

DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS (TÍTULO VII-BIS CÓDIGO PENAL) Y SU DESARROLLO NORMATIVO EN EL DERECHO PENAL ECONÓMICO COLOMBIANO 1991-2021
THE PROTECTION OF INFORMATION AND DATA (TITLE VII-BIS CRIMINAL CODE) AND ITS EVOLUTION IN COLOMBIAN ECONOMIC CRIMINAL LAW 1991-2021

Edgar Valencia Cardona¹

Universidad Internacional Iberoamericana, México

[edgar.valencia@doctorado.unini.edu.mx] [<https://orcid.org/0000-0003-3919-794X>]

Información del manuscrito:

Recibido/Received: 04/05/2025

Revisado/Reviewed: 11/06/2025

Aceptado/Accepted: 20/06/2025

Resumen

Palabras clave:

derecho penal económico, protección de la información y de los datos, delitos informáticos, cibernéticos o cibercrímenes y desarrollo normativo.

Este documento expone de manera detallada los resultados de la investigación contenida en Tesis Doctoral, la cual se inscribe en el marco del derecho penal económico colombiano, en la cual se analiza el desarrollo normativo del bien jurídico tutelado "Protección de la Información y de los Datos" inscrito en el Título VII-Bis del Código Penal, Ley 599 de 2000 entre 1991 y 2021, con especial énfasis en la Ley 1273 de 2009 que tipificó delitos informáticos o cibercrímenes y buscó subsanar vacíos legales previos. Se evidencia en el resultado investigativo que la legislación ha resultado insuficiente y tardía frente a las necesidades reales de la sociedad, porque estos delitos afectan tanto derechos fundamentales como la estructura económica de entidades públicas y privadas, y que las normas vigentes no han sido efectivas, pues antes de 2009 se sancionaban con normas ordinarias, lo que generaba vacíos jurídicos que aún persisten. A través de un enfoque cualitativo y de análisis histórico-hermenéutico que abarca el estudio de normas, jurisprudencia, convenios, políticas públicas y tratados internacionales adoptados por Colombia, se profundiza en la interpretación de las deficiencias, desfases y vacíos legales presentes en el marco normativo previo, permitiendo así, identificar los retos y limitaciones en la protección jurídica de la información y los datos en el contexto del derecho penal económico colombiano. Finalmente, se plasman las probables carencias inmersas en la norma y que afectan el orden económico y social, en esta medida, se recomienda actualizar el conjunto normativo para enfrentar eficazmente los retos que plantea la criminalidad informática en Colombia.

¹ Autor de correspondencia.

Abstract

Keywords:

Economic criminal law, information and protection of data, cybercrimes, cybercrimes and normative development.

This document provides a detailed account of the research findings contained in the Doctoral Thesis, which is framed within the scope of Colombian economic criminal law. It analyzes the normative development of the legally protected interest "Protección de la Información y de los Datos" Título VII-Bis del Código Penal, Ley 599 de 2000 between 1991 and 2021, with particular emphasis on Ley 1273 de 2009, which typified computer crimes or cybercrimes and sought to address previous legal gaps. The research results show that the legislation has been insufficient and delayed in meeting the real needs of society, as these crimes affect both fundamental rights and the economic structure of public and private entities. The current regulations have not been effective, since before 2009 such conduct was sanctioned under ordinary rules, which led to legal gaps that still persist. Through a qualitative and historical-hermeneutic approach, encompassing the study of laws, case law, conventions, public policies, and international treaties adopted by Colombia, the interpretation of deficiencies, mismatches, and legal gaps in the previous regulatory framework is deepened. This allows for the identification of the challenges and limitations in the legal protection of information and data within the context of Colombian economic criminal law. Finally, the probable shortcomings embedded in the regulation, which affect the economic and social order, are set out. In this regard, it is recommended to update the normative framework to effectively address the challenges posed by computer crime in Colombia.

Introducción

El presente artículo plantea como pregunta de investigación: ¿Cuál ha sido el desarrollo normativo en lo atinente a la protección de la información y de los datos (Título VII-bis Código Penal) en el derecho penal económico colombiano desde 1991 a 2021? De esta manera el estudio se enfoca en la evolución legislativa normativa y complementaria con la inclusión de la Ley 1273 de 2009 en el Código Penal (Ley 599 de 2000) como Título VII-Bis, que tipificó en el territorio colombiano los delitos informáticos, cibernéticos o ciberdelitos. En este análisis, se examina cómo las referidas reformas han permitido sancionar conductas delictivas asociadas al uso indebido de las TIC, que no estaban reguladas penalmente de manera específica.

Inicialmente, se conceptualiza sobre la clasificación de las conductas punibles o aquellos actos delictivos que involucran la intervención, manipulación e interacción con aparatos electrónicos para la transmisión de datos. Estos, se concretan cuando algunas personas aprovechan la oportunidad e ingresan o permanecen arbitrariamente en los sistemas informáticos con el propósito de cometer actos que violentan derechos fundamentales y, en otras ocasiones, atentan contra la estructura económica de organizaciones privadas y públicas, generando consecuencias significativas en ambos ámbitos. A propósito del tema, Acosta, M., Benavides, M., y García, N. (2000) en su artículo titulado delitos informáticos, impunidad organizacional y su complejidad en el mundo de los negocios, afirman que los delitos informáticos, “son actos ilícitos cometidos mediante el uso inapropiado de la tecnología, atentando contra la privacidad de la información de terceras personas”. Mas adelante, Donna (2010) plantea que esta rama del Derecho se debe estudiar junto con los delitos que lesionan o ponen en peligro la actividad reguladora del Estado en la economía y el fortalecimiento de las actividades mercantiles, el intercambio de bienes y servicios, apertura al aprendizaje y acceso de forma efectiva al conocimiento tecnológico. Complementariamente, Hernández (2009) advierte que los delitos informáticos pueden afectar la integridad, confidencialidad y disponibilidad de los sistemas informáticos, situación que se planteó en la iniciativa normativa del año 2009, la cual consistía en construir un bien jurídico específico y definir verbos rectores emanados con el avance tecnológico y la interacción informática con los seres humanos, lo que conlleva a intentar agravar las sanciones en conductas actualmente tipificadas, y en otros asuntos pretende regular comportamientos no contemplados en la ley penal ordinaria, transferidos de la creciente criminalidad, no solo con las conductas afines al uso de aparatos informáticos, sino aquellos comportamientos considerados colaterales para lograr el nivel normativo-punitivo igual o mejor a los estándares internacionales, con avances significativos en materia de control y sanción a infracciones cometidas con el uso de sistemas informáticos y la manipulación y/o tráfico de datos personales.

