MLS – LAW AND INTERNATIONAL POLITICS (MLSLIP)
https://www.mlsjournals.com/MLS-Law-International-Politics
ISSN: 2952-248X
(2025) MLS-Educational Research, 4 (1), 34-51. doi.org/10.29314/mlser.v4i1.4067.

THE PROTECTION OF INFORMATION AND DATA (TITLE VII-BIS CRIMINAL CODE) AND ITS EVOLUTION IN COLOMBIAN ECONOMIC CRIMINAL LAW 1991-2021

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

Edgar Valencia Cardona[1]
International Iberoamerican University, Mexico
[edgar.valencia@doctorado.unini.edu.mx] [https://orcid.org/0000-0003-3919-794X]

Manuscript information:
Recibido/Received: 04/05/2025
Revisado/Reviewed: 11/06/2025
Aceptado/Accepted: 20/06/2025

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

Abstract

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.

[1] Corresponding author.

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.

Introduction

This article poses as a research question: what has been the normative development regarding the protection of information and data (Title VII-bis Criminal Code) in Colombian economic criminal law from 1991 to 2021? Thus, the study focuses on the normative and complementary legislative evolution with the inclusion of Law 1273 of 2009 in the Penal Code (Law 599 of 2000) as Title VII-Bis, which typified computer crimes, cybercrimes or cybercrimes in the Colombian territory. This analysis examines how the aforementioned reforms have made it possible to punish criminal conduct associated with the misuse of ICTs, which were not specifically regulated by criminal law.

Initially, the classification of punishable conducts or those criminal acts that involve the intervention, manipulation and interaction with electronic devices for data transmission is conceptualized. These take place when some people take advantage of the opportunity and arbitrarily enter or remain in computer systems for the purpose of committing acts that violate fundamental rights and, on other occasions, attack the economic structure of private and public organizations, generating significant consequences in both areas. On this subject, Acosta, M., Benavides, M., and García, N. (2000) in their article entitled computer crimes, organizational impunity and its complexity in the business world, state that computer crimes "are illicit acts committed through the inappropriate use of technology, infringing on the privacy of third parties' information". Further on, Donna (2010) states that this branch of law should be studied together with crimes that harm or endanger the regulatory activity of the State in the economy and the strengthening of commercial activities, the exchange of goods and services, openness to learning and effective access to technological knowledge. In addition, Hernández (2009) warns that computer crimes can affect the integrity, confidentiality and availability of computer systems, a situation that was raised in the 2009 regulatory initiative, which consisted in building a specific legal asset and defining guiding verbs emanating from technological progress and computer interaction with human beings, which leads to attempt to aggravate the penalties in currently typified conducts, and in other matters it intends to regulate behaviors not contemplated in the ordinary criminal law, transferred from the growing criminality, not only with the conducts related to the use of computer devices, but those behaviors considered collateral to achieve the normative-punitive level equal or better to international standards, with significant advances in terms of control and punishment of offenses committed with the use of computer systems and the manipulation and/or trafficking of personal data.

The study is based on theories that highlight the complexity and multi-faceted nature of this type of crime, underscoring the need to adapt the legal framework to the challenges posed by criminality in the digital and globalized environment; Witker (2006) analyzes how economic globalization has facilitated the expansion of criminal organizations that operate transnationally, taking advantage of legal loopholes, inadequate criminal policies and deficiencies in criminal systems in some States, which leads to crimes such as human trafficking, drug trafficking, money laundering and cybercrime operating in multiple jurisdictions with relative impunity. Also, Montalvo (2021) in "Delincuencia y delitos trasnacionales facilitados por la globalización", shows that the phenomenon of global integration intensifies the operation of transnational criminal organizations.

