Maestría en Derecho procesal penal y teoría del delito
Informe final de investigación

Aproximación Al Bien Jurídico Protegido En Los Delitos Informáticos

Approximation To The Legal Asset Protected in Computer Crimes

La nueva era del ciberdelito: Un análisis a partir del derecho a la privacidad en el ciberespacio.[1]

The new era of cybercrime: An analysis based on the right to privacy in cyberspace.

Arles Corrales Rúa[2]

Resumen

En la actual era digital, el ciberdelito representa una amenaza multifacética y en evolución, desafiando los marcos legales y éticos establecidos. La creciente incidencia de delitos como el ransomware y el phishing subraya la necesidad urgente de proteger la privacidad en el ciberespacio, evidenciando cómo estos crímenes afectan tanto a individuos como a organizaciones. La aplicación efectiva de la ley se ve obstaculizada por la rapidez de la innovación tecnológica y la transnacionalidad del ciberespacio. Examinar los enfoques de Europa y Colombia hacia la protección de datos personales proporciona insights valiosos sobre cómo enfrentar estos retos. Un buen gobierno es crucial para una respuesta efectiva, demandando leyes adecuadas, concienciación en ciberseguridad y colaboración internacional. Este análisis resalta la importancia de un enfoque integrado y colaborativo para asegurar la privacidad y fomentar un entorno digital seguro.

Palabras clave: Era corrales4743, Ciberseguridad, Ciberdelitos, Gobernanza, privacidad.

[1] Arles Corrales Rúa

[2] Estudiante 4 semestre Maestría en Procesal Penal y Teoría del Delito Universidad Autónoma Latinoamericana, arles.corrales4743@unaula.edu.co

Abstract

In today's digital age, cybercrime represents a multifaceted and evolving threat, challenging established legal and ethical frameworks. The growing incidence of crimes such as ransomware and phishing underscores the urgent need to protect privacy in cyberspace, highlighting how these crimes affect both individuals and organizations. Effective law enforcement is hampered by the speed of technological innovation and the transnationality of cyberspace. Examining the European and Colombian approaches to personal data protection provides valuable insights on how to address these challenges. Good governance is crucial for an effective response, demanding adequate laws, cybersecurity awareness and international collaboration. This analysis highlights the importance of an integrated and collaborative approach to ensuring privacy and fostering a secure digital environment.

Key words: Digital era, Cybersecurity, Cybercrime, Governance, privacy.

Tabla de contenido

Maestría en Derecho procesal penal y teoría del delito
Informe final de investigación

La nueva era del ciberdelito: El bien jurídico desde el derecho a la privacidad en el ciberespacio.

Introducción

En la era digital actual, el ciberdelito emerge como una de las amenazas más complejas y de rápida evolución, desafiando los marcos legales, las políticas de seguridad y los principios éticos que rigen nuestras sociedades. Este escenario en constante cambio ha impulsado la necesidad de una comprensión profunda y actualizada de las vulnerabilidades en el ciberespacio, especialmente en relación con el derecho a la privacidad. La metodología cualitativa adoptada en este análisis, con un enfoque analítico-descriptivo, permite una exploración detallada de los diversos aspectos y dimensiones del ciberdelito, subrayando las implicaciones para la privacidad individual y colectiva en el entorno digital.

El ciberespacio, un dominio vasto y sin fronteras, es un terreno fértil para diversas formas de delincuencia que explotan las vulnerabilidades tanto tecnológicas como humanas. La violación de datos personales se ha convertido en una preocupación central, con incidentes que van desde el robo de identidad hasta el acceso y divulgación no autorizados de información confidencial. En este contexto, fenómenos como el ransomware y el phishing representan riesgos significativos, no solo por el daño económico que pueden causar sino también por su impacto en la confianza y la seguridad en el ámbito digital.

El ransomware, que secuestra información vital exigiendo un rescate para su liberación, y el phishing, que engaña a los usuarios para que divulguen datos sensibles, son manifestaciones claras de cómo la ciberdelincuencia ha evolucionado hacia métodos cada vez más sofisticados y dirigidos (Li, 2021). Estos delitos no solo vulneran la privacidad y la seguridad de los individuos, sino que

también plantean desafíos críticos para las organizaciones y los gobiernos, que deben proteger la integridad de sus sistemas de información y la confidencialidad de los datos que gestionan.

La aplicación efectiva de la ley en este dominio es, por tanto, un desafío formidable. Los marcos legales existentes a menudo luchan por mantenerse al día con la velocidad de la innovación tecnológica y la naturaleza transnacional del ciberespacio (Meištė, Jakštienė, & Lankauskienė, 2023). El análisis de casos específicos, como el enfoque europeo en la protección de datos personales y la experiencia de Colombia en la misma área, ofrece perspectivas valiosas respecto a cómo diferentes jurisdicciones están respondiendo estos desafíos.

Siendo, el papel del buen gobierno es fundamental en la configuración de una respuesta efectiva y equilibrada a los ciberdelitos. Esto implica no solo la creación y aplicación de leyes y regulaciones adecuadas sino también la promoción de la conciencia y la educación en ciberseguridad, la cooperación entre diferentes actores a nivel nacional e internacional, y la garantía de que se respeten los derechos y libertades fundamentales en el proceso.

El presente artículo tiene como objetivo analizar la evolución y el impacto del ciberdelito en la era digital y cómo afecta el derecho a la privacidad en el ciberespac, para llevarlo a cabo se evaluará la legislación vigente en materia de ciberdelito y derecho a la privacidad, identificando lagunas y áreas de mejora para la protección de datos personales en el ciberespacio y se indagarán sobre las modalidades más comunes de ciberdelito que afectan la privacidad de los usuarios, analizando casos específicos y sus consecuencias para proponer medidas preventivas y de respuesta efectivas; lo anterior ha sido desarrollado bajo una metodología cualitativa, que revela la complejidad del ciberdelito en la era actual y subraya la importancia crítica de abordar estas cuestiones desde múltiples perspectivas, integrando consideraciones legales, técnicas, éticas y políticas. Cuya construcción es la siguiente: I) Vulnerabilidad en el ciberespacio. II) Desafíos en la aplicación de la ley. III) El buen gobierno y su papel en la acción y prevención de la administración de justicia. A partir de esos

elementos se pretende visibilizar el enfoque holístico y colaborativo respecto al derecho a la privacidad en el ciberespacio y avanzar hacia un entorno digital más seguro y justo para todos.

1. Vulnerabilidades en el ciberespacio: Un enfoque a partir del Derecho a la privacidad.

En el vasto y dinámico entorno del ciberespacio, la privacidad emerge como un derecho fundamental constantemente amenazado por una gama diversa de vulnerabilidades, por lo que estas brechas no solo comprometen la integridad de la información personal y corporativa, sino que también desafían los principios básicos de la libertad y la autonomía en la era digital. El análisis de estas vulnerabilidades desde la perspectiva del derecho a la privacidad revela tanto la magnitud de los retos como los caminos hacia posibles soluciones.

Es por ello, la digitalización masiva de la información y la omnipresencia de internet han facilitado sin duda el acceso y la difusión del conocimiento, pero también han expuesto datos personales a riesgos sin precedentes. Las vulnerabilidades en el ciberespacio, desde fallos de software hasta esquemas de ingeniería social, ofrecen a los actores maliciosos múltiples vías para invadir la privacidad individual y corporativa (Fuentes, 2022). Estas vulnerabilidades no reconocen fronteras y pueden ser explotadas desde cualquier rincón del mundo, lo que complica aún más su detección y mitigación.

En este sentido, la protección del derecho a la privacidad en el ciberespacio requiere un enfoque multidimensional que abarque tanto medidas técnicas como legales; entonces, en el plano técnico, la implementación de protocolos de seguridad robustos y el cifrado de datos son esenciales para salvaguardar la información contra accesos no autorizados (Silva, 2020). Sin embargo, la dimensión técnica por sí sola es insuficiente si no se acompaña de un marco legal sólido que defina claramente los derechos y las responsabilidades en el ámbito digital (Toscano, 2017).

Por otro lado, la legislación en materia de ciberseguridad y privacidad debe evolucionar para mantenerse a la par con las cambiantes tácticas de los ciberdelincuentes[3]. Esto implica no solo la creación de leyes que penalizan eficazmente el acceso ilegítimo y la explotación de datos personales sino también el establecimiento de normativas que obliguen a las empresas a adoptar medidas de seguridad adecuadas (Crespo, et al, 2022). La transparencia en el tratamiento de datos y el consentimiento informado se erigen como pilares fundamentales en la protección de la privacidad.

Asimismo, el papel de las autoridades reguladoras es crucial en la supervisión y el cumplimiento de estas normativas. Sin embargo, la jurisdicción limitada y la naturaleza global del ciberespacio plantean desafíos significativos para la aplicación de la ley. La cooperación internacional se convierte, por lo tanto, en un componente indispensable en la lucha contra las vulnerabilidades que amenazan la privacidad online (Red Iberoamericana de Protección de Datos, 2017).

Por otra parte, la concienciación y la educación desempeñan un rol vital en la prevención de violaciones a la privacidad ya que, los usuarios del ciberespacio deben estar informados sobre los riesgos asociados a su actividad en línea y sobre las mejores prácticas para proteger su información personal. Esto incluye desde la gestión prudente de las contraseñas hasta el reconocimiento de tácticas de engaño como el phishing (Hernández, 2022).

Así que, las empresas, por su parte, deben asumir la responsabilidad de proteger los datos de sus clientes y empleados, implementando políticas de seguridad de la información y promoviendo una cultura organizacional que priorice la privacidad. La adopción de normas internacionales como

[3] Cabe destacar que, si bien es cierto para cualquier disciplina del conocimiento se hace utópico estar a la vanguardia frente a diferentes eventos o situaciones; en el caso del derecho se puede hacer mucho más complejo a causa de los diferentes avances que se dan en demás áreas del conocimiento y prever todos estos eventos no hace parte de la visión holística del ser humano; no obstante a ello, el derecho si podrá prevenir la necesidad de brindar cobertura integral frente a derechos vitalicios que pese a los diferentes avances o desarrollos tecnológicos (como es el caso) no puedan ser perturbados, como bien lo es el Derecho a la privacidad.

el ISO/IEC 27001 puede proporcionar un marco de referencia para la gestión eficaz de la seguridad de la información (Consejo Nacional de Política económica y social, 2019).

En última instancia, la protección de la privacidad en el ciberespacio es una responsabilidad compartida que involucra a individuos, empresas y gobiernos. La creación de un entorno digital seguro y respetuoso de la privacidad requiere un compromiso colectivo y acciones coordinadas. Mientras el ciberespacio sigue evolucionando, la vigilancia constante y la adaptación proactiva son esenciales para salvaguardar el derecho a la privacidad en esta nueva era digital.

1.1 Violación de datos personales en el ciberespacio.

En un primer momento, la violación de datos personales en el ciberespacio se ha convertido en una preocupación creciente en la sociedad digital actual, por ende, a medida que la tecnología avanza y se integra más profundamente en nuestra vida cotidiana, la cantidad de información personal almacenada y compartida en línea continúa expandiéndose (Estrella y Martínez, 2022). Esta tendencia ha sido acompañada por un aumento en los incidentes de violaciones de datos, donde la información personal es expuesta, robada o utilizada de manera indebida, planteando serios riesgos para la privacidad y la seguridad de los individuos afectados.