El estudio se apoya en teorías que destacan la complejidad y el carácter pluriofensivo de esta clase de delitos, subrayando la necesidad de adaptar el marco jurídico a los desafíos que plantea la criminalidad en el entorno digital y globalizado; Witker (2006) analiza, cómo la globalización económica ha facilitado la expansión de organizaciones criminales que operan transnacionalmente, aprovechando vacíos jurídicos, políticas criminales inadecuadas y deficiencias en sistemas penales en algunos Estados, lo que conduce a que delitos como el

tráfico de personas, narcotráfico, lavado de dinero y cibercrimen operen en múltiples jurisdicciones con impunidad relativa. También, Montalvo (2021) en “Delincuencia y delitos transnacionales facilitados por la globalización”, demuestra que el fenómeno de la integración mundial intensifica la operatividad de organizaciones criminales transnacionales.

La investigación plantea como objetivo general analizar el desarrollo y los cambios significativos en la normatividad y jurisprudencia, respecto al bien jurídicamente tutelado “De la Protección de la Información y de los Datos” (Título VII-Bis Código Penal) desde 1991 hasta 2021. Antes de la Ley 1273 de 2009, los delitos informáticos en Colombia eran tratados bajo la categoría de “delitos contra el patrimonio económico” (Nieto & Mejía, 2009). Como lo señalan Correa y Davara (2017) la ausencia de una tipificación específica para conductas como el phishing resultaba en la imposición de penas mínimas, evidenciando la insuficiencia del marco legal para afrontar los desafíos que plantean los crímenes tecnológicos en un entorno globalizado, donde las redes criminales aprovechan tanto los avances tecnológicos como los flujos económicos transfronterizos. Acto seguido, se despliegan cuatro objetivos específicos: en primer lugar, identificar y describir la génesis del bien jurídicamente tutelado en el ámbito constitucional mediante un análisis histórico y comparativo; en segundo término, analizar el desarrollo normativo y las reformas legislativas que han incidido en su configuración dentro del ordenamiento jurídico; en tercer lugar, examinar la jurisprudencia relevante emitida por las altas cortes respecto a su interpretación y aplicación, finalmente evaluar los avances normativos en materia de protección de la información y los datos en el contexto del derecho penal económico interno, identificando los principales desafíos contemporáneos.

Como preámbulo a la revisión literaria (capítulo II) se pretende contextualizar al lector sobre la génesis y desarrollo científico de los aparatos electrónicos para la transmisión de datos, explorando tanto su evolución histórica y los periodos en que surgieron, como los avances en los sistemas y la ciencia informática, tanto a nivel global como regional. Asimismo, se abordará el origen y la expansión de Internet y las TIC, cuyo crecimiento ha propiciado la aparición de nuevas modalidades delictivas. Se profundiza en la conceptualización y clasificación de los delitos informáticos o cibercrímenes, destacando su impacto en la intimidad y el patrimonio económico, entre otros bienes jurídicos, lo que permitirá una comprensión más sólida del enfoque propuesto en este trabajo. Junto con los antecedentes se ilustrará a través de un análisis exhaustivo, los diferentes aportes teóricos que dan sustento al estudio con el cual se pretende identificar el desarrollo del marco normativo legal y complementario del bien jurídico tutelado.

Posteriormente se abordarán y conceptualizará las categorías y/o tipos de delitos informáticos o cibercrímenes identificados a nivel global y regional hasta la fecha, al igual que se dará a conocer los organismos que protegen a las personas frente a las conductas ilícitas conocidas como delitos informáticos, conociendo el origen, concepto, antecedentes y evolución del derecho penal económico a nivel global y regional, destacando la estrecha relación entre el desarrollo de la informática y la necesidad de actualizar los marcos normativos. En este contexto, se resalta la importancia del Título VII-Bis del Código Penal colombiano como respuesta normativa a los desafíos que plantea la criminalidad informática en una sociedad cada vez más digitalizada.

Justificación

En Colombia, dentro del contexto del conocimiento científico económico penal colombiano cuyo desarrollo normativo legal y complementario se haya sustentada en reglas y principios generales que irradian en la estructura del entramado dogmático-jurídico punitivo, ha llamado la atención a autores como Acosta, (2020) quien examina la evolución y efectividad de la legislación nacional frente a esta problemática que exige tener como punto de partida conocer cuáles fueron las primeras conductas delictivas de este tipo. Por lo que se tiene como referencia que las mismas se originaron a inicios de los años 90, época en la cual se introduce la informática en Colombia y se empieza el mercadeo de software y hardware, en consecuencia, las conductas atentatorias al bien jurídicamente protegido, se intensifica en gran medida con la manipulación de instrumentos y herramientas informáticas y la consecuente coexistencia con el Internet en casi todos los lugares del territorio colombiano.

Ante esta necesidad y con base en el momento procesal penal coexistente en nuestra sociedad, el legislador observa la necesidad de expedir normatividad complementaria sancionatoria a conductas perturbadoras atentatorias a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos incorporadas en el imaginario colectivo, como delitos informáticos, cibernéticos o cibercrímenes; comportamientos concretados con la intervención, la manipulación e interacción de las TIC, ya sea lugares de trabajo, vivienda, educativos y otros, donde individuos con conocimientos avanzados o no en computación, ingresan arbitrariamente a los sistemas informáticos de forma abusiva, con la firme idea de cometer actos ilegales contra la estructura económica, organizaciones privadas y públicas, empresas y/o a uno o más individuos, tal como lo señalan Acosta, Benavides, Merck y otros (2020).

A partir del año 2009, se regulan de forma inicial los comportamientos anómalos, producto del avance tecnológico o los llamados delitos cibernéticos, informáticos o cibercrímenes a través de la Ley 1273 de 2009 con la cual, se intenta dar posibles soluciones a afectaciones derivadas de conductas ilícitas vinculadas al contexto empresarial, industrial y comercial. Esta normatividad sancionatoria de carácter común u ordinario que, a su vez, enfrenta manifestaciones delictivas estudiadas a partir de la teoría del delito enmarcado intrínsecamente en el entramado del Derecho Penal nuclear, que subsana parcialmente el vacío jurídico normativo relacionado con conductas delictivas que aún persisten con la utilización (en algunas ocasiones incorrectamente) de las TIC, generando con esto, legitimidad en su protección a través del Derecho Penal colombiano (Vargas, C., 2018).