The general objective of the research is to analyze the development and significant changes in the regulations and jurisprudence, with respect to the legally protected right "On the Protection of Information and Data" (Title VII-Bis Penal Code) from 1991 to 2021. Prior to Law 1273 of 2009, computer crimes in Colombia were treated under the category of "crimes against economic patrimony" (Nieto & Mejía, 2009). As pointed out by Correa and Davara (2017) the absence of a specific criminalization for conducts such as phishing resulted in the imposition of minimal penalties, evidencing the insufficiency of the legal framework to face the challenges posed by technological crimes in a globalized environment, where criminal networks take advantage of both technological advances and cross-border economic flows. Then, four specific objectives are developed: first, to identify and describe the genesis of the legally protected good in the constitutional sphere through a historical and comparative analysis; second, to analyze the normative development and legislative reforms that have influenced its configuration within the legal system; third, to examine the relevant jurisprudence issued by the high courts regarding its interpretation and application; finally, to evaluate the normative advances in the field of information and data protection in the context of domestic economic criminal law, identifying the main contemporary challenges.

As a preamble to the literature review (Chapter II), the aim is to contextualize the reader on the genesis and scientific development of electronic devices for data transmission, exploring both their historical evolution and the periods in which they emerged, as well as the advances in computer science and systems, both globally and regionally. It will also address the origin and expansion of the Internet and ICTs, the growth of which has led to the emergence of new forms of crime. The conceptualization and classification of computer crimes or cybercrimes are discussed in depth, highlighting their impact on privacy and economic assets, among other legal assets, which will allow a more solid understanding of the approach proposed in this work. Together with the background, the different theoretical contributions that support the study will be illustrated through an exhaustive analysis, with the purpose of identifying the development of the legal and complementary normative framework of the protected legal right.

Subsequently, the categories and/or types of computer crimes or cybercrimes identified to date at the global and regional levels will be discussed and conceptualized, as well as the organizations that protect individuals against illegal conduct known as computer crimes, and the origin, concept, background and evolution of economic criminal law at the global and regional levels will be explained, highlighting the close relationship between the development of information technology and the need to update regulatory frameworks. In this context, the importance of Title VII-Bis of the Colombian Criminal Code is highlighted as a regulatory response to the challenges posed by computer crime in an increasingly digitalized society.

Justification

In Colombia, within the context of the Colombian criminal economic scientific knowledge whose legal and complementary normative development is based on general rules and principles that radiate in the structure of the punitive dogmatic-legal framework, has drawn the attention of authors such as Acosta, (2020) who examines the evolution and

effectiveness of the national legislation in the face of this problem that requires having as a starting point to know which were the first criminal conducts of this type. Therefore, it is considered that they originated in the early 90's, a period in which computer technology was introduced in Colombia and the marketing of software and hardware began, consequently, the behaviors that violate the legally protected good intensified to a great extent with the manipulation of computer instruments and tools and the consequent coexistence with the Internet in almost all parts of the Colombian territory.

In view of this need and based on the coexisting criminal procedural moment in our society, the legislator observes the need to issue complementary regulations to punish disruptive behaviors that violate the confidentiality, integrity and availability of computer systems incorporated in the collective imagination, as computer crimes, cybercrimes or cybercrimes; behaviors that take place with the intervention, manipulation and interaction of ICTs, whether in workplaces, homes, schools and other places, where individuals with advanced knowledge or not in computing, arbitrarily enter computer systems in an abusive way, with the firm idea of committing illegal acts against the economic structure, private and public organizations, companies and/or one or more individuals, as stated by Acosta, Benavides, Merck and others (2020).

Since 2009, anomalous behaviors, product of technological progress or the so-called cybercrimes, computer crimes or cybercrimes are initially regulated through Law 1273 of 2009, which attempts to provide possible solutions to affectations derived from illicit conducts linked to the business, industrial and commercial context. This sanctioning normativity of common or ordinary character that, in turn, faces criminal manifestations studied from the theory of crime intrinsically framed in the framework of nuclear Criminal Law, which partially fills the legal normative gap related to criminal behaviors that still persist with the use (sometimes incorrectly) of ICT, generating with this, legitimacy in its protection through the Colombian Criminal Law (Vargas, C., 2018).