Por su parte, las violaciones de datos pueden ocurrir de diversas maneras, incluyendo ataques cibernéticos a empresas que almacenan grandes volúmenes de información personal, fallos de seguridad en el software (Muñoz, barroso y García, 2022), o incluso a través de tácticas de ingeniería social que engañan a los individuos para que revelen su propia información. Independientemente del método, el resultado es a menudo el mismo: los datos personales caen en manos equivocadas, lo que puede tener consecuencias devastadoras para las víctimas, desde el fraude financiero hasta el robo de identidad (Avdreev, et al, 2021).

Bajo este contexto, la magnitud y frecuencia de estas violaciones subrayan la vulnerabilidad inherente de la información personal en el ciberespacio. A pesar de los esfuerzos continuos para

mejorar la seguridad de la información, los ciberdelincuentes constantemente encuentran nuevas formas de explotar las debilidades en los sistemas de seguridad (Añasco, Morocho, & Hallo, 2023). Esto no solo refleja la naturaleza siempre cambiante de la tecnología y la ciberseguridad, sino también la importancia crítica de mantenerse vigilantes y actualizados con las mejores prácticas de protección de datos (Akbari, et al, 2024).

Entonces, la responsabilidad de proteger los datos personales no recae únicamente en los individuos, sino también en las organizaciones que los recopilan y almacenan; debido a que las leyes y regulaciones, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea (Consejo de la Unión Europea, 2013), han sido implementadas para obligar a las empresas a adoptar medidas de seguridad más estrictas y a ser más transparentes sobre cómo se utiliza y se protege la información personal. Sin embargo, la implementación efectiva de estas regulaciones sigue siendo un desafío, dado el entorno digital global y descentralizado (Chib, Bentley, & Wardoyo, 2019).

Por otra parte, la prevención de violaciones de datos requiere un enfoque multifacético que incluye tanto tecnología de punta en ciberseguridad como una cultura de concienciación sobre la seguridad de la información (Solé, 2023). Las medidas tecnológicas, como el cifrado de datos y la autenticación de dos factores, pueden ofrecer capas significativas de protección. Paralelamente, la educación y capacitación de los usuarios y empleados sobre los riesgos de seguridad y las mejores prácticas pueden reducir significativamente la probabilidad de violaciones resultantes de errores humanos o engaños (Chib, Bentley, & Wardoyo, 2019).

A largo plazo, la lucha contra las violaciones de datos personales en el ciberespacio dependerá de la colaboración internacional entre gobiernos, empresas y la sociedad civil; dado que los actores maliciosos a menudo operan a través de fronteras nacionales, es crucial una cooperación efectiva para perseguir y sancionar a los responsables de estas violaciones (Kwon, y otros, 2023).

Asimismo, el desarrollo de normas y tecnologías globales para la protección de datos personales será esencial para crear un entorno digital más seguro y resiliente.

En conclusión, las violaciones de datos personales representan uno de los desafíos más significativos para la privacidad y la seguridad en el ciberespacio. Aunque es poco probable que el riesgo de tales violaciones se elimine por completo, mediante la adopción de medidas de seguridad robustas, la promoción de la concienciación sobre la seguridad de la información y la cooperación internacional, se pueden mitigar los daños y proteger mejor la privacidad de los individuos en la era digital.

1.1.1 Ransomware y Extorsión

El fenómeno del ransomware y la extorsión representa una de las amenazas más insidiosas y de rápido crecimiento en el panorama actual de los ciberdelitos ya que, este tipo de software malicioso, que secuestra datos críticos o sistemas enteros y exige un pago por su liberación, ha evolucionado para convertirse en una herramienta predilecta entre los ciberdelincuentes, afectando a individuos, empresas y gobiernos a nivel global (Alegre Rodríguez & Padilla López, 2023).

El modus operandi del ransomware es alarmantemente simple pero efectivo: una vez que infecta un sistema, cifra archivos, bases de datos o incluso sistemas operativos completos, haciendo que sean inaccesibles para el usuario o la organización (Rachel, 2021). A continuación, los atacantes demandan un rescate, generalmente en criptomonedas para mantener el anonimato, a cambio de la clave de descifrado. La víctima se enfrenta entonces a un dilema crítico: perder sus datos de forma permanente o ceder ante las demandas de los criminales, sin garantía alguna de recuperar el acceso a sus archivos (Consejo de Europa, 2021).[4]

[4] El modus operandi del ransomware es alarmantemente simple pero efectivo: una vez que infecta un sistema, cifra archivos, bases de datos o incluso sistemas operativos completos, haciendo que sean inaccesibles para el usuario o la organización. A continuación, los atacantes demandan un rescate, generalmente en criptomonedas para mantener el anonimato, a cambio de la clave de descifrado. La víctima se enfrenta entonces a un dilema

Este tipo de ciberdelito tiene un impacto devastador a varios niveles. En primer lugar, está el daño económico directo: el costo del rescate, que puede alcanzar sumas exorbitantes, y las pérdidas asociadas al tiempo de inactividad, la interrupción del negocio y la recuperación del sistema (Roztocki, Soja, & Roland Weistroffer, 2019). Pero más allá de lo financiero, el ransomware puede tener graves consecuencias sobre la privacidad y la seguridad de los datos sensibles, comprometiendo información personal, financiera o confidencial, lo que puede tener repercusiones a largo plazo (Avdreev, et al, 2021).

Además, el pago del rescate plantea un dilema ético y estratégico. Aunque puede parecer la única opción viable para recuperar los datos, financiar a los ciberdelincuentes solo perpetúa el ciclo de ataques, proporcionándoles los recursos para perfeccionar sus métodos y perpetrar más incursiones (Comisión de Asuntos jurídicos, 2017). Esto ha llevado a un intenso debate sobre si las víctimas deben o no cumplir con las demandas de los extorsionadores.

Desde la perspectiva de la prevención y respuesta, la lucha contra el ransomware exige un enfoque holístico y multinivel. En el ámbito técnico, es crucial implementar medidas de seguridad robustas, como copias de seguridad regulares, actualizaciones de software, segmentación de redes y formación en concienciación sobre ciberseguridad para los usuarios (Pirni, Giampellegrini, & Raffini, 2019). Las estrategias de respuesta ante incidentes también son fundamentales, proporcionando a las organizaciones un plan claro para actuar rápidamente y mitigar los daños en caso de un ataque.

En ese sentido, el ransomware y la extorsión en el contexto de los ciberdelitos constituyen una amenaza compleja y en evolución que requiere una respuesta coordinada y multidisciplinaria (Roztocki, Soja y Rolland, 2019). A través de la prevención efectiva, la preparación para incidentes y la colaboración internacional, es posible construir una defensa más sólida contra esta forma de

---

crítico: perder sus datos de forma permanente o ceder ante las demandas de los criminales, sin garantía alguna de recuperar el acceso a sus archivos.

ciberdelincuencia y proteger los activos digitales críticos en nuestra sociedad interconectada (Fuente, 2022).

1.1.2 Phishing y Engaños

El phishing y los engaños en el ámbito digital son técnicas cada vez más sofisticadas utilizadas por los ciberdelincuentes para obtener información confidencial de manera fraudulenta. Estos métodos se basan en la manipulación psicológica y la ingeniería social, apuntando a la confianza y a veces al descuido o la ignorancia de los usuarios para engañarlos y hacer que divulguen datos personales, credenciales de acceso o información financiera (Akbari, et al, 2024).

El phishing, en particular, es una forma de engaño que implica el envío de comunicaciones aparentemente legítimas, pero falsas, que buscan persuadir a la víctima para que realice ciertas acciones. Esto puede incluir hacer clic en un enlace malicioso, descargar un archivo adjunto infectado o ingresar información sensible en un sitio web fraudulento que imita a uno legítimo (Van Dijk & Van Deursen , 2014). Los ataques de phishing pueden dirigirse a un amplio espectro de individuos a través de correos electrónicos masivos o pueden ser altamente personalizados, dirigidos a individuos específicos o empresas, en lo que se conoce como "spear phishing".[5]

En este contexto, los engaños en el ciberespacio no se limitan al phishing. Existen múltiples variantes, como el vishing (phishing a través de llamadas telefónicas) y el smishing (phishing mediante mensajes SMS), que utilizan diferentes medios para alcanzar el mismo fin: la extracción indebida de información personal (Pinto, et al, 2018). Los atacantes adaptan constantemente sus

[5] Cabe destacar que, este tipo de ataques en su forma masiva, estos ataques se lanzan a un gran número de destinatarios con la esperanza de que una pequeña fracción responda, mientras que el spear phishing representa una táctica más insidiosa y calculada, donde los ciberdelincuentes invierten tiempo y recursos en investigar y personalizar sus mensajes para engañar específicamente a individuos o entidades, aumentando significativamente las probabilidades de éxito. Esta segmentación precisa refleja un profundo entendimiento de las dinámicas humanas y organizacionales, explotando la confianza y los patrones de comunicación para infiltrarse eficazmente en los sistemas y obtener información valiosa o acceso no autorizado.

estrategias para explotar las últimas tendencias tecnológicas y los eventos actuales, lo que aumenta la probabilidad de engañar a sus objetivos.

Entonces, la efectividad del phishing y otros engaños radica en su capacidad para generar un sentido de urgencia o miedo, presionando a las víctimas para que actúen rápidamente y sin cuestionar la legitimidad de la solicitud (Ayuso García & Ayuso Sánchez, 2010). Por ejemplo, un ataque de phishing puede simular una alerta de seguridad crítica o una notificación de acceso no autorizado a una cuenta, instando al usuario a "confirmar" su identidad o "verificar" su información de inmediato (Akobari, et al, 2024).

Así que, combatir el phishing y los engaños requiere una combinación de medidas técnicas, educativas y de políticas. A nivel individual, es crucial desarrollar una mentalidad crítica y verificar siempre la autenticidad de las comunicaciones recibidas, especialmente si solicitan información sensible (Añasco, Morocho, & Hallo, 2023). Las herramientas tecnológicas, como los filtros de correo electrónico y los programas de seguridad, también juegan un papel importante en la detección y bloqueo de intentos de phishing.

Las organizaciones, por su parte, deben implementar políticas de seguridad de la información y programas de capacitación para educar a sus empleados sobre los riesgos del phishing y cómo evitarlos. La simulación de ataques de phishing y otros ejercicios prácticos pueden ser especialmente efectivos para preparar al personal y mejorar su capacidad para reconocer y responder adecuadamente a estos engaños (Miquel y Aced, 2018).

Es menester destacar que, a pesar de que las tácticas y herramientas utilizadas por los ciberdelincuentes continúan evolucionando, una combinación de vigilancia, educación y medidas de seguridad adecuadas puede ayudar a mitigar estos riesgos y proteger la privacidad y los activos digitales de individuos y organizaciones.

1.2 Los ciberdelincuentes en la vulneración de datos en el ciberespacio: Un enfoque desde el derecho penal.

La vulneración de datos en el ciberespacio es uno de los problemas más graves que enfrentan las sociedades modernas en la era digital. Los ciberdelincuentes, utilizando una variedad de técnicas y herramientas sofisticadas, explotan las vulnerabilidades en los sistemas informáticos para acceder, robar o manipular información sensible. Desde el enfoque del derecho penal, estas actividades no solo constituyen una amenaza significativa para la privacidad y la seguridad, sino que también desafían los marcos legales tradicionales que deben adaptarse para abordar estos nuevos tipos de delitos.