Según Arévalo, S. (2021) en su documento "Prevención delitos informáticos", las conductas ilícitas surgidas con Internet afectan especialmente a menores de edad y vulneran sus derechos, lo que evidencia la necesidad de actualizar la legislación colombiana para responder a las nuevas formas de criminalidad tales como el ciberacoso o cyberbullying, el grooming, el phishing, la pornografía infantil, el sexting y el skimming, enfatizando en la importancia de la prevención, para lo cual, proporciona información sobre herramientas y métodos de protección contra estos delitos informáticos. Por su parte, Camargo, L. (2021), en "Regulación en Colombia de los delitos informáticos" expone la evolución y el marco conceptual de estas conductas, allí afirma que las TIC han facilitado la comisión de estos delitos y generado un amplio campo de riesgos, por lo que se propone definir y catalogarlos como fraudes informáticos, sabotaje informático, posesión de software malicioso, acceso no

autorizado y revelación de secretos, suplantación de identidad, espionaje informático, acceso ilícito a sistemas informáticos, estafas para obtener datos, entre otros. Da cuenta que, para las autoridades, es difícil demostrar la comisión de estos ciberdelitos y la presentación de innumerables contratiempos para recolectar pruebas, ya que las antedichas conductas punibles, se pueden ejecutar de forma rápida y fácil, esto también complica identificar al responsable del hecho. Finalmente, identifica factores que incrementan la vulnerabilidad de los usuarios frente a los cibercriminales, tales como el descuido, falta de tomar precauciones mínimas (Ej. antivirus), el uso de contraseñas débiles y conexión a redes públicas para realizar transacciones. Como señala Miró (2012) las conductas delictivas cometidas a través de las tecnologías de la información y la comunicación forman parte de la realidad criminológica actual, destacando la aparición de nuevas formas de vulnerar la intimidad y el patrimonio de las personas, que se valen de la ingeniería social, especialmente mediante delitos como el fraude informático como el Scams (con pérdida de dinero) el Hoax (cuando solo hay engaño) el Phishing (hurto de información) el Pharming (direccionamiento a un sitio web fraudulento) estas formas de delincuencia cibernéticas surgen con el fin de aprovechar la transnacionalidad de Internet para atacar intereses patrimoniales y personales a través del ciberracismo o el ciberterrorismo.

Es oportuno destacar, que el estudio desarrollado en la presente tesis está íntimamente relacionado con el derecho penal económico colombiano, puesto que el eje principal del mismo se consolidará en la protección de la información y de los datos y su desarrollo normativo en el campo del derecho penal económico colombiano desde 1991 hasta 2021. Por lo que resulta relevante conocer que en nuestro medio jurídico existe referencia acerca del concepto de esta rama del derecho punitivo, propuesto como el conjunto de normas tutelantes del bien jurídico del orden económico de los Estados, que en sentido estricto se debe entender como la regulación jurídica del intervencionismo estatal en la economía, (Agustia, J., y Vargas, M., 2019) y que pretende dar solución a los conflictos suscitados dentro del ámbito de producción, distribución y acceso de los comerciantes, fabricantes y consumidores de bienes y servicios, considerando que su intención va dirigida a generar equilibrio entre la comisión ilícita y su posterior castigo o sanción. Abadías, A., y Bustos M. (2020) en la obra “Temas prácticos para el estudio del derecho penal económico” nos dice: “Esta especialidad del Derecho tiene la función de proteger a la sociedad de delitos societarios, fiscales, estafas, delitos contra el patrimonio, contra los consumidores, la financiación ilegal de partidos, el cohecho, malversación, prevaricación administrativa, blanqueo de capitales, tráfico de influencias, corrupción empresarial, estafas piramidales” y que además, el derecho penal económico estudia la responsabilidad penal de las personas jurídicas, toda vez que comporta características propias para investigar y sancionar actos delictivos de connotación particular, como es el caso de las conductas delictivas ya tratadas, que si bien, la tipificación se incorpora en el derecho penal nuclear con las adiciones ya conocidas, los procedimientos acostumbrados para la judicialización de los responsables requieren del ente acusador y los investigadores asignados para cada caso, tener conocimientos propios en la disciplina informática.

Por otra parte, se infiere que la regulación incorporada al derecho penal ordinario en el año 2009, relacionada con la ya citada protección de la información y de los datos, no puede ser entendida como instrumento desestimulante del desarrollo empresarial, comercial o industrial de la sociedad, Ortiz de Urbina, E., (2020) el autor afirma que al precisar los tipos

penales, la antijuridicidad y sanción correspondiente a dichas conductas, se busca una legitimación por parte del derecho sancionador de tipo ético-jurídico. En este sentido, el derecho penal económico y el derecho penal ordinario persiguen fines regulatorios, por lo cual, la legitimación del primero será válida en la disposición que satisfaga los criterios de legitimidad del segundo, en cuanto a la culpabilidad del autor, dado que, el injusto en uno, debe estar en el mismo plano y/o sentido del otro para que conlleve, consecuentemente una sanción equitativa y justa frente a la sociedad.

El aporte y la relevancia para la comunidad académica se da, de manera significativa al analizar de forma integral la evolución normativa y la protección penal a la información y de los datos entre 1991-2021, en cuanto al marco normativo, la expedición de leyes y demás normas complementarias, especialmente, en lo concerniente al bien jurídico tutelado: “De la Protección de la Información y de los Datos” (Título VII-bis del Código Penal colombiano). Este análisis que abarca tanto el desarrollo legislativo como las perspectivas doctrinales y jurisprudenciales provee insumos valiosos para la academia y la formulación de políticas públicas, al evidenciar situaciones en las cuales el derecho penal económico protege, ampara y brinda seguridad jurídica, a través del conjunto normativo punible producto del desarrollo sistemático de esta vertiente del derecho. Consecuente con esto, se identificarán los vacíos, desfases y retos en la legislación frente al auge de estas conductas y la globalización; ya que su relevancia radica en comprobar cómo la respuesta legal ha sido insuficiente para enfrentar las nuevas formas de criminalidad tecnológica y así, contribuir a la estructuración del procedimiento metodológico planteado, de modo que agregue insumo importante para avanzar socialmente en la identificación punitiva emergente en el seno de la comunidad cibernética, donde es imprescindible la utilización de herramientas y aparatos electrónico e informáticos de todo orden.

Los motivos personales que conducen a la elección del presente tema de investigación consignado en la tesis de doctorado en Derecho Económico y de la Empresa, se da gracias a la importancia de concientizar en el imaginario colectivo de quienes se interesen en el impacto y desarrollo digital en nuestro territorio, el cual logró transformar a partir de la década de los 90, el entorno social físico y real hasta convertirlo en algo virtual, toda vez que los aparatos electrónicos hacen parte de la cotidianidad de los seres humanos y el uso de los mismos, que en la mayoría de ocasiones por descuidos de los usuarios conducen a generar amenazas y vulnerabilidades, afectando el patrimonio económico de ellos, de empresas y/o agrupaciones económicas.

