalia.gov.co/colombia/gestion/estadisticas/delitos/ (tabla del delito acceso abusivo a un sistema de información)

División Cero. (2021). Ley 1273 de 2009 - Coloquialmente conocida como Ley de Delitos Informáticos. Recuperado de: https://www.divisioncero.com/tutoriales/ley_1273_de_2009_delitos_informaticos/

Universidad de Panamá Centro Regional Universitario de Panamá Oeste. (2021). “Delitos Cibernéticos”. Recuperado de: https://www.studocu.com/latam/document/universidad-de-panama/derecho-penal/delitos-ciberneticos-up/28427235

Guerrero, J. (2020). "La práctica de los delitos informáticos en Colombia". Universidad Militar Nueva Granada. Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/31941/jaguerreroga.pdf?sequence=1&isAllowed=y

Guerrero Martínez, R. (10 de marzo del 2020). Derechos humanos de cuarta

generación y las tecnologías de la información y de la comunicación [Derechos Fundamentales a Debate]. Comisión Estatal de Derechos Humanos Jalisco, Jalisco, México. Recuperado de: http://cedhj.org.mx/revista%20DF%20Debate/articulos/revista_No12/ADEBATE-12-art8.pdf

Gamba Velandia, J. A. (2020). El delito informático en el marco jurídico colombiano y el derecho comparado: caso de la transferencia no consentida de activos . Universidad Externado de Colombia.

La Estrella de Panamá. (2014, May 25). ¿Cómo se penalizan los delitos cibernéticos?. Recuperado de https://www.laestrella.com.pa/internacional/mundo/140525/delitos-penalizan-ciberneticos

Marin, J et al. (2019). Modelo Ontológico de los Ciberdelitos: Caso de estudio Colombia. Revista Ibérica de Sistemas y Tecnologías de información; Lousada No E17.244- 257. Recuperado de: https://www.proquest.com/openview/ef48269d2b309b4657581d7bc7b8172a/1?pq-origsite=gscholar&cbl=1006393

Mosquera, A., Ledezma, E., & Bechara, Y. (2020). "Análisis jurídico de la ley 1273 del 2009 y el surgimiento y expansión del delito de hurto". Universidad Cooperativa de Colombia. Recuperado de: https://repository.ucc.edu.co/items/cc5f260c-7626-4b26-bf80-5412894f6ae0

Martins dos Santos, B. (2022, May 16). Convenio de Budapest sobre la Ciberdelincuencia en América Latina. Derechos Digitales. Recuperado de: https://www.derechosdigitales.org/18451/convenio-de-budapest-sobre-la-ciberdelincuencia-en-america-latina/

Mejía-Lobo, M., Hurtado-Gil, S. V., y Grisales Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. Revista De Ciencias Sociales, XXIX(2), 356-372.

Ojeda, J., Rincón, F. Arias, M.; Daza, L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11 (28), 41-66

Parada, R. A., & Errecaborde, J. D. (2018). Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet . Pensamiento Penal. Recuperado de: https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Riofrío Martínez-Villalba, J. (2014). LA CUARTA OLA DE DERECHOS HUMANOS: LOS DERECHOS DIGITALES. Revista Latinoamericana De Derechos Humanos, 25(1), 15-45. Recuperado de: https://www.revistas.una.ac.cr/index.php/derechoshumanos/article/view/6117

Rodríguez C., O. E, et al. (2022). Percepción de la ciberseguridad: : ciberdelitos, normas legales y políticas de seguridad. Visión Antataura, 6(2), 103–122. Recuperado de: https://revistas.up.ac.pa/index.php/antataura/article/view/3387

Sánchez, Z. (2017). "Análisis de la Ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia". Universidad Nacional Abierta y a Distancia. Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1&isAllowed=y

Sánchez Quintero, C. (2021). Redes Sociales y gestión de crisis, en entorno de ciberseguridad y ciberdefensa. Revista Científica. V No.(5), 47-55. https://revista.insude.mil.do/index.php/rscd/article/view/61

Temperini, M. G. I. (2014). Delitos Informáticos en Latinoamérica: Un

estudio de derecho comparado. 1ra. Parte. Recuperado de: http://sedici.unlp.edu.ar/handle/10915/42145

Villavicencio Terreros, F. (2014). Delitos Informáticos. IUS ET VERITAS, 24(49), 284- 304. Recuperado de: https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Vega Aguilar, J. A., & Arévalo Minchola, M. (2022). Ciberdelitos, Análisis en el sistema penal. Iustitia.