Los ciberdelincuentes emplean múltiples métodos para vulnerar los datos en el ciberespacio, incluyendo ataques de phishing, malware, ransomware y hacking. Cada uno de estos métodos puede tener consecuencias devastadoras para las víctimas, ya sean individuos, empresas o instituciones gubernamentales. El derecho penal tiene la tarea de definir y sancionar estas conductas delictivas, asegurando que los responsables enfrenten las consecuencias legales correspondientes y acordes al marco legal aplicable dentro de su jurisdicción (Cardona, et al, 2022).

El phishing es una técnica común utilizada por los ciberdelincuentes para engañar a las personas y obtener información confidencial, como contraseñas y detalles financieros. Este método implica el envío de correos electrónicos o mensajes que parecen legítimos pero que en realidad son fraudulentos (Hamdi, et al, 2021). Desde el punto de vista del derecho penal, el phishing se considera una forma de fraude electrónico, y las legislaciones de muchos países han tipificado este delito, imponiendo severas penas a quienes lo cometen.

Autores como (Morelo, Lázaro y GIsbert, 2023), indican que el malware, otro método utilizado por los ciberdelincuentes, incluye software malicioso diseñado para infiltrarse y dañar los sistemas informáticos. Tipos específicos de malware, como el ransomware, secuestran los datos de la

víctima y exigen un rescate para liberarlos. El derecho penal aborda, tanto el uso, como la distribución de malware bajo delitos como el acceso no autorizado a sistemas informáticos y la extorsión, en ese orden de ideas, las penas pueden incluir prisión y multas significativas, reflejando la gravedad de estos actos (Miquel y Aced, 2018).

El hacking, que implica la penetración no autorizada de sistemas informáticos, es otro delito clave en el ciberespacio; lo cual implica que, los hackers pueden robar datos, alterar información o causar daños a infraestructuras críticas (Añasco, Morocho, & Hallo, 2023). Autores como (Caterini & Castellano, 2022), dan a entender que las leyes penales en muchas jurisdicciones han evolucionado para incluir el hacking como un delito específico, con sanciones que varían según la gravedad del acto y el daño causado. La dificultad de rastrear y capturar a los hackers debido a la naturaleza transnacional de Internet añade una capa de complejidad a la persecución penal de estos delitos (Agustina, 2021).

La protección de datos en el ciberespacio también implica la cooperación internacional, ya que los ciberdelincuentes a menudo operan a través de fronteras (Añasco, Morocho, & Hallo, 2023). Tratados y acuerdos internacionales, como la Convención de Budapest sobre el Cibercrimen, buscan armonizar las leyes penales y facilitar la colaboración entre países en la lucha contra el cibercrimen (Fuentes Benítez, 2022). Así las cosas, esta cooperación es esencial para asegurar que los ciberdelincuentes no encuentren refugio en jurisdicciones con leyes más laxas, ello, en vista de la falta de jurisdicción, así como de competencia por parte de autoridades nacionales.

La aplicación del derecho penal en el contexto de la vulneración de datos también enfrenta desafíos relacionados con la evidencia digital. Por lo que, la recopilación, preservación y presentación de pruebas digitales en los tribunales requiere técnicas especializadas y una comprensión profunda de la tecnología (Figueroa, 2013). Las leyes deben adaptarse para asegurar que los procedimientos de

recolección de evidencia respeten los derechos de los acusados y al mismo tiempo sean eficaces para asegurar condenas justas.

Finalmente, la vulneración de datos en el ciberespacio por parte de ciberdelincuentes es una amenaza creciente que requiere una respuesta robusta desde el derecho penal. Definir claramente los delitos, imponer penas severas, fomentar la cooperación internacional y adaptar los procedimientos de recolección de evidencia son pasos cruciales para combatir este fenómeno. Solo a través de un enfoque integral y adaptativo se puede proteger adecuadamente la información en la era digital y garantizar la seguridad y privacidad de los datos de todos los usuarios del ciberespacio.

2.1 Desafíos en la Aplicación de la Ley.

La aplicación de la ley en el contexto contemporáneo enfrenta una serie de desafíos sin precedentes que se extienden desde el ámbito local hasta el global. Estos retos son multifacéticos, abarcando aspectos tecnológicos, sociales, políticos y éticos, y requieren respuestas innovadoras y colaborativas para asegurar la efectividad y la justicia en la aplicación de la ley.

Uno de los desafíos más significativos es el ritmo acelerado de la evolución tecnológica, por lo que, la aparición de nuevas tecnologías como la inteligencia artificial, la biometría, y las redes sociales ha transformado el escenario del crimen y, por ende, las estrategias requeridas para combatirlo (Aguirre & Jiménez , 2020). La ciberdelincuencia, por ejemplo, plantea problemas particulares en términos de jurisdicción y extraterritorialidad, ya que los delitos pueden cometerse desde cualquier lugar del mundo, dificultando la identificación y persecución de los infractores (Roztocki, Soja y Roland, 2019).

Además, la globalización ha incrementado la complejidad de la aplicación de la ley, con delitos que a menudo trascienden fronteras nacionales, lo que requiere una cooperación internacional más estrecha y mecanismos efectivos de colaboración entre agencias de aplicación de la ley de diferentes países. Sin embargo, las diferencias en los marcos legales y en los recursos disponibles

pueden obstaculizar esta cooperación, dejando espacios seguros para los delincuentes (Consejo Nacional de Política Económica y Social, 2016).

Por otro lado, las cuestiones de privacidad y derechos civiles emergen como preocupaciones críticas en la aplicación de la ley moderna. El uso de tecnologías de vigilancia y recolección de datos debe equilibrarse cuidadosamente con el respeto a la privacidad individual y las libertades fundamentales (Ronancio, Vélez y Agudelo, 2022). Esto requiere un marco legal claro y transparente, así como un debate público informado sobre los límites y controles adecuados para estas tecnologías.

El aumento de la polarización social y política en muchas sociedades también representa un desafío para la aplicación de la ley, ya que puede erosionar la confianza y la cooperación entre la comunidad y las fuerzas del orden (Jiménez, Maretelo y Jaimes, 2017). La percepción de injusticia o discriminación en la aplicación de la ley puede provocar tensiones comunitarias y socavar la legitimidad y eficacia de las autoridades.[6]

En respuesta a estos desafíos, es esencial promover la innovación y la adaptabilidad dentro de las agencias de aplicación de la ley, ello implica la adopción de nuevas tecnologías y metodologías, la formación continua del personal, y la creación de marcos legales y colaborativos que puedan responder eficazmente a las cambiantes dinámicas del crimen y la justicia, máxime al hacer mención de conductas típicas y antijurídicas cometidas en el metaverso o el ciberespacio (Tavares & Bitencourt, 2021). Por ende, se analizará en concreto, el caso europeo, así como el colombiano, con el fin de entender desde la perspectiva legal cuales son las estrategias que ha implementado esta

[6] Cuando los ciudadanos perciben que la justicia se aplica de manera desigual o sesgada, se genera una brecha que dificulta la colaboración necesaria entre la población y las fuerzas de seguridad. Esta falta de cooperación es fundamental, pues el éxito en la prevención y resolución de crímenes a menudo depende de la información y el apoyo proporcionado por la comunidad. Además, la percepción de parcialidad o discriminación puede llevar a protestas y disturbios, los cuales no solo ponen en riesgo la estabilidad social, sino que también desvían recursos y atención de las actividades de vigilancia y respuesta a delitos, incluyendo aquellos cometidos en el ciberespacio. Que supone entonces una tarea mucho más compleja para el Estado, en conjunto con sus instituciones.

organización, así como el Estado colombiano, y determinar qué tan viable es, en un contexto social, donde las personas desplazan sus actividades, tareas y rutina general a espacios digitales (Consejo de la Unión Europea, 2013).

2.1 Caso Europeo en la protección de datos personales en el ciberespacio.

La protección de datos personales en el ciberespacio es una preocupación creciente en la era digital, y Europa se ha posicionado a la vanguardia en la implementación de medidas robustas para salvaguardar la privacidad de sus ciudadanos. El caso europeo en la protección de datos personales destaca por su enfoque integral y normativo, siendo el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) la piedra angular de esta estrategia.

Por otro lado, la implementado en mayo de 2018, el GDPR ha transformado el paisaje de la privacidad de datos en Europa y más allá, estableciendo un marco legal sólido que impone obligaciones estrictas a las organizaciones y otorga derechos significativos a los individuos respecto al tratamiento de sus datos personales (Puerto y Sferrazza, 2018). Este reglamento se aplica a todas las empresas que operan dentro de la UE, así como a aquellas que ofrecen bienes o servicios a ciudadanos de la UE, independientemente de su ubicación, lo que subraya el alcance global de su impacto (Parlamento Europeo y el Consejo de la Unión Europea, 2014).

Una de las características distintivas del GDPR es el principio de consentimiento explícito, que requiere que las organizaciones obtengan un permiso claro e inequívoco de los individuos antes de procesar sus datos personales. Esto ha fortalecido el control de los usuarios sobre su información, asegurando que su tratamiento sea transparente y bajo su propio consentimiento (Figueroa, 2013). Además, el GDPR introduce el derecho al olvido, que permite a los individuos solicitar la eliminación de sus datos personales cuando ya no son necesarios para el propósito original o cuando retiran su consentimiento. Este derecho refleja la creciente demanda de los ciudadanos de tener mayor autonomía sobre su información en el ciberespacio.

Por ello, la obligación de notificar brechas de seguridad es otra disposición clave del GDPR, que exige a las organizaciones informar a las autoridades competentes y a los afectados en un plazo máximo de 72 horas después de detectar una violación de datos. Esta medida busca incrementar la transparencia y garantizar una respuesta rápida a incidentes que puedan comprometer la privacidad o la seguridad de la información personal (Parlamento Europea y Consejo de Europa, 2013).

El GDPR también ha establecido fuertes incentivos para el cumplimiento, imponiendo severas multas por violaciones que pueden ascender hasta el 4% del volumen de negocio anual global de la entidad infractora o 20 millones de euros, lo que sea mayor. Estas sanciones han motivado a las empresas a adoptar medidas proactivas para asegurar la protección de datos, incluyendo la designación de un delegado de Protección de Datos (DPO) en ciertos casos (Martínez, 2020).

El caso europeo demuestra el compromiso con la protección de la privacidad en el ciberespacio y sirve como un modelo a seguir para otras regiones. El impacto del GDPR se extiende más allá de sus fronteras, influyendo en políticas de privacidad globales y promoviendo un enfoque más consciente y respetuoso hacia el tratamiento de los datos personales. A medida que avanzamos hacia un futuro cada vez más digitalizado, la experiencia europea en la protección de datos personales ofrece valiosas lecciones sobre la importancia de equilibrar los beneficios tecnológicos con los derechos fundamentales de los individuos.

2.2 Caso colombiano en la protección de datos personales en el ciberespacio

Colombia ha tomado pasos significativos para fortalecer la protección de datos personales en el ciberespacio, reflejando una creciente conciencia sobre la importancia de salvaguardar la información personal en la era digital. A través de diversas iniciativas legislativas y regulatorias, Colombia se ha esforzado por establecer un marco legal robusto que responda a los desafíos emergentes relacionados con la privacidad y la seguridad de los datos en línea.

Uno de los pilares en la protección de datos personales en Colombia es la Ley Estatutaria 1581 de (2012), que establece los principios, derechos, deberes y procedimientos para garantizar el derecho al habeas data. Esta ley aplica a cualquier tratamiento de datos personales dentro del territorio colombiano y establece directrices claras para el manejo de información personal, enfatizando la importancia del consentimiento del titular de los datos, la seguridad de la información y la transparencia en el tratamiento de datos.