Metodología

Con el propósito de desarrollar los parámetros trazados y siguiendo la línea de razonamiento del enfoque metodológico, resulta esencial que el marco estratégico de la investigación sea coherente y práctico para abordar eficazmente el problema y alcanzar los objetivos propuestos. En este sentido, el diseño de la investigación se inscribe en el paradigma cualitativo, la cual se centra en comprender y explorar la realidad normativa punitiva en cuanto a la protección de la información y de los datos conforme a lo dispuesto en el Título VII-bis Código Penal, en el contexto del derecho penal económico colombiano entre 1991 y 2021. Desde la perspectiva interpretativa y naturalista, el enfoque busca captar

y describir fenómenos sociales, culturales y humanos en su contexto natural, evitando reducirlos a variables numéricas. Arias (2012), en la obra: "El Proyecto de Investigación: Introducción a la Metodología Científica", sostiene que las investigaciones documentales y bibliográficas, el análisis básico consiste en descomponer la información en ideas principales y secundarias, para identificar vínculos e implicaciones y a la vez, traducir o descifrar el sentido de estas, percibiendo los acontecimientos de forma acertada. Igualmente anota, que la investigación bibliográfica es un diseño documental que se apoya en fuentes secundarias, como libros y artículos, para recopilar, seleccionar y analizar información de forma sistemática. En la misma línea, Hernández-Sampieri, Fernández-Collado y Baptista-Lucio (2014) en la sexta edición de "Metodología de la investigación" sostienen que el enfoque cualitativo recurre a la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación. En consecuencia, dentro del trabajo investigativo, se procederá a recopilar y analizar los instrumentos normativos expedidos por el legislador colombiano en lo referente al desarrollo normativo del bien jurídico tutelado.

El diseño no experimental transversal seleccionado en este proceso es procedente y conduce a definir el paradigma de análisis que surge para comprender los fenómenos que atañen al derecho penal económico. Se adopta un enfoque explicativo, orientado a identificar y analizar las posibles deficiencias de la norma penal ordinaria que sirve de sustento para el reconocimiento y la aplicación del derecho penal económico en materia de la protección de la información y de los datos. Este tipo de investigación es pertinente ya que se estudian fenómenos nuevos o poco explorados, centrándose en los detalles y particularidades, para que finalmente, se generen conclusiones sólidas y determinantes sobre la cuestión de estudio.

Como complemento de este proceso metodológico, se suma a la presente investigación la aplicación de los métodos histórico-jurídico y exploratorio jurídico, en donde, el primero, permite enfocar la pregunta de investigación en la sucesión evolutiva de los aspectos generales del desarrollo normativo del bien jurídico tutelado "De la Protección de la Información y de los Datos", analizando la sucesión de disposiciones legales y demás normas complementarias tipificadas en el Título VII-Bis Código Penal (Ley 599,2000).

De esta manera, el método histórico-lógico es una herramienta que permite entender el objeto de estudio en su evolución histórica, destacando sus aspectos generales y tendencias de desarrollo, el cual es fundamental para revelar la génesis y evolución de instituciones y normas jurídicas, así como para comprender la formación de los sistemas jurídicos, como lo señala Villabella (2020), es fundamental para comprender el origen y evolución de las instituciones y normas jurídicas, así como para identificar las tendencias y transformaciones que han dado forma a los sistemas jurídicos.

Por su parte, el método exploratorio jurídico se orienta al análisis de temas normativos poco estudiados o novedosos, permitiendo identificar vacíos y aspectos no abordados previamente en el derecho, y proporcionando una visión preliminar que podrá ser profundizada posteriormente mediante enfoques descriptivos o explicativos. Esta combinación metodológica, permitirá develar una visión integral y crítica acerca de las carencias, los desfases o los vicios legales que pueda tener la norma cuando se trata de aplicarla a la realidad.

La población objeto del estudio investigativo comprende el conjunto normativo y su desarrollo legislativo desde 1991 a 2021 en cuanto al tema de la protección de la información y de los datos. Para la recolección de datos e información necesaria para lograr los objetivos trazados se acudió inicialmente a fuentes especializadas como bases de datos académicas, revistas científicas, trabajos y monografías de grado, entre otros. De la misma forma, se compiló información de fuentes primarias como Constitución Política de Colombia de 1991, Ley 599 de 2000, Ley 1273 de 2009 y Ley 1581 de 2012 y otras normas complementarias, sumado a las Gacetas del Congreso de la República y boletines de la Corte Constitucional, de los cuales se extrajo la jurisprudencia (Sentencias o Fallos) como también, los Tratados y Convenios ratificados por Colombia y las políticas públicas relacionadas con la protección de datos. Todo lo anterior, disponible y sin restricción de acuerdo con lo preceptuado en la Ley 1712 de 2014 que trata sobre la transparencia y derecho de acceso a la información pública en Colombia. Adicionalmente, se contempla consultar información relevante publicada en sitios web de organismos internacionales, regionales y locales que contengan temas relacionados con el derecho penal económico y los delitos informáticos.

La información recolectada se obtuvo mediante análisis de fuentes primarias y secundarias de tipo documental, bibliográfica y electrónicas con la utilización de herramientas denominada fichas de registro de datos, ante lo cual se procede a observar de forma directa la misma, esto, de acuerdo con lo planteado por Marshall y Rossman (1989) lo cual implica una observación sistemática de “eventos, comportamientos y artefactos en el escenario social elegido para ser estudiado”. Tras la aplicación de esta técnica, se procede a elaborar las plantillas estructuradas que consolide la información clara y objetiva, las cuales serán procesadas, logrando así, los resultados esperados que se incorporarán en el correspondiente trabajo investigativo.

Durante la realización de la investigación se emplea el muestreo probabilístico, acudiendo a la selección representativa que ha dado lugar al desarrollo normativo del bien jurídico relacionados con el objeto de estudio, lo cual ofrece mejor oportunidad de crear una muestra fiable y representativa y así lograr mayor precisión en los resultados, esto, en concordancia con lo expuesto por Salamanca-Crespo y Martín-Crespo (2007) quienes afirman que el muestreo probabilístico es “el mejor modo de obtener los datos” ya que son “decisiones que se toman en el campo, pues queremos reflejar la realidad y los diversos puntos de vista de los participantes, los cuales nos resultan desconocidos al iniciar el estudio”. Este enfoque permite una comprensión profunda y contextualizada de los fenómenos estudiados. En conclusión, la selección adecuada y congruente de información sobre la población requerida en este trabajo investigativo, especialmente en lo relacionado con el ámbito legal, exige una cuidadosa consideración en el manejo de las normativas vigentes, ya que el marco legal establece principios como la transparencia y la circulación restringida de los datos, asegurando que los procedimientos de recolección, tratamiento y uso, respeten los derechos fundamentales y protejan la privacidad de los individuos, lo que refuerza la validez ética del producto de la investigación.