El Reglamento a la Ley 1581, Decreto 1377 de 2013, complementa y reglamenta la ley anterior, proporcionando un marco detallado para la implementación de las políticas de protección de datos. Este reglamento destaca la necesidad de informar a los titulares sobre la recolección y uso de sus datos, así como garantizar el derecho a conocer, actualizar y rectificar la información que se almacena sobre ellos (Consejo Nacional de Política Económica y Social, 2010).

Además, la Superintendencia de Industria y Comercio (SIC) desempeña un papel crucial como autoridad de vigilancia y control en materia de protección de datos personales en Colombia. La SIC tiene la autoridad para imponer sanciones y garantizar el cumplimiento de las normativas relacionadas con la privacidad de datos, actuando como un ente regulador y de supervisión en este ámbito crucial (Consejo Nacional de Política Económica y Social, 2016).

El caso colombiano también refleja un esfuerzo por adaptarse a la dinámica cambiante del ciberespacio y los avances tecnológicos. Se ha reconocido la importancia de proteger la información personal no solo en el ámbito tradicional sino también en entornos digitales, lo que ha llevado a la implementación de directrices específicas para la gestión de datos personales en la nube y en el contexto del comercio electrónico (Gurría, 2009).

En el contexto internacional, Colombia ha buscado alinear su legislación con estándares globales, como los establecidos por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), de la cual Colombia es miembro. Esto no solo refuerza el marco de protección de datos en

el país, sino que también facilita el intercambio de información y la cooperación en asuntos relacionados con la privacidad de datos a nivel internacional (Red Iberoamericana de Protección de Datos, 2017).

Sin embargo, a pesar de estos avances, la protección de datos personales en el ciberespacio en Colombia enfrenta desafíos continuos, como la necesidad de aumentar la conciencia y educación sobre ciberseguridad entre los ciudadanos y las empresas, y la adaptación constante del marco legal a las nuevas tecnologías y modalidades de ciberdelincuencia (Red Iberoamericana de Protección de Datos, 2006).

En conclusión, el caso colombiano ilustra un compromiso creciente con la protección de datos personales en el ciberespacio, a través de la implementación de leyes, regulaciones y estructuras institucionales. Aunque aún hay desafíos por superar, Colombia está avanzando en la dirección correcta, buscando equilibrar los beneficios de la era digital con la protección de los derechos fundamentales de sus ciudadanos en el ámbito de la privacidad de datos.

3. Desafíos de seguridad de los sistemas informáticos: Las nuevas modalidades del cibercrimen.

En la actualidad, los sistemas informáticos enfrentan una serie de desafíos de seguridad debido a las nuevas modalidades del cibercrimen. La rápida evolución de la tecnología y el aumento de la conectividad global han generado un entorno en el que las amenazas cibernéticas se han vuelto más sofisticadas y difíciles de combatir. Entre los principales desafíos se encuentran el ransomware, el phishing, y la transnacionalidad del ciberespacio, cada uno presentando problemas únicos que requieren respuestas innovadoras y colaborativas (Yanping, et al, 2012), (Roztocki, Soja, & Roland Weistroffer, 2019).

En ese orden de ideas, como previamente se expuso el ransomware es una de las amenazas más insidiosas en el panorama de la ciberseguridad. Siendo este tipo de software malicioso cifra los datos de las víctimas y exige un rescate para liberar la información (Opazo, 2019). Las consecuencias de un ataque de ransomware pueden ser devastadoras, no solo por el costo económico directo del rescate, sino también por las interrupciones operativas y el potencial daño a la reputación de las organizaciones afectadas, a causa de ello, autores como (Abdulaziz, et al, 2024) proponen el uso de tecnologías Blockchain a fin de evadir ataques de ransomware, así como otras modalidades de ciberdelitos[7]. La naturaleza anónima de las transacciones con criptomonedas facilita a los delincuentes evadir la justicia, complicando aún más la lucha contra este tipo de cibercrimen (Radanliev, 2024).

El phishing, por otro lado, se basa en la ingeniería social para engañar a las personas y obtener información confidencial, como contraseñas y detalles financieros. Los ataques de phishing han evolucionado para ser cada vez más sofisticados y específicos, utilizando técnicas como el spear phishing para dirigirse a individuos concretos dentro de una organización. La educación y concienciación de los usuarios son esenciales para combatir este tipo de amenaza, así como el desarrollo de tecnologías avanzadas de filtrado y detección de correos electrónicos maliciosos (Fu, Wang, & Feng, 2024).

La transnacionalidad del ciberespacio añade una capa adicional de complejidad a la aplicación de la ley en el ámbito de los ciberdelitos (Silva García & Montoya Barreto, 2022). Los delincuentes pueden operar desde cualquier lugar del mundo, lo que dificulta la identificación y

[7] Las tecnologías blockchain pueden aumentar la seguridad frente a los ataques de ransomware mediante su inmutabilidad y transparencia, lo que asegura la integridad de los datos; su descentralización, que elimina puntos únicos de fallo; y el fortalecimiento de sistemas de identidad y autenticación. Además, la trazabilidad y registro de incidentes de blockchain ayudan en la respuesta a ataques, y los contratos inteligentes pueden automatizar la protección de datos. Sin embargo, su implementación presenta desafíos y debe integrarse con otras estrategias de ciberseguridad para ser verdaderamente efectiva (MarzoratI, 2019); (Abdulaziz, y otros, 2024).

persecución de los infractores. Siendo crucial la cooperación internacional para abordar este desafío, requiriendo la coordinación entre diferentes jurisdicciones y la adopción de marcos legales armonizados que faciliten la colaboración y el intercambio de información (Parada, 2018).[8]

Además de estos desafíos específicos, existe una necesidad constante de mejorar la infraestructura de seguridad informática (Pérez, 2018. Las organizaciones deben invertir en tecnologías avanzadas de ciberseguridad, como el cifrado de datos y la autenticación multifactor, para proteger sus sistemas y datos contra accesos no autorizados. Asimismo, la implementación de políticas de seguridad rigurosas y la formación continua del personal son fundamentales para fortalecer la defensa contra las amenazas cibernéticas (Hamdi, et al, 2021).

En ese orden de ideas, los desafíos de seguridad de los sistemas informáticos en la era digital son vastos y multifacéticos (Recskó & Aranyossy, 2024). La lucha contra las nuevas modalidades del cibercrimen requiere un enfoque integral que combine medidas tecnológicas, educativas y de política pública. Solo a través de una respuesta coordinada y colaborativa, que involucre a gobiernos, organizaciones y ciudadanos, será posible crear un entorno digital más seguro y resiliente frente a las crecientes amenazas del ciberespacio.

3.1 Las transacciones electrónicas y confianza en el comercio electrónico: Análisis de delitos como el fraude de informático, phishing y comercio en línea.

Las transacciones electrónicas y el comercio en línea se han convertido en componentes esenciales de la economía global. Sin embargo, junto con sus beneficios, estos avances han traído consigo una serie de desafíos de seguridad, principalmente debido a la proliferación de delitos como

[8] La comisión del ciberdelito se configura complejamente debido a la transnacionalidad del ciberespacio, donde los delincuentes pueden operar desde cualquier lugar del mundo, dificultando su identificación y persecución. Esta dispersión geográfica exige una cooperación internacional eficaz, ya que las jurisdicciones nacionales son insuficientes para abordar las amenazas cibernéticas globales (Avdeev, Avdeeva, Smirnova, Rassolov, & Khvatova, 2021).

el fraude informático, el phishing y otros tipos de estafas en el comercio en línea. La confianza en el comercio electrónico depende en gran medida de la capacidad para mitigar estos riesgos y garantizar la seguridad de las transacciones.

El fraude informático es uno de los mayores obstáculos para la confianza en el comercio electrónico. Este tipo de delito abarca una variedad de actividades ilegales, incluyendo la falsificación de identidades, la manipulación de datos financieros y la creación de sitios web falsos para engañar a los consumidores. Los ciberdelincuentes utilizan técnicas avanzadas para interceptar información sensible, como números de tarjetas de crédito y credenciales de inicio de sesión, lo que puede resultar en pérdidas financieras significativas para las víctimas y las empresas involucradas.

Así las cosas, el phishing, tal y como se expuso previamente implica el envío de correos electrónicos fraudulentos que parecen provenir de fuentes legítimas, como bancos o servicios de pago en línea, con el objetivo de persuadir a los destinatarios para que revelen información personal o financiera (Requejo, 2020). A medida que las técnicas de phishing se vuelven más sofisticadas, los ataques pueden ser difíciles de detectar incluso para usuarios experimentados; siendo necesaria la educación y concienciación del público son cruciales para reducir la efectividad de estas tácticas engañosas (Valero, et, al, 2023).

El comercio en línea también enfrenta desafíos de seguridad relacionados con la integridad de las plataformas y la autenticidad de los productos vendidos. Por un lado, los sitios web falsos y los vendedores fraudulentos pueden engañar a los consumidores para que compren productos que nunca se entregan o que son de calidad inferior a la prometida. Autores como (Poy & Carriegos, 2017), exponen que este tipo de fraude no solo afecta a los consumidores, sino que también puede dañar la reputación de las plataformas legítimas de comercio electrónico, reduciendo la confianza general en el mercado en línea (Serventich, 2022).

Para combatir estas amenazas, es esencial que las empresas de comercio electrónico implementen medidas de seguridad robustas. Esto incluye el uso de certificados SSL para asegurar las transacciones, la implementación de sistemas de autenticación de múltiples factores y la realización de auditorías de seguridad regulares para identificar y corregir vulnerabilidades. Además, las plataformas deben establecer políticas claras de reembolso y protección al comprador para proporcionar una capa adicional de confianza a los consumidores.

A causa de la transformación de la comisión delictiva en materia de ciberdelitos, es menester aclarar que, a menudo son perpetrados por redes criminales que operan a través de fronteras nacionales (Ángeles, 2023), es crucial que los países trabajen juntos para compartir información y desarrollar estrategias efectivas para la prevención y persecución de estos delitos. Por ende, la armonización de las leyes de ciberseguridad y la creación de acuerdos de cooperación internacional pueden ayudar a crear un frente unido contra los ciberdelincuentes.

Los usuarios también juegan un papel fundamental en la protección contra el fraude en el comercio en línea. La adopción de buenas prácticas de seguridad, como el uso de contraseñas fuertes y únicas, la verificación de la autenticidad de los sitios web antes de realizar compras y la vigilancia de los estados de cuenta bancarios para detectar transacciones no autorizadas, puede ayudar a mitigar el riesgo de ser víctima de estos delitos (Barceló, 2021).

Lo cual sugiere que, la confianza en el comercio electrónico depende de la capacidad de todas las partes involucradas para enfrentar los desafíos de seguridad planteados por el fraude informático, el phishing y otras estafas en línea. A través de la implementación de tecnologías avanzadas de seguridad, la cooperación internacional y la educación de los usuarios, es posible crear un entorno más seguro para las transacciones electrónicas. Solo mediante un esfuerzo conjunto se puede garantizar que el comercio en línea siga siendo una opción viable y segura para consumidores y empresas en la era digital.

3.2 Delitos contra el patrimonio, el fraude electrónico, la estafa en línea y el robo de identidad: Un análisis a partir del bien jurídico protegido y los intereses económicos.

En la era digital, los delitos contra el patrimonio, incluyendo el fraude electrónico, la estafa en línea y el robo de identidad, se han convertido en amenazas significativas tanto para los individuos como para las organizaciones. Estos delitos no solo afectan el bienestar económico de las víctimas, sino que también socavan la confianza en el ecosistema digital. Así las cosas, el bien jurídico protegido en estos delitos es principalmente el patrimonio (Zaffaroni, 2009), que se refiere a los activos y recursos económicos de una persona o entidad. La protección del patrimonio es fundamental para garantizar la estabilidad financiera y la seguridad económica de los individuos y las empresas. Los ciberdelincuentes atacan este bien jurídico a través de diversas tácticas, cada una diseñada para explotar vulnerabilidades en los sistemas de seguridad y la falta de conocimiento de las víctimas (Fang, et al, 2024); (Consejo de Europa, 2021).

El fraude electrónico es una de las formas más comunes de delitos contra el patrimonio en el entorno digital. Este tipo de fraude implica el uso de tecnologías de la información y la comunicación para engañar a las víctimas y obtener beneficios económicos ilegítimos. Ejemplos comunes incluyen el phishing, el pharming y el spoofing, donde los delincuentes crean sitios web falsos o envían correos electrónicos fraudulentos para robar información personal y financiera. El impacto económico de estos delitos puede ser devastador, ya que las víctimas no solo pierden dinero, sino que también pueden enfrentar costos adicionales asociados con la recuperación de sus datos y la restauración de su identidad.

La estafa en línea, por otro lado, involucra la manipulación y el engaño a través de plataformas de comercio electrónico y redes sociales. Según Silva y Montoya (2022), los estafadores pueden crear perfiles falsos, productos inexistentes o servicios fraudulentos para atraer a los usuarios y robar su dinero. En ese orden de ideas, este tipo de delito no solo afecta el patrimonio de las víctimas,

sino que también daña la reputación de las plataformas legítimas de comercio en línea. La pérdida de confianza en estas plataformas puede tener un efecto dominó, reduciendo la participación del consumidor y afectando negativamente la economía digital en su conjunto (Ángeles, 2023).

El robo de identidad es otro delito grave contra el patrimonio que tiene consecuencias a largo plazo. Los delincuentes que roban la identidad de una persona pueden utilizar esa información para abrir cuentas bancarias, solicitar tarjetas de crédito o incluso cometer otros delitos bajo el nombre de la víctima. Asimismo, el proceso de recuperación de una identidad robada es complicado y puede llevar meses o incluso años, durante los cuales las víctimas pueden enfrentar dificultades financieras y emocionales; por lo que, la protección de la identidad digital se ha convertido en una prioridad crucial para prevenir estos ataques.

Desde la perspectiva de los intereses económicos, los delitos contra el patrimonio representan una amenaza significativa para la estabilidad financiera de los individuos y las organizaciones. Además de ello, las pérdidas directas asociadas con estos delitos incluyen dinero robado, costos legales y administrativos, y pérdida de productividad. Por tanto, las empresas pueden enfrentar sanciones regulatorias y pérdidas reputacionales que afectan su posición en el mercado. Para las economías nacionales, la proliferación de estos delitos puede resultar en una disminución de la confianza en el sistema financiero y una reducción en la inversión y el crecimiento económico (Jordi, 2023).

La lucha contra los delitos contra el patrimonio requiere un enfoque multifacético que combine medidas tecnológicas, educativas y legislativas. Según Kumar, et al (2018), las empresas deben invertir en tecnologías avanzadas de ciberseguridad, como el cifrado de datos y la inteligencia artificial para detectar y prevenir fraudes. Asimismo, es crucial educar a los consumidores sobre los riesgos y las mejores prácticas para proteger su información personal y financiera. Desde el ámbito legislativo, la creación y aplicación de leyes estrictas que penalicen estos delitos y protejan a las

víctimas es esencial para disuadir a los delincuentes y proporcionar un marco legal sólido para la persecución de estos crímenes.

En síntesis, los delitos contra el patrimonio, como el fraude electrónico, la estafa en línea y el robo de identidad, representan una amenaza significativa en la era digital. Entendiendo así que, la protección del bien jurídico del patrimonio y la seguridad de los intereses económicos requieren un enfoque integral que involucre a todas las partes interesadas, desde los gobiernos y las empresas hasta los individuos. Solo a través de una colaboración efectiva y la implementación de medidas de seguridad robustas se puede garantizar un entorno digital seguro y confiable para todos.

3.3 De los delitos contra la piratería, la copia ilegal de software, música, películas y otros contenidos protegidos por derechos de autor.

Los delitos contra la piratería y la copia ilegal de software, música, películas y otros contenidos protegidos por derechos de autor han adquirido una relevancia considerable. Estos delitos no solo afectan los intereses económicos de los creadores y las industrias culturales, sino que también plantean desafíos significativos para la protección de los derechos de propiedad intelectual. La piratería digital se ha convertido en una actividad global que aprovecha la naturaleza transnacional del ciberespacio, complicando los esfuerzos de las autoridades para combatirla (Añasco, Morocho, & Hallo, 2023).

Según Pardo (2018), el bien jurídico protegido en estos delitos es el derecho de autor, que otorga a los creadores el control exclusivo sobre el uso y distribución de sus obras. Este derecho es fundamental para incentivar la creatividad y la innovación, asegurando que los autores reciban una compensación justa por su trabajo. Sin embargo, la piratería digital socava este principio al permitir la distribución no autorizada de contenidos, reduciendo los ingresos de los creadores y las empresas que dependen de la explotación legítima de estas obras (Ivanova, 2023); (Moya, 2018).

La copia ilegal de software es uno de los aspectos más problemáticos de la piratería. El software pirata no solo representa una pérdida económica significativa para las empresas desarrolladoras, sino que también conlleva riesgos de seguridad para los usuarios. El software no autorizado a menudo carece de actualizaciones de seguridad y soporte técnico, dejando a los usuarios vulnerables a ataques cibernéticos y malware.

Por un lado, las plataformas ilegales de descarga y transmisión de contenido audiovisual han proliferado, facilitando el acceso gratuito a obras protegidas por derechos de autor. Esto no solo reduce las ventas y los ingresos por licencias de las industrias musicales y cinematográficas, sino que también afecta la viabilidad económica de los proyectos creativos (Hernández, 2022). La reducción de ingresos puede limitar la capacidad de los artistas y productores para invertir en nuevas obras, afectando negativamente la diversidad y calidad de los contenidos disponibles.

La lucha contra la piratería requiere un enfoque multifacético que combine la tecnología, la legislación y la educación. Las tecnologías de gestión de derechos digitales (DRM) son herramientas cruciales para proteger los contenidos contra la copia no autorizada y garantizar que solo los usuarios legítimos puedan acceder a las obras. Sin embargo, estas tecnologías deben ser complementadas por un marco legal robusto que penalice efectivamente la distribución y el uso de contenidos pirateados. Así las cosas, la cooperación internacional es esencial para abordar la naturaleza transnacional de la piratería, facilitando la persecución de infractores y el desmantelamiento de redes de distribución ilegal (Dos Santos, 2019).

Además de las medidas tecnológicas y legales, la educación desempeña un papel vital en la lucha contra la piratería. Es esencial concienciar a los usuarios sobre las implicaciones éticas y legales del uso de contenidos pirateados. Autores como (Malathi, Suganthi, & Jospin, 2024), refieren a la necesidad de promover una cultura de respeto por los derechos de autor y destacar los beneficios de consumir contenidos a través de canales legítimos puede contribuir significativamente a reducir la

demanda de obras piratas. Las campañas educativas dirigidas a diferentes grupos demográficos, incluidos estudiantes y profesionales, pueden ayudar a fomentar un mayor respeto por la propiedad intelectual (Jifei, etal, 2024).

Las plataformas de distribución de contenidos también tienen un papel crucial en la lucha contra la piratería. Ofrecer acceso asequible y conveniente a contenidos legítimos puede reducir el incentivo para recurrir a fuentes ilegales. Servicios de suscripción y modelos de negocio basados en la accesibilidad y la facilidad de uso pueden competir eficazmente con las plataformas piratas, proporcionando a los consumidores opciones legales atractivas y sostenibles. Solo a través de una colaboración continua y esfuerzos coordinados se puede crear un entorno digital que respete y valore la creatividad y la innovación, garantizando la sostenibilidad de las industrias culturales y el acceso justo a los contenidos para todos.

4. El buen gobierno y su papel en la acción y prevención de la administración de justicia frente a ciberdelitos.

El buen gobierno desempeña un papel fundamental en la administración de justicia, especialmente en el contexto de la prevención y acción frente a ciberdelitos. Este concepto implica la gestión eficiente, ética y transparente de los recursos y la autoridad para garantizar la seguridad, el bienestar y el respeto por los derechos de los ciudadanos (Rodríguez, 2019). En la era digital, donde los ciberdelitos se han convertido en una amenaza creciente, el papel del buen gobierno es crucial para establecer un marco robusto que permita prevenir, detectar y responder efectivamente a estas infracciones.

En primer lugar, el buen gobierno implica la adopción de políticas claras y eficaces que definan la naturaleza de los ciberdelitos y establezcan procedimientos adecuados para su investigación y sanción (Molero, et al, 2023). Esto incluye la creación de leyes específicas que

aborden la variedad de delitos cibernéticos, desde el fraude en línea hasta el terrorismo cibernético, pasando por la explotación infantil en internet y los ataques a la infraestructura crítica (Organización de las Naciones Unidas, 2019).

Un aspecto crucial del buen gobierno en este contexto es la asignación de recursos suficientes para la prevención y lucha contra los ciberdelitos (Oleiwi, 2023). Esto no solo implica inversiones en tecnología y herramientas de ciberseguridad sino también en la capacitación de personal especializado que pueda entender y enfrentar las complejidades de la ciberdelincuencia (Roncancio, Vélez y Agudelo, 2022).

La colaboración interinstitucional e internacional también es vital en el buen gobierno frente a los ciberdelitos. Dado que estas actividades delictivas a menudo trascienden las fronteras nacionales, es imprescindible que exista una coordinación efectiva entre diferentes jurisdicciones y organismos para compartir información, estrategias y recursos que permitan una acción conjunta contra los ciberdelincuentes (Bibri, Sharif y Krogstie, 2023).

El buen gobierno también implica asegurar la participación ciudadana y la transparencia en la gestión de la ciberseguridad (Mejía, 2019). Los ciudadanos deben estar informados sobre los riesgos y las medidas de prevención contra los ciberdelitos, y deben tener canales disponibles para denunciar sospechas de actividades delictivas en línea. Además, la transparencia en las acciones gubernamentales ayuda a construir confianza en las instituciones encargadas de combatir el ciberdelito (Ferriz, 2022).

La justicia rápida y eficaz es otro componente esencial del buen gobierno en la lucha contra los ciberdelitos. Los sistemas judiciales deben estar preparados para manejar casos de ciberdelincuencia con la celeridad y la eficacia requeridas, lo que implica no solo contar con el marco legal adecuado sino también con jueces y fiscales capacitados en las particularidades de estos delitos Hancco, 2022)

La prevención es igualmente crucial y debe ser una prioridad dentro de las políticas de buen gobierno. Esto incluye programas de educación y concienciación para el público en general, así como estrategias específicas para proteger a los grupos más vulnerables, como los niños y los ancianos, de los peligros del ciberespacio (Hernández, 2019)[9].

En términos de acción, el buen gobierno debe garantizar que existan mecanismos eficientes para la detección y respuesta rápida ante incidentes de ciberdelincuencia. Esto incluye la capacidad de realizar investigaciones forenses digitales, la implementación de respuestas inmediatas ante incidentes de seguridad cibernética y la recuperación de información y sistemas afectados (Karagiannis & Vergidis, 2021).