Resultados

Con la finalidad de lograr los resultados esperados en esta investigación cualitativa, se recurre al proceso de categorización de la información recolectada, ya que este procedimiento permite identificar temas relevantes, eventos recurrentes y patrones de ideas dentro de los datos, facilitando su análisis e interpretación. Las categorías funcionan como agrupaciones conceptuales que reúnen elementos con características comunes, lo que contribuye a reducir, organizar y estructurar la información de manera que sea más manejable y comprensible para el investigador. Así, la categorización se consolida como un proceso cognitivo y organizativo esencial, que implica clasificar y agrupar conceptos o información en función de criterios o características compartidas, optimizando el abordaje y la comprensión del fenómeno estudiado. Es postura respaldada por Lakoff, (1987) en su obra “Fundamental women, fire and dangerous things” quien argumenta que la categorización es un proceso activo y fundamental para el pensamiento, la percepción, la acción y el lenguaje, toda vez que comprendemos o producimos enunciados, estamos utilizando categorías lingüísticas y conceptuales, y en este proceso dinámico, flexible y dependiente de la experiencia, los prototipos juegan un papel importante ya que abren una puerta a la comprensión compleja y realista de la mente humana.

Tomando como base el planteamiento anterior y considerando la necesidad de estructurar el análisis del desarrollo investigativo, se propone la aplicación del proceso de categorización para abordar de manera amplia los aspectos normativos, tecnológicos y jurídicos implicados.

Categorías

Categoría 1: Desarrollo del bien jurídico tutelado “de la protección de la información y de los datos” (1991-2021)

Subcategorías:

- a) *Desarrollo Constitucional.* Se refiere al conjunto de disposiciones constitucionales diseñadas para proteger las garantías y derechos de las personas, especialmente en lo que respecta a las posibles vulneraciones en cuanto a la dignidad humana y demás derechos fundamentales. Se encuentra preceptuados en los artículos 15, 21, 42, 44 y 74 de la Carta Magna de 1991.
- b) *Desarrollo normativo.* Se refiere a la evolución de las normas tales como Leyes, Decretos y demás disposiciones en lo que respecta a la protección de la información y los datos personales, impulsado por la necesidad de adaptar y apropiar las leyes a los avances tecnológicos y a las nuevas formas de delincuencia, asegurando con esto la protección de los derechos fundamentales relacionados con la privacidad y el manejo de datos personales. Entre otras normas encontramos: Ley 527-1999; Ley 599-2000; Ley 679-2001; Ley 962-2006; Ley 1032-2006; Ley 1266-2008; Ley 1273-2009; Ley 1336-2009; Ley 1581-2012; Decreto 1727-2009; Decreto 2952-2010; Decreto 1377 de 2013.
- c) *Desarrollo jurisprudencial.* Se concreta con la expedición de Fallos o Sentencias de la Corte Constitucional en la toma de decisiones judiciales, haciendo énfasis en el derecho a la protección de datos personales y el derecho al Habeas Data, el cual

ha sido decisivo para definir las prerrogativas de los titulares de datos personales a conocer, actualizar y rectificar su información en bases de datos públicas y privadas. Algunos ejemplos son: T-414/1992; SU-082/1995; C-748/2011; T-050-2016 entre otras.

- d) *Desarrollo a nivel de tratados y convenios internacionales ratificados por Colombia.* Refleja el compromiso del Estado colombiano con la protección de los datos personales y la privacidad adaptando su legislación a las exigencias del entorno digital global contemporáneo frente a la vulneración por parte de bandas ciberdelictivas, al adherirse al convenio de Budapest, y así garantizar el respeto a los derechos fundamentales relacionados con la información personal en un contexto global.
- e) *Desarrollo a nivel de Políticas Públicas internas.* El desarrollo de Políticas Públicas en Colombia, que hace referencia al tema de la protección de la información y de los datos (1991 y 2021) ha evolucionado a través de los documentos CONPES 3920-2018 que estableció la política nacional de explotación de datos (Big Data), el CONPES 3701-2011 "Lineamientos de política para ciberseguridad y ciberdefensa", el CONPES 3854-2016 que establece la "Política nacional de seguridad digital" y el CONPES 3995-2020 sobre la "política nacional de confianza y seguridad digital en Colombia".

Categoría 2: Análisis de la protección legal de la información y datos

Subcategorías:

- a) *Protección de la información y datos.* Es el conjunto de habilidades, medidas y normatividad para proteger la información personal y sensible contra accesos no autorizados, hurto y en general todo acto de inseguridad o comprometimiento de la información personal o empresarial. Lo anterior, con la finalidad de tomar medidas para proteger su integridad contra manipulación o ataques con malware o virus informáticos.
- b) *Clasificación de datos.* Proceso mediante el cual se organizan y categorizan los datos personales o de una organización privada o pública, según su nivel de sensibilidad, confidencialidad, importancia o relevancia. Esto es fundamental para la gestión de la información y la ciberseguridad, permitiendo determinar qué medidas de protección deben aplicarse a cada tipo de dato, con el cumplimiento normativo y estándares internacionales que finalmente mitiga e identifica el riesgo asociado con la pérdida o el acceso no autorizado a la información.
- c) *Seguridad de datos.* Es la práctica de proteger la información digital contra accesos no autorizados, hurtos y en general otras amenazas durante todo el ciclo de vida, ya que su finalidad es individualizar quien o quienes pueden ver o manipular los datos, limitando el acceso a personas autorizadas mediante autenticación y autorización, de esta forma salvaguarda, tanto la integridad como la confidencialidad y disponibilidad de los datos.
- d) *Tecnología y delito.* Se refieren a la confluencia entre las actividades delictivas y los avances tecnológicos en la medida en que pueden afectar la seguridad, la privacidad, la propiedad intelectual o el patrimonio de individuos, empresas o

Estados. Ahí se hace necesario desarrollar normatividad y protocolos investigativos para prevenir y combatir las vulnerabilidades de los sistemas informáticos y redes de interconexión.