Por otro lado, el buen gobierno en la lucha contra los ciberdelitos también debe contemplar la resiliencia y la capacidad de recuperación de las infraestructuras críticas y los sistemas esenciales. Esto significa no solo proteger estos activos de posibles ataques sino también asegurar que puedan recuperarse y restablecerse rápidamente en caso de ser comprometidos (Medan, 2020). Por ende, el buen gobierno es esencial para crear un entorno digital seguro y confiable, donde los derechos y la seguridad de los ciudadanos estén protegidos frente a la amenaza de los ciberdelitos. A través de políticas claras, recursos adecuados, colaboración, transparencia, justicia eficaz y estrategias de prevención y resiliencia, el gobierno puede jugar un papel decisivo en la mitigación y respuesta a estos delitos en la era digital (Solé, 2023)

[9] Ello, denota entonces que al implementar programas educativos y de sensibilización, los gobiernos pueden equipar a los ciudadanos con el conocimiento y las herramientas necesarias para navegar por el ciberespacio de manera segura, minimizando así su susceptibilidad a ciberataques y fraudes. Esto es particularmente importante para grupos vulnerables como niños y ancianos, quienes pueden no estar naturalmente familiarizados con las amenazas digitales y, por lo tanto, requieren orientación específica y apoyo para defenderse contra los riesgos que pueden encontrar en línea. En última instancia, tales estrategias preventivas no solo protegen a los individuos, sino que también fortalecen la resiliencia comunitaria y nacional ante los crecientes desafíos del ciberespacio.

4.1 Políticas públicas en materia de ciberseguridad y gobierno digital: Analizando el caso colombiano.

La transformación digital de Colombia ha avanzado significativamente en la última década, impulsada por diversas políticas públicas que buscan fortalecer la ciberseguridad y fomentar la confianza en el entorno digital. La Dirección de Política Económica y Social ha emitido varios Documentos CONPES que establecen las bases para una estrategia nacional integral en materia de ciberseguridad y gobierno digital. Entre los más relevantes se encuentran los documentos CONPES 3701, 3854 y 3995, los cuales delinean las acciones y estrategias del gobierno colombiano para enfrentar las crecientes amenazas en el ciberespacio y promover un entorno digital seguro y confiable.

El Documento CONPES 3701, emitido en 2011, estableció los lineamientos de política para ciberseguridad y ciberdefensa en Colombia. Su objetivo principal era fortalecer las capacidades del Estado para enfrentar amenazas cibernéticas, incluyendo la creación del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) y el Centro Cibernético Policial (CCP). Esta política se centró en el desarrollo de capacidades gubernamentales y en la protección de infraestructuras críticas, sin embargo, no atendió de manera suficiente el desarrollo de capacidades para ciudadanos y otros sectores.

En 2016, se emitió el Documento CONPES 3854, que redefinió la estrategia nacional en seguridad digital con un enfoque más amplio e inclusivo. Este documento reconoció la necesidad de una gestión de riesgos más proactiva y de involucrar a múltiples partes interesadas, incluyendo ciudadanos, sectores económicos y organizaciones. Se establecieron estrategias para fortalecer la defensa y la soberanía nacional en el entorno digital, promoviendo la cooperación nacional e internacional en ciberseguridad.

El más reciente Documento CONPES 3995, emitido en 2020, formuló una política nacional enfocada en ampliar la confianza digital y mejorar la seguridad digital en Colombia. Este documento se centró en tres pilares: el fortalecimiento de las capacidades en seguridad digital de los ciudadanos, el sector público y el sector privado; la actualización del marco de gobernanza en materia de seguridad digital; y la adopción de modelos, estándares y marcos de trabajo en nuevas tecnologías. La política busca una sociedad digital inclusiva y competitiva, abordando la ciberseguridad no solo como un reto técnico, sino también como un desafío social y económico.

Uno de los avances más significativos en términos de generar confianza digital se dio con la promulgación de la Ley Estatutaria 1581 de 2012, que establece el derecho de las personas a conocer, actualizar y rectificar su información personal. Este marco legal reconoce los datos personales como un bien jurídico protegido y proporciona una base sólida para la protección de la privacidad en el entorno digital.

Además, la implementación de la Política de Gobierno Digital en 2018, mediante el Decreto 1008, consolidó el enfoque de seguridad y privacidad de la información como habilitadores transversales del desarrollo digital. Esta política no solo busca proteger los datos personales, sino también fomentar la transparencia y la confianza en los servicios digitales ofrecidos por el Estado.

En ese orden de ideas, las políticas públicas en materia de ciberseguridad y gobierno digital en Colombia han evolucionado para enfrentar las complejas amenazas del ciberespacio. Desde el fortalecimiento de las capacidades gubernamentales en ciberdefensa hasta la inclusión de ciudadanos y sectores económicos en la gestión de riesgos de seguridad digital, estas políticas reflejan un enfoque integral y proactivo para construir un entorno digital seguro y confiable. La continua adaptación y actualización de estas estrategias serán esenciales para mantener la seguridad y la confianza en la era digital.

4.2 El contraste entre las políticas públicas y su rol en contra de la ciberdelincuencia transnacional.

El auge de la ciberdelincuencia transnacional ha planteado desafíos significativos para los gobiernos de todo el mundo, requiriendo políticas públicas robustas y cooperación internacional para mitigar sus efectos. En Colombia, las políticas públicas en materia de ciberseguridad y gobierno digital han evolucionado considerablemente en la última década, con el objetivo de fortalecer la defensa contra las amenazas cibernéticas y proteger tanto a las infraestructuras críticas como a los ciudadanos. A pesar de estos esfuerzos, la naturaleza transnacional de la ciberdelincuencia sigue presentando retos únicos que requieren respuestas coordinadas y adaptativas.

El Documento CONPES 3701, emitido en 2011, marcó un hito en la formulación de políticas de ciberseguridad en Colombia. Este documento estableció la creación del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) y el Centro Cibernético Policial (CCP), enfocándose en la protección de infraestructuras críticas y el fortalecimiento de las capacidades del Estado para enfrentar amenazas cibernéticas. Sin embargo, la eficacia de estas medidas frente a la ciberdelincuencia transnacional depende en gran medida de la cooperación internacional y la capacidad de los gobiernos para coordinar acciones a través de fronteras.

El Documento CONPES 3854 de 2016 amplió la estrategia nacional al incluir a múltiples partes interesadas y promover la cooperación internacional en ciberseguridad. Este enfoque más inclusivo reconoció que la lucha contra la ciberdelincuencia transnacional no puede ser solo una tarea del gobierno, sino que requiere la colaboración activa del sector privado, las organizaciones no gubernamentales y los ciudadanos. La política enfatizó la necesidad de compartir información y recursos con otros países para fortalecer las defensas colectivas y mejorar la capacidad de respuesta ante incidentes cibernéticos que cruzan fronteras.

A pesar de estos avances, la ciberdelincuencia transnacional sigue evolucionando, y los delincuentes encuentran nuevas formas de explotar las vulnerabilidades en los sistemas globales. El Documento CONPES 3995 de 2020 abordó esta realidad al enfocarse en mejorar la confianza digital y actualizar el marco de gobernanza en seguridad digital. Por lo que, se promueve la adopción de estándares internacionales y mejores prácticas en nuevas tecnologías, reforzando así la capacidad del país para participar en iniciativas globales de ciberseguridad.

El contraste entre las políticas públicas nacionales y la naturaleza transnacional de la ciberdelincuencia resalta la importancia de la cooperación internacional. Iniciativas como la Convención de Budapest sobre el Ciberdelito proporcionan un marco legal para la colaboración y el intercambio de información entre países (Zhuo, Irresberger y Bostandzic , 2024). La participación de Colombia en estos tratados y acuerdos internacionales es crucial para mejorar su capacidad de respuesta y asegurar que las políticas nacionales estén alineadas con los estándares globales.

En conclusión, las políticas públicas en materia de ciberseguridad en Colombia han avanzado significativamente, pero enfrentar la ciberdelincuencia transnacional requiere un esfuerzo continuo y coordinado a nivel internacional. La evolución de los Documentos CONPES refleja un reconocimiento creciente de la necesidad de cooperación y adaptación para proteger eficazmente a los ciudadanos y las infraestructuras críticas frente a las amenazas cibernéticas globales. Solo a través de una colaboración estrecha y la adopción de estándares internacionales se puede fortalecer la resiliencia frente a la ciberdelincuencia transnacional.

Conclusiones

En la era digital, los ciberdelitos presentan una serie de desafíos complejos que requieren un análisis profundo desde el derecho penal, tanto en su estructura básica como en su aplicación pura. Los documentos y análisis revisados en esta conversación, en particular el enfoque Colombiano

reflejado en los Documentos CONPES, proporcionan una base sólida para entender cómo se configuran estos delitos y cuáles son las estrategias más efectivas para enfrentarlos.

El bien jurídico protegido en los ciberdelitos es fundamentalmente la seguridad de la información y la privacidad de los datos personales. En el contexto del derecho penal, estos bienes jurídicos son esenciales para garantizar la estabilidad y la confianza en las interacciones digitales. Los ciberdelitos como el phishing, el ransomware y la piratería de contenidos violan estos bienes jurídicos, afectando tanto a individuos como a organizaciones. La protección de estos bienes requiere una actualización constante de las normativas legales para adaptarse a la evolución tecnológica y las nuevas formas de delincuencia en el ciberespacio.

La estructura básica del derecho penal en relación con los ciberdelitos se centra en la tipificación de conductas delictivas, la definición de penas y la creación de procedimientos judiciales adecuados para perseguir y sancionar estos delitos. En Colombia, la Ley 1581 de 2012 y los Documentos CONPES, como el 3701, 3854 y 3995, han establecido un marco legal robusto para enfrentar estas amenazas. Estos documentos destacan la importancia de proteger los datos personales, asegurar la infraestructura crítica y promover la cooperación internacional para combatir la ciberdelincuencia transnacional.

El derecho penal puro en el contexto de los ciberdelitos implica la aplicación de principios y normas penales tradicionales a nuevas formas de criminalidad digital. Esto incluye la tipificación clara de delitos como el acceso no autorizado a sistemas informáticos, la distribución de malware y el fraude electrónico. La complejidad de estos delitos, especialmente su carácter transnacional, requiere una adaptación continua del derecho penal para asegurar que los responsables sean efectivamente perseguidos y sancionados. La cooperación internacional, facilitada por acuerdos como la Convención de Budapest, es esencial para lograr una aplicación eficaz del derecho penal puro en este ámbito.

La lucha contra la ciberdelincuencia transnacional subraya la necesidad de una cooperación internacional estrecha y la armonización de los marcos legales. Los esfuerzos de Colombia para alinearse con estándares globales y participar en iniciativas internacionales reflejan un reconocimiento de la importancia de estas estrategias. La adopción de marcos legales armonizados facilita el intercambio de información y la colaboración entre países, permitiendo una respuesta más eficaz a las amenazas cibernéticas que trascienden las fronteras nacionales.

Un componente crucial en la lucha contra los ciberdelitos es la educación y concienciación de la población. Las políticas públicas deben incluir programas de formación en ciberseguridad tanto para individuos como para organizaciones. La educación sobre los riesgos asociados con el uso de tecnologías digitales y las mejores prácticas para proteger la información personal puede reducir significativamente la vulnerabilidad frente a los ciberdelincuentes.

Por lo que, la innovación y la adaptabilidad son esenciales para enfrentar la evolución constante de los ciberdelitos. Las políticas públicas y el derecho penal deben ser lo suficientemente flexibles para incorporar nuevas tecnologías y métodos de protección. La inversión en investigación y desarrollo de tecnologías avanzadas de ciberseguridad, junto con la formación continua de profesionales en este campo, es fundamental para mantener un entorno digital seguro y resiliente. En conclusión, la protección del bien jurídico en los ciberdelitos, la estructura del derecho penal y su aplicación pura requieren un enfoque integral que combine medidas legales, tecnológicas y educativas. Solo a través de un esfuerzo coordinado y adaptativo será posible enfrentar eficazmente las amenazas del ciberespacio y garantizar la seguridad y privacidad de los datos en la era digital, realizar estudios más específicos sobre el tema toda vez que la legislación Colombiana tiene como base la emitida en la Comunidad Económica Europea, motivo por el cual las universidades deben de realizar estudios más profundos sobre esta nueva modalidad de delinquir.

Referencias

Abdulaziz, A., Alameer, A., Alsaleh, H., Alkadyan, F., Allheeib, N., Alhadlag, A., & Alabdulkarim , Y. (2024). Data Mesh Meets Blockchain. *International Journal of Computational Intelligence Systems, 17*(27), 1-15. doi:https://doi.org/10.1007/s44196-024-00404-z

Aguirre, R., & Jiménez , C. (2020). Tecnologías de la información y la comunicación para la conservación y promoción de la diversidad cultural en el marco del pluralismo jurídico. *Revista digital de Derecho Administrativo, 22*, 1- 15.

Agustina, J. (2021). Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma? *Estudios Penales Y Criminológicos, 41*, 707-777. doi:https://doi.org/10.15304/epc.41.7433

Akbari, Y., Al Maadeed, S., Elharrouss, O., Ottakath, N., & Khelifi, F. (2024). Hierarchical deep learning approach using fusion layer for Source Camera Model Identification based on video taken by smartphone[Formula presented]. *Expert Systems with Applications, 238*, 1-10. doi:https://doi-org.iue.basesdedatosezproxy.com/10.1016/j.eswa.2023.121603

Alegre Rodríguez, L., & Padilla López, R. (2023). GOBIERNO DIGITAL, MODERNIZACIÓN DEL ESTADO Y SERVICIO AL CIUDADANO Consideraciones en una estrategia de gobierno digital en Perú. *VISUAL Review. International Visual Culture Review , 13*(2), 1-8. doi:https://doi.org/10.37467/revvisual.v10.4567

Ángeles, J. (2023). Los guardianes de acceso al metaverso. (Re)pensando el Derecho de la competencia de la Unión Europea. *Cuadernos de Derecho Transnacional, 15*(1), 275- 296. doi:10.20318/cdt.2023.7541

Añasco, C., Morocho, K., & Hallo, M. (2023). Using Data Mining Techniques for the Detection of SQL Injection Attacks on Database Systems. *Escuela Politecnica Nacional. Revista Politecnica, 51*(2), 19- 28. doi:10.33333/rp.vol51n2.02

Avdeev, V., Avdeeva, O., Smirnova, V., Rassolov, I., & Khvatova, M. (2021). Improvement of information technology and its impact on information security. (11, Ed.) *International Journal of Emerging Technology and Advanced Engineering*. Obtenido de https://ijetae.com/files/Volume11Issue11/IJETAE_1121_02.pdf

Ayuso García, M., & Ayuso Sánchez, M. (2010). El acceso a fuentes abiertas al conocimiento en ciencia y tecnología en américa latina y el caribe. *Revista General de Informacion y Documentacion, 20*(1), 115- 139.

Barceló Compte, R. (2021). El impacto de la tecnología blockchain en la contratación privada: ¿hacia una contratación inteligente? *Revista de Internet, Derecho y Política*(33), 1-13. Obtenido de https://diposit.ub.edu/dspace/bitstream/2445/178441/1/712773.pdf

Bibri, S., Alexandre, A., Sharifi, A., & Krogstie, J. (2023). Environmentally sustainable smart cities and their converging AI, IoT, and big data technologies and solutions: an integrated approach to an extensive literature review. *Energy Informatics, 6*(1), 1- 39. doi:10.1186/s42162-023-00259-2

Cardona Centeno, E., Duarte Mondragón, S. L., Torres Ospina, E. F., & Mateus Franco, L. M. (2022). Resocialization of the penalty: Challenges from the new information and communication technologies. *Revista de Ciencias Sociales*, 303- 314. doi:10.31876/rcs.v28i4.39132

Caterini, M., & Castellano, P. S. (2022). El sistema penal en la encrucijada ante el reto de la inteligencia artificial. *Revista de Internet, Derecho y Politica*(35), 1-19. doi:https://doi.org/10.7238/idp.v0i35.392754

Chib, A., Bentley, C., & Wardoyo, R.-J. (2019). Distributed digital contexts and learning: Personal empowerment and social transformation in marginalized populations. *Grupo Comunicar Ediciones, 27*(58), 51- 60. doi:10.3916/C58-2019-05

Comisión de Asuntos jurídicos. (2017). Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica. *Parlamento Europeo Informe A8- 0005/2017*, 1- 31. Obtenido de https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html

Congreso de la República de Colombia. (2012). *Ley 1581.* Bogotá D.C: Diario Oficial No. 48.587. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Consejo de Europa. (2021). *Convención de Budapest sobre la ciberdelincuencia*. Estrasburgo: Consejo de Europa. División de Ciberdelito.

Consejo de la Unión Europea. (2013). *Recomendación del Consejo de la Unión Europea 2013/C120/01*. Bruselas: Consejode la Unión Europea. Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013H0426(01)

Consejo Nacional de Política Económica y Social. (2010). *CONPES 3650.* Bogotá D.C: Departamento Nacional de Planeación.

Consejo Nacional de Política Económica y Social. (2016). *CONPES 3854.* Bogotá D.C: Departamento Nacional de Planeación. Obtenido de https://colaboracion.dnp.gov.co/cdt/conpes/econ%C3%B3micos/3854.pdf

Consejo Nacional de Política económica y social. (2019). *Documento CONPES 3975. Política para la Transformación Digital e Inteligencia Artificial.* Bogotá D.C: Departamento Nacional de Planeación.

Crespo Mejía, Y. A., Carrión León, K. E., Paredes López, J. A., & Infante Miranda, M. E. (2022). Etapas del proceso penal: Importancia de la Defensa Material y técnica. *Universidad y Sociedad, 14*(S4), 70- 80. Obtenido de https://www-scopus-com.iue.basesdedatosezproxy.com/record/display.uri?eid=2-s2.0-85138517426&origin=resultslist&sort=plf-f&src=s&sid=0bea73850a6f563b7320c5acef691593&sot=b&sdt=b&s=TITLE-ABS-KEY%28Proceso+penal%29&sl=39&sessionSearchId=0bea73850a6f563b7320

Dos Santos, D. (2019). A territorialidade no contexto da criminalidade global: considerações sobre a influência do ciberespaço na delimitação jurisdicional. *Revista Brasileira de Direito Processual Penal, 5*(2), 597- 622. doi:10.22197/rbdpp.v5i2.235

Estella, F., & Martínez, A. (2022). Derecho a la Competencia vs Privacidad: ¿El Gran Dilema en los Nuevos Mercados Digitales? *Revista Cuadernos de Derecho Transnacional, 14*(1), 169- 195. doi:10.20318/cdt.2022.6682

Fang, J., Feng, T., Guo, X., Ma, R., & Lu, Y. (2024). Blockchain-cloud privacy-enhanced distributed industrial data trading based on verifiable credentials. *Journal of Cloud Computing, 13*(30), 1-17. doi:https://doi.org/10.1186/s13677-023-00530-7

Ferriz Sánchez, R. (2022). Participación ciudadana y Buen Gobierno democrático. Posibilidades y límites en la era digital. *Revista Espanola de Derecho Constitucional*(125), 341- 355.

Figueroa G., R. (2013). El derecho a la privacidad en la jurisdicción de protección. *Revista Chilena de Derecho, 40*(3), 859- 889. doi:10.4067/s0718-34372013000300005

Fu, B., Wang, Y., & Feng, T. (2024). CT-GCN+: a high-performance cryptocurrency transaction graph convolutional model for phishing node classification. *Cybersecurity, 7*(3), 1-16. doi:https://doi.org/10.1186/s42400-023-00194-5

Fuentes Benítez, E. (2022). El derecho fundamental a la protección de datos personales en Argentina y en el mundo : los conflictos extraterritoriales por los delitos informáticos. *Universidad de San Andrés. Tesis de Pregrado*, 1- 56. Obtenido de http://hdl.handle.net/10908/22383

Gurría, J. A. (2009). El buen gobierno para el desarrollo económico y social. Revista del CLAD Reforma y Democracia. *Revista del CLAD Reforma y Democracia*, 7- 22.

Hamdi , K., Padilla, J. J., Vernon-Bido, D., Saikou, Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. *Journal of Cibersecurity*, 1- 13. doi:https://doi.org/10.1093/cybsec/tyab005

Hancco Arias, J. F. (2022). COMPETITIVENESS: A STRATEGIC RESOURCE-BASED APPROACH TO BUSINESS MANAGEMENT. *TECHNO Review. International Technology, Science and Society Review*, *11*(5), 1- 15. doi:10.37467/revtechno.v11.4449

Hernandez Palma, O. I. (2019). Pluralismo jurídico del siglo xxi y los derechos digitales: reflexiones en torno a la sentencia su-420 de 2019 de la Corte Constitucional Colombiana. *JUSTICIA*, *27*(41), 137- 149. Obtenido de https://doi.org/10.17081/just.27.41.5702

Hernández Peña, J. C. (2022). Campañas Electorales, Big Data y perfilado ideológico. Aproximación a su problemática desde el Derecho Fundamental a la Protección de Datos. *Revista Espanola de Derecho Constitucional*, *2022*(124), 41- 73. doi:10.18042/cepc/redc.124.02

Ivanova, L. (2023). Responsabilidad penal por delitos cibernéticos en los países BRICS. *Revista de Derecho de los BRICS., 10*(1), 59-87. doi:https://doi.org/10.21684/2412-2343-2023-10-1-59-87

Jifei, Z., Guisen, W., Yuhan, Z., Lei, C., Xiao, L., & Shouting, Z. (2024). Security issues of the gold industry chain based on smart blockchain in the context of the Internet of Things. *Scientific Reports, 14*(2728), 1-16. doi:https://doi-org.consultaremota.upb.edu.co/10.1038/s41598-024-52274-2

Jiménez-Pitre, I., Martelo, R., & Jaimes, J. (2017). Escuela de gobierno basada en TIC: Determinante para la accesibilidad e integralidad del empoderamiento digital. *Informacion Tecnologica*, *28*(5), 75- 86. doi:http://dx.doi.org/10.4067/S0718-07642017000500010

Jordi, J. (24 de abril de 2023). *La ciberdelincuencia sigue en aumento: Los ciberataques se multiplican*. Obtenido de EY: https://www.ey.com/es_es/cybersecurity/la-ciberdelicuencia-sigue-aumento-los-ciberataques-se-multiplican

Karagiannis, C., & Vergidis, K. (2021). Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information, 12*(5), 1-16. doi:https://doi.org/10.3390/info12050181

Kumar, D., Paccagnella, R., Murley, P., Hennenfent, E., Mason, J., Bates, A., & Bailey, M. (2018). Skill Squatting Attacks on Amazon Alexa. *USENIX*(27), 33-47. Obtenido de https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kumar.pdf

Kwon, T., Song, J., Jung, H., Chun, S., Lee, H., Kang, M., . . . Cho, E. (2023). How to decentralize the internet: A focus on data consolidation and user privacy. *Computer Networks*, *234*, 1-17. doi:https://doi-org.iue.basesdedatosezproxy.com/10.1016/j.comnet.2023.109911

Li, G. (2021). State control by stealth in the big data era - from WeChat to the Social Credit System in China. *Journal of Telecommunications and the Digital Economy*, *9*(4), 88- 109. Obtenido de https://search.informit.org/doi/10.3316/informit.344219843460305

Malathi, P., Suganthi, D., & Jospin, J. (2024). Intelligent encryption with improved zealous method to enhance the anonymization of public health records in cloud. *Journal of Autonomous Intelligence, 7*(1), 1-13. Obtenido de https://jai.front-sci.com/index.php/jai/article/view/567/731

Martínez López-Sáez, M. (2020). La garantía del derecho al olvido: protección de datos, retos futuros y propuestas de regulación de situaciones de vulnerabilidad en la Unión Europea. *Universidad de Valencia. Tesis Doctoral*, 1- 812. Obtenido de https://hdl.handle.net/10550/75363

MarzoratI, O. (2019). “Las nuevas tecnologías frente al blockchain y los contratos inteligentes. (Las necesidades de información de los abogados en la era online). *DECONOMI*, 1-18. Obtenido de http://www.derecho.uba.ar/publicaciones/revista-deconomi/articulos/Ed-0004-N08-MARZORATI.pdf

Medan, S. (2020). Violación del derecho a la privacidad electrónica en el derecho internacional público. *Revista Opcion, 36*(27), 663- 683.