Categoría 3: Delitos económicos

Subcategorías:

- a) *Análisis de los delitos económicos relacionados con la tecnología.* El análisis identifica delitos comunes cometidos con fines económicos con la intermediación de aparatos tecnológicos, para afectar el patrimonio de terceros, destacando la necesidad de desarrollar estrategias efectivas para combatir tales conductas delictivas en un mundo cada vez más digitalizado.
- b) *Impacto de los delitos económicos en el patrimonio económico.* Se refiere al impacto negativo que pueden originar al momento de afectar tanto a nivel microeconómico, como macroeconómico, por lo que estas acciones conllevan consecuencias sobre el patrimonio de individuos, empresas y los Estados, al igual que la economía en general, conduciendo a generar falta de confianza en las instituciones financieras y en el sistema económico y a la vez, repercutiendo en la inversión extranjera directa e indirecta.
- c) *Influencia de la globalización en la aparición de nuevos delitos.* Se da dentro de los procesos de globalización y la manera como han facilitado la creación y expansión de formas novedosas de criminalidad, con la intervención de las TIC las cuales han facilitado espacios para el crecimiento de redes criminales organizadas que operan a nivel internacional a través de la red de Internet, donde la globalización ha creado nuevos mercados para bienes y servicios ilícitos, como drogas, armas y tráfico de órganos humano, entre otros.

Categoría 4: Derecho penal económico

Subcategorías:

- a) *Contextualización del derecho penal económico en el marco jurídico colombiano.* Se centra en la protección de bienes jurídicos supraindividuales, como el orden económico y social, mediante sanciones penales, logrando a través del derecho penal económico, la garantía y seguridad en las interacciones comerciales entre individuos y en algunas ocasiones entre el Estado y otros actores, frente a situaciones relacionadas con actividades delictivas contra el patrimonio económico, el orden económico social y la administración pública.
- b) *Relación del derecho penal económico con delitos informáticos y/o cibercrímenes.* Se basa en la confluencia entre las actividades delictivas que afectan el orden económico y social y aquellas que se cometen mediante el uso de TIC, que a la postre tienen un impacto directo en el patrimonio económico de personas, empresas y el Estado, por lo que se hace necesario desarrollar la legislación efectiva, eficaz y pertinente.
- c) *Influencia del derecho penal económico en la globalización y tecnología.* Se manifiesta, en cómo el derecho penal económico debe proteger el orden económico en general frente a las amenazas (prácticas desleales y fraudulentas) que representan tanto la globalización como las tecnologías en evolución constante, la cual debe incluir la regulación jurídica de actividades económicas y la protección

contra esas fuerzas que han transformado el panorama delictivo a medida que el mundo se ha vuelto más interconectado y digitalizado.

Análisis de los datos

Para alcanzar los objetivos trazados en esta investigación, se implementó la técnica de revisión y análisis documental como método principal para la recolección de información. Según Corbetta (2007) quien afirma que el análisis documental es una de las herramientas más apropiadas para la recolección de datos en documentos o material judicial, debido a la naturaleza de este, toda vez que “un documento es un material informativo sobre un determinado fenómeno social que existe con independencia del investigador”. Esta técnica posibilita una aproximación sistemática y rigurosa a la realidad estudiada, facilitando la interpretación y comprensión de los hechos a través del análisis de fuentes primarias y secundarias, lo que resulta especialmente pertinente cuando se abordan temas jurídicos o institucionales. Marshall y Rossman (1989) definen el análisis de datos como “la descripción sistemática de eventos, comportamientos y artefactos en el escenario social elegido para ser estudiado”. Por lo tanto, deviene que una vez se aplique la correspondiente técnica enfocada a explorar las implicaciones jurídicas dirigidas a observar los cambios normativos se procederá a elaborar los registros correspondientes que contenga la información clara y objetiva, con la finalidad de lograr las metas trazadas.

Se llevaron a cabo los siguientes pasos:

Primero. Recopilación y organización de datos e información, la cual consiste en relacionar los preceptos constitucionales; al igual que la normatividad (leyes y Decretos) expedidos por el legislador y el gobierno nacional, antes y después de la promulgación de la Constitución Política de 1991; la Jurisprudencia relevante; los documentos de Política Pública (documentos CONPES); y los Tratados y Convenios suscritos por el Estado colombiano. Estos aspectos contextuales y normativos son extraídos de las fuentes primarias como la Constitución Política de Colombia, Código Penal colombiano, leyes complementarias, revisión jurisprudencial de la Corte Constitucional los cuales servirán para fundamentar la presente propuesta y la planificación metodológica con la cual se elaborará una clasificación cronológica, con la finalidad de organizar los datos recopilados en una línea de tiempo, identificando los hitos legislativos y jurisprudenciales más importantes.

Segundo. Se realizó análisis de contenido, donde se examina detalladamente los preceptos jurídicos de cada ley o sentencia relevante, identificando los cambios y evoluciones en la protección de la información y los datos.

Tercero. Se analizó e identificaron las tendencias, los avances y desarrollo normativo en cuanto al bien jurídicamente tutelado.

Cuarto. Se hizo comparación con estándares internacionales, donde se contrastaron las normas colombianas frente a instrumentos ratificados por Colombia en materia de protección de datos, información y delitos informáticos.

Quinto. Se realizó un análisis estadístico, allí se examinaron los datos descriptivos sobre la aplicación de estas normas en el contexto del derecho penal económico en Colombia.

Sexto. Se llevó a cabo, interpretación de resultados y evaluación de los hallazgos en el contexto del derecho penal económico colombiano, analizando la efectividad y las implicaciones de los cambios normativos hasta el año 2021, logrando a través del análisis con

enfoque cualitativo conocer cómo se implementaron los nuevos tipos penales en la legislación punitiva, con la finalidad de verificar si han respondido eficazmente a contrarrestar el accionar delincencial en nuestro territorio.

Conclusiones

Las implicaciones de esta tesis doctoral resaltan la necesidad de fortalecer y actualizar el marco normativo colombiano para enfrentar los retos de la criminalidad informática y la protección de datos en la era digital, lo que requiere revisar la legislación y adoptar estándares internacionales que permitan respuestas más efectivas y coordinadas. Así mismo la investigación subraya la necesidad de articular políticas públicas, cooperación internacional y estrategias penales que se adapten a la dinámica tecnológica, aportando insumos valiosos para el debate académico y la formación en derecho penal económico, motivando a los operadores jurídicos y legisladores a repensar el papel del derecho penal económico como herramienta de protección social y económica en un contexto de transformación digital y global a futuro.

De este modo, el producto de la investigación evidencia el desarrollo normativo del bien jurídico tutelado: “De la Protección de la Información y de los Datos” en el contexto del derecho penal económico colombiano, desde 1991 hasta el año 2021, el cual ha experimentado una evolución progresiva orientada a abordar los desafíos de la cibercriminalidad, sin embargo, la creciente preocupación global y local por el aumento de los ciberdelitos, sugiere la necesidad de una revisión continua y fortalecimiento del marco legal para proteger adecuadamente los derechos fundamentales y la estructura económica de las organizaciones, ya que persisten desafíos importantes que pueden ser aprovechados por la criminalidad organizada que ha impulsado la creación de normas y mecanismos de protección de la información y los datos personales, persisten desafíos derivados de la rápida evolución de las TIC, la inteligencia artificial y la masificación de dispositivos electrónicos. A pesar de estos desafíos la protección de derechos como la intimidad, el buen nombre y el Habeas Data están garantizados constitucionalmente y regulados por normas que exigen el manejo adecuado de la información tanto en el sector público como privado.

Se concluye que el desarrollo normativo en torno a la protección de la información y de los datos, evidencia que ha evolucionado de manera limitada en respuesta jurídica frente a los desafíos que plantea la cibercriminalidad, ya que necesitó de la vía jurisprudencial y de constantes interpretaciones para lograr dar alcance a los retos presentados y a las nuevas modalidades ilícitas, esto se releja en el estudio socio-jurídico (2019) diez años después de promulgada la Ley de delitos informáticos en Colombia (Ley 1273 de 2009) donde se demuestra que, si bien dicha ley representó un avance en la protección frente a los delitos informáticos, persiste la necesidad de actualizar y fortalecer continuamente el marco legal para garantizar una protección efectiva frente a las nuevas formas de criminalidad, consolidando así el papel de la normativa como instrumento esencial para la defensa de los derechos fundamentales y la estabilidad del orden económico en el entorno digital.

Finalmente, es importante destacar que el análisis comparativo de los marcos normativos para la protección de datos personales en América Latina revela que, en la era digital, este tema ha adquirido una relevancia sin precedentes, impulsando a los países de la

región a desarrollar y fortalecer regulaciones específicas orientadas a salvaguardar la privacidad y los derechos de sus ciudadanos frente a los desafíos tecnológicos y las nuevas amenazas en el manejo de la información personal, ya que Argentina fue pionera con la Ley 25.326 de 2000, que está siendo revisada para alinearse con el Reglamento General de Protección de Datos (RGPD) europeo. Brasil promulgó la Ley General de Protección de Datos (LGPD) en 2018, inspirada en el RGPD, y elevó la protección de datos a un derecho fundamental en su Constitución en 2022. Chile está reformando su legislación para adaptarse a estándares internacionales. Ecuador implementó la Ley Orgánica de Protección de Datos Personales en 2021. En México, existen dos leyes fundamentales que regulan la protección de datos personales, cada una enfocada en ámbitos distintos, una Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP de jul-5-2010) y otra, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSSO de 2017), Perú, dispone de la Ley de Protección de Datos Personales (LDPD) No.29733 de 2011 (vigencia-2013). Paraguay, implementó la Ley 6.534 de 2020 "De Protección de Datos Personales Crediticios" (vigencia oct-28-2020). Uruguay, cuenta con la Ley No.18.331 de Protección de Datos Personales y Acción de "Habeas Data". Venezuela, presenta un caso particular, ya que no cuenta con una ley específica de protección de datos personales, Sin embargo, cuenta con la Ley Sobre Protección a la Privacidad de las Comunicaciones, que busca proteger la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones entre personas.

Referencias

- Abadías Selma, A., & Bustos Rubio, M. (2020). *Temas prácticos para el estudio del Derecho penal económico*. Ed. Colex. <https://dialnet.unirioja.es/servlet/libro?codigo=776981>.
- Acosta, M., Benavidez Merck, M. & García, P. (2020). Cybercrime: Impunity organizational and its complexity in the business of the world (Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios). *Revista Venezolana de Gerencia*, 25 (89).
- Agustia, J., y Vargas Ovalle, M. (2019). derecho penal económico y de la Empresa Universidad de Cataluña. <https://dialnet.unirioja.es/servlet/autor?codigo=2450175>
- Almanza Gutierrez, J. (2015). La nueva concepción del delito económico en México y la aparición de la persona jurídica privada como sujeto activo; para el caso del Estado de Puebla. <https://hdl.handle.net/20.500.12371/9501>
- Arévalo Fonseca, S. J. (2022). *Prevención en delitos informáticos*. Fundación Universitaria San Mateo. <https://cipres.sanmateo.edu.co/ojs/index.php/libros/article/view/545>.
- Arias, F. (2012). *El proyecto de investigación: Introducción a la metodología científica* (6ª ed.). Editorial Episteme.
- Camargo Cardona, L. (s.f.). *Regulación de los delitos informáticos en Colombia*. Universidad Piloto de Colombia. <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/5727/Articulo%20regulaci%C3%B3n%20delitos%20informaticos%20en%20Colombia.pdf?sequence=1>

- Congreso de la República de Colombia. (2000). Ley 599 de 2000. Por la cual se expide el Código Penal. *Diario Oficial*. <https://www.suin-juriscol.gov.co/viewDocument.asp?id=1663230>
- Congreso de la República de Colombia. (2008, diciembre 31). Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de información financiera y comercial. *Diario Oficial*. <https://www.suin-juriscol.gov.co/viewDocument.asp?id=1676616>
- Congreso de la República de Colombia. (2012, octubre 17). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. *Diario Oficial* <https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507>
- Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia. Budapest. https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF.
- Consejo de Europa. (1973). Resolución (74) 29 Protección de los datos personales y la función normativa del Consejo De Europa. <https://rm.coe.int/16804d1c51>
- Consejo Superior de política criminal. <https://www.politicacriminal.gov.co/Instancias/Consejo-Superior-de-Pol%C3%ADtica-Criminal/Qu%C3%A9-es-el-CSPC>
- Constitución Política de Colombia de 1991. Gaceta Constitucional 116 del 20 de julio de 1991. http://www.secretariassenado.gov.co/senado/basedoc/constitucion_politica_1991.html
- Corte Constitucional de Colombia. (1993, 2 de diciembre). Sentencia C-488 de 1993. M.P.: Vladimiro Naranjo Mesa. <https://www.corteconstitucional.gov.co/relatoria/1993/C-488-93.htm>
- Corte Constitucional de Colombia. (1993, 3 de septiembre). Sentencia T-349 de 1993. M.P.: Eduardo Muñoz. Cifuentes <https://www.corteconstitucional.gov.co/relatoria/1993/T-349-93.htm>
- Corte Constitucional de Colombia. (1995, 18 de abril). Sentencia SU-082 de 1995. M.P.: Eduardo Muñoz. Cifuentes <https://www.corteconstitucional.gov.co/relatoria/1995/SU082-95.htm>
- Corte Constitucional de Colombia. (1997, 10 de octubre). Sentencia T-552 de 1997. M.P.: Alejandro Martínez Caballero. <https://www.corteconstitucional.gov.co/relatoria/1997/T-552-97.htm>
- Corte Constitucional de Colombia. (2002, 26 de agosto). Sentencia T-729 de 2002. M.P.: Marco Gerardo Monroy Cabra. <https://www.corteconstitucional.gov.co/relatoria/2002/T-729-02.htm>
- Corte Constitucional de Colombia. (2012, 12 de abril). Sentencia T-260 de 2012. M.P.: Humberto Antonio Sierra Porto. <https://www.corteconstitucional.gov.co/relatoria/2012/T-260-12.htm>
- Corte Constitucional de Colombia. (2014, 23 de enero). Sentencia T-020 de 2014. M.P.: Jorge Iván Palacio Palacio. <https://www.corteconstitucional.gov.co/relatoria/2014/T-020-14.htm>
- Corte Constitucional de Colombia. (2015, 27 de abril). Sentencia T-198 de 2015. M.P.: Jorge Iván Palacio Palacio. <https://www.corteconstitucional.gov.co/relatoria/2015/T-198-15.htm>