Meištė, R., Jakštienė, S., & Lankauskienė, A. (2023). Improvement of Operational Processes by Ensuring Work Safety in Production. *Vide. Tehnologija. Resursi - Environment, Technology, Resources, 3*, 176- 182. doi:https://doi.org/10.17770/etr2023vol3.7313

Mejía Cambar, O. (2019). Análisis al reglamento General de Protección de Datos en la Unión Europea: Un Vistazo a la Actualidad de la Era Digital. *La Revista de Derecho, 40*(1), 93-104. doi:https://doi.org/10.5377/lrd.v40i1.8909

Miquel Segarra, S., & Aced, C. (2018). El rol de la comunicación interna ante los desafíos de la digitalización. *Communication Papers Media Literacy & Gender Studies, 7*(15), 27- 41.

Molero-Aranda, T., Lázaro Cantabrana, J. L., & Gisbert Cervera, M. (2023). Safety, Inclusion and Technology: A technological solution for emergency situations. *Siglo Cero, 54*(2), 11- 28. doi:10.14201/scero202354231421

Moya Vargas, M. F. (2018). Sentido de justicia y proceso penal. *Utopia y Praxis Latinoamericana, 23*(1), 50- 63. doi:10.5281/zenodo.1772686

Muñoz Flores, F., Barroso Gutiérrez, J., & García Báez, A. (2022). Estandarización digital, vulnerabilidad social y gobierno abierto: el caso de XBRL en Europa. *Revista Espanola de la Transparencia*(15), 313- 327. doi:https://doi.org/10.51915/ret.222

Oleiwi, R. (2023). La medida en que Los libros de texto cumplen los requisitos de la transformación digital en contabilidad y auditoría. *Intenational jounal of profetional business review, 8*(5), 1-12. doi:https://doi.org/10.26668/businessreview/2023.v8i5.1509

Opazo, M. (2019). ¿Es científico el discurso elaborado por la dogmática jurídica? Una defensa de la pretensión de racionalidad del discurso dogmático elaborado por la ciencia del derecho penal. *Politica Criminal, 14*(27), 549- 598. doi:10.4067/S0718-33992019000100549

Organización de las Naciones Unidas. (2019). *La era de la interdependencia digital*. Nueva York: Organizaciones de las Naciones Unidas. Obtenido de https://www.un.org/es/un75/impact-digital-technologies

Parada García, G. E. (2018). La historicidad del delito en la manualística del derecho penal colombiano. *Vniversitas, 67*(137), 1- 21. doi:10.11144/Javeriana.vj137.hdmp

Pardo Vargas, A. (2018). Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. *Universidad César Vallejo. Tesis de Maestría.*, 1- 204. Obtenido de https://hdl.handle.net/20.500.12692/20372

Parlamento Europea y Consejo de Europa. (2013). *Directiva 2013/40/UE*. Bruselas: Diario Oficial de la Unión Europea. Obtenido de https://www.boe.es/doue/2013/218/L00008-00014.pdf

Parlamento Europeo y el Consejo de la Unión Europea. (2014). *Directiva 2014/62 de 15 de mayo de 2014.* Bruselas: Diario Oficial de la Unión Europea. Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014L0062

Pérez Salazar, B. (2018). Construcción de paz en el orden del derecho transnacional penal: El caso Colombiano. *Utopia y Praxis Latinoamericana, 23*(1), 65- 78. doi:10.5281/zenodo.1772945

Pinto Rico, R. A., Hernández Medina, M. J., Pinzón Hernández, C. C., Díaz López, D. O., & García Ruíz, J. C. (2018). Inteligencia de fuentes abierta (OSINT) para operaciones de ciberseguridad. “Aplicación de OSINT en un contexto colombiano y análisis de sentimientos". *Revista Vínculos: Ciencia, Tecnología y Sociedad, 15*(2), 195- 214. doi:https://doi.org/10.14483/2322939X

Pirni, A., Giampellegrini, P., & Raffini, L. (2019). Digital transformation and egovernment. For a research agenda on the Liguria region. *OBETS, 14*(2), 471- 490. doi:10.14198/OBETS2019.14.2.07

Poy, R., & Carriegos, M. (2017). Assessment of the Recent Postgraduates in Cybersecurity on Barriers and Required Skills for Their Early Career. *In: Pérez García, H., Alfonso-Cendón, J., Sánchez González, L., Quintián, H., Corchado, E. (eds) International Joint Conference SOCO'17-CISIS'17-ICEUTE'17 León, Spain, September 6–8, 2017, Proceeding. SOCO ICEUTE CISIS 2017 2017 2017*, 6-8. doi:https://doi.org/10.1007/978-3-319-67180-2_69

Puerto, M. I., & Sferrazza Taibi, P. (2018). La sentencia Schrems del Tribunal de Justicia de la Unión Europea: Un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional. *Revista Derecho del Estado*(40), 209- 236. doi:10.18601/01229893.n40.0

Rachel, L. (2 de septiembre de 2021). *Lawsuits say Siri and Google are listening, even when they're not supposed to*. Obtenido de The Washington Post: https://www.washingtonpost.com/technology/2021/09/02/apple-siri-lawsuit-privacy/

Radanliev, P. (2024). The rise and fall of cryptocurrencies: defining the economic and social values of blockchain technologies, assessing the opportunities, and defining the financial and cybersecurity risks of the Metaverse. *Financial Innovation, 10*(1), 1-34. doi:https://doi.org/10.1186/s40854-023-00537-8

Recskó, M., & Aranyossy, M. (2024). User acceptance of social network-backed cryptocurrency: a unified theory of acceptance and use of technology (UTAUT)-based analysis. *Financial Innovation, 10*(57), 1-29. doi:https://doi.org/10.1186/s40854-023-00511-4

Red Iberoamericana de Protección de Datos. (2006). Autorregulación y Protección de Datos Personales. *Documento Elaborado por el Grupo de Trabajo reunido en Santa Cruz de la Sierra – Bolivia. Los días 3 a 5 de mayo*.

Red Iberoamericana de Protección de Datos. (2017). Estándares de Protección de Datos Personales para los Estados Iberoamericanos. *XV Encuentro Iberoamericano de Protección de Datos*, 1-34. Obtenido de https://www.redipd.org/es/documentos/estandares-iberoamericanos

Requejo Alarcón, G. (2020). Interés público y despenalización de los delitos contra el honor cometidos a través de la prensa. Una evaluación de la experiencia peruana. *Politica Criminal, 15*(30), 1009- 1051. doi:10.4067/S0718-33992020000201009

Rodríguez, Y. (2019). Inteligencia de Fuentes Abiertas (OSINT): Características, debilidades y engaño. *Revista de Estudios en Seguridad Internacional*, 1- 15.

Roncancio Bedoya, A. F., Velez Jaramillo, E. A., & Agudelo Taborda, S. (2022). Dinámicas sobre el Buen Gobierno alrededor de la Regulación del Acceso a las TICS en Colombia: El Internet como Mediador de Derechos Sociales. *Verba Iuris*, 107- 117. doi:https://doi.org/10.18041/0121-0021/verbaiuris.47.2022.XXXX

Roztocki, N., Soja, P., & Roland Weistroffer, H. (2019). The role of information and communication technologies insocioeconomic development: towards a multi-dimensional framework. *Information Technology for Development, 25*(2), 171- 183. doi:https://doi.org/10.1080/02681102.2019.1596654

Serventich, C. (2022). Inteligencia artificial en el proceso penal. ¿Más vale humano conocido o algoritmo por conocer? *Revista Juridica Austral, 3*(2), 869- 880. doi:10.26422/RJA.2022.0302.ser

Silva Aguirre, D. (2020). La imputación objetiva del nexo lógico en el tipo penal de violación de datos personales. *Universidad Autónoma de Bucaramanga*, 29-37. Obtenido de http://hdl.handle.net/20.500.12749/11897

Silva García, G., & Montoya Barreto, J. (2022). Avatares de la criminalidad de cuello blanco transnacional. *Revista Cientifica General Jose Maria Cordova, 20*(39), 609- 629. doi:10.21830/19006586.1042

Solé Ponce, J. (2023). Buen gobierno y derecho a una buena administración desde una perspectiva de calidad normativa. A propósito del libro de la profesora Maria De Benedetto, Corruption from a Regulatory Perspective. *Eunomia. Revista en Cultura de la Legalidad*(24), 377- 401. Obtenido de 10.20318/eunomia.2023.7679

Tavares, A., & Bitencourt, C. (2021). Diálogo entre o Direito e a Engenharia de Software para um novo paradigma de transparência: controle social digital. *Revista Eurolatinoamericana de Derecho Administrativo, 8*(1), 9- 34. doi:https://doi.org/10.14409/redoeda.v8i1.9676

Toscano, M. (2017). Sobre el concepto de privacidad: la relación entre privacidad e intimidad. *Revista Isegoria*(57), 533-552.

Valero, C., Pérez, J., Solera Cotanilla, S., Vega Barbas, M., Suarez Tangil, G., Alvarez Campana, M., & López, G. (2023). Analysis of security and data control in smart personal assistants from the user's perspective. *Future Generation Computer Systems, 144*, 12-23. doi:https://doi-org.iue.basesdedatosezproxy.com/10.1016/j.future.2023.02.009

Van Dijk, J., & Van Deursen , A. (2014). *Digital skills: unlocking the information society.* New York: Palgrave Macmillan.

Yanping, Z., Yang, X., Ghaboosi, K., Zhang, J., & Deng, H. (2012). A Survey of cyber crimes. *Security Comm. Networks*, 422- 437. doi:https://doi.org/10.1002/sec.331

Zaffaroni, E. R. (2009). *Estructura Básica del Derecho Penal.* Buenos Aires, Argentina: Editora AR S.A.

Zhuo, X., Irresberger, F., & Bostandzic , D. (2024). How are texts analyzed in blockchain research? A systematic literature review. *Financial Innovation, 10*(60), 1-35. doi:https://doi.org/10.1186/s40854-023-00501-6