- Corte Constitucional de Colombia. (2015, 12 de mayo). Sentencia T-277 de 2015. M.P.: Jorge Iván Palacio Palacio. <https://www.corteconstitucional.gov.co/relatoria/2015/T-277-15.htm>
- Corte Constitucional de Colombia. (2018, 6 de marzo). Sentencia T-114 de 2018. M.P.: Diana Fajardo Rivera. <https://www.corteconstitucional.gov.co/relatoria/2018/T-114-18.htm>
- Corte Constitucional de Colombia. (2018, 17 de mayo). Sentencia T-238 de 2018. M.P.: Gloria Stella Ortiz Delgado. <https://www.corteconstitucional.gov.co/relatoria/2018/T-238-18.htm>
- Corte Constitucional de Colombia. (2019, 3 de octubre). Sentencia SU-420 de 2019. M.P.: Gloria Stella Ortiz Delgado. <https://www.corteconstitucional.gov.co/relatoria/2019/SU420-19.htm>
- Corte Constitucional de Colombia. (2019, 5 de junio). Sentencia C-224 de 2019. M.P.: Antonio José Lizarazo Ocampo. <https://www.corteconstitucional.gov.co/relatoria/2019/C-224-19.htm>
- Corte Constitucional de Colombia. (2020, 3 de febrero). Sentencia T-030 de 2020. M.P.: Gloria Stella Ortiz Delgado. <https://www.corteconstitucional.gov.co/relatoria/2020/T-030-20.htm>
- Corte Constitucional de Colombia. (2021, 14 de julio). Sentencia T-275 de 2021. M.P.: José Fernando Reyes Cuartas. <https://www.corteconstitucional.gov.co/relatoria/2021/T-275-21.htm>
- Cybercrime Convention Committee (T-CY). (2020). The Budapest Convention on Cybercrime: benefits and impact in practice. Consejo de Europa. <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>.
- Davara Fernández, E. & Davara Fernández, L. (2017). *Delitos informáticos*. Thomson Reuters Aranzadi.
- Departamento Nacional de Planeación. (CONPES). Política Nacional de Confianza y Seguridad Digital. República de Colombia. <https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf>
- Donna, E. A. (2011). *Derecho penal*. Parte Especial II-B. Rubinzal-Culzoni Editores. <https://www.derechopenalenlared.com/libros/donna-derecho-penal-especial.pdf>.
- Hernández-Sampieri, R., Fernández-Collado, C., & Baptista Lucio, M. P. (2014). *Metodología de la investigación* (6ª ed.). McGraw Hill Interamericana Editores.
- Lakoff, G. (1987). *Women, fire, and dangerous things: What categories reveal about the mind*. University of Chicago Press.
- Miró, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons. <https://www.marcialpons.es/libros/el-cibercrimen/9788415664185/>
- Montalvo Velásquez, C., Freja Calao, A., & Bolaño García, B. (2021). *Delincuencia y Delitos Transnacionales Facilitados por la Globalización*. Editorial Universidad del Atlántico.
- Nieto Martín, A., & Mejía Patiño, O. A. (2009). *Estudios de Derecho penal económico*. Universidad de Ibagué.
- Organización de Naciones Unidas. ONU. (2012). Declaración de Río sobre el delito cibernético.

- https://www.comjib.org/wp-content/uploads/imgDrupal/Declaracion_Rio_ciberdelito.pdf
- Organización de Estados Americanos (OEA). (2011). Principios y recomendaciones preliminares sobre la Protección de Datos (Documento CP/CAJP-2921/10, 17 de octubre de 2011). https://www.oas.org/dil/esp/cp-cajp-2921-10_rev1_corr1_esp.pdf
- Organización de los Estados Americanos (OEA). (2002). Convención Interamericana contra la Delincuencia Organizada Transnacional. Adoptada en la Asamblea General el 15 de diciembre de 2000. <https://www.oas.org/juridico/spanish/tratados/a-66.html>
- Organización de Estados Americanos (OEA). (1998). Declaración ministerial relativa a la protección de la intimidad en las redes globales. http://www.oas.org/es/sla/ddi/docs/Declaracion_OCDE_Proteccion_Intimidad_red_es.pdf
- Ortiz de Urbina, E. (2020). La responsabilidad penal de los directivos de empresa. <https://elderecho.com/la-responsabilidad-penal-de-los-directivos-de-empresa>.
- Policía Nacional de Colombia. (s.f.). Centro Cibernético Policial (CCP). <https://www.policia.gov.co/ciberseguridad>.
- Presidencia de la República de Colombia. (1989). Decreto 1360 de 1989. Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor. *Diario Oficial* No. 38871. <https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1273449>
- Presidencia de la República de Colombia. (2012). Decreto 2364 de 2012. Por medio del cual se reglamenta el uso de las firmas electrónicas y se dictan otras disposiciones. *Diario Oficial* No. 48574. <https://www.suin-juriscol.gov.co/viewDocument.asp?id=1442265>
- Real Academia Española. (s. f.). Diccionario de la lengua española (22.a ed.). <https://dle.rae.es/cultura?m=form>.
- Real Academia Española. (s. f.). Informática. En Diccionario de la lengua española (23a ed.). Recuperado de <https://dle.rae.es>.
- Salamanca Castro, A. B., & Martín-Crespo Blanco, C. (2007). El muestreo en la investigación cualitativa. *NURE Investigación*, (27), marzo-abril.
- Vargas, C. (2018). Las Tecnologías de la Información y la Comunicación (TIC) en la educación. *Revista Diálogo de Saberes*, 10(2), 45-60.
- Villabella Armengol, C. M. (2020). *Estudios de Derecho Constitucional*. UNIJURIS.
- Witker Velásquez, J. A. (2007). *Globalización y delitos económicos*. Instituto de investigaciones jurídicas, UNAM. <https://dialnet.unirioja.es/servlet/articulo?codigo=5207238>