According to Arévalo, S. (2021) in his document "Prevention of computer crimes", illicit conducts arising with the Internet especially affect minors and violate their rights, which shows the need to update Colombian legislation to respond to new forms of criminality such as cyberbullying, grooming, phishing, child pornography, sexting and skimming, emphasizing the importance of prevention, for which he provides information on tools and methods of protection against these computer crimes. Camargo, L. (2021), in "Regulación en Colombia de los delitos informáticos" (Regulation of computer crimes in Colombia), explains the evolution and conceptual framework of these conducts, where he states that ICTs have facilitated the commission of these crimes and generated a wide field of risks, for which he proposes to define and catalog them as computer fraud, computer sabotage, possession of malicious software, unauthorized access and disclosure of secrets, identity theft, computer espionage, illegal access to computer systems, data scams, among others. It shows that, for the authorities, it is difficult to prove the commission of these cybercrimes and the presentation of innumerable setbacks to collect evidence, since the aforementioned punishable conducts, can be executed quickly and easily, this also complicates identifying the person responsible for the act. Finally, it identifies factors that increase the vulnerability of users to cybercriminals, such as carelessness, failure to take minimum precautions (e.g. antivirus), the use of weak passwords and connection to public networks for transactions. As Miró (2012) points out, criminal behaviors committed through information and

communication technologies are part of the current criminological reality, highlighting the emergence of new ways to violate the privacy and property of individuals, using social engineering, especially through crimes such as computer fraud like Scams (with loss of money), Hoax (when there is only deception), Phishing (theft of information), Pharming (directing to a fraudulent website), these forms of cybercrime arise in order to take advantage of the transnationality of the Internet to attack patrimonial and personal interests through cyber-racism or cyber-terrorism.

It should be noted that the study developed in this thesis is closely related to Colombian economic criminal law, since its main focus will be consolidated in the protection of information and data and its regulatory development in the field of Colombian economic criminal law from 1991 to 2021. Therefore, it is relevant to know that in our legal environment there is reference to the concept of this branch of punitive law, proposed as the set of rules protecting the legal good of the economic order of the States, which strictly speaking should be understood as the legal regulation of state interventionism in the economy, (Agustia, J., and Vargas, M., 2019) and which aims to provide a solution to the conflicts arising within the scope of production, distribution and access of traders, manufacturers and consumers of goods and services, considering that its intention is aimed at generating balance between the unlawful commission and its subsequent punishment or sanction. Abadías, A., and Bustos M. (2020) in the work "Temas prácticos para el estudio del derecho penal económico" tells us: "This specialty of law has the function of protecting society from corporate crimes, tax crimes, fraud, crimes against property, against consumers, illegal party financing, bribery, embezzlement, administrative malfeasance, money laundering, influence peddling, corporate corruption, pyramid schemes" and that in addition, economic criminal law studies the criminal liability of legal persons, although the typification is incorporated in the nuclear criminal law with the additions already known, the usual procedures for the prosecution of those responsible require the prosecuting entity and the investigators assigned to each case to have their own knowledge in the computer discipline.

On the other hand, it is inferred that the regulation incorporated into ordinary criminal law in 2009, related to the aforementioned protection of information and data, cannot be understood as an instrument that discourages business, commercial or industrial development of society. Ortiz de Urbina, E., (2020) states that by specifying the criminal types, the unlawfulness and punishment corresponding to such conducts, a legitimization is sought on the part of the sanctioning law of an ethical-legal type. In this sense, economic criminal law and ordinary criminal law pursue regulatory purposes, therefore, the legitimacy of the former will be valid in the provision that satisfies the criteria of legitimacy of the latter, in terms of the culpability of the perpetrator, since the unjust in one, must be in the same plane and / or sense of the other to entail, consequently, an equitable and fair sanction before society.

The contribution and relevance for the academic community is significantly given by analyzing in a comprehensive manner the regulatory evolution and the criminal protection of information and data between 1991-2021, in terms of the regulatory framework, the issuance of laws and other complementary rules, especially with regard to the protected legal right: "On the Protection of Information and Data" (Title VII-bis of the Colombian Criminal Code). This analysis, which covers both the legislative development and the doctrinal and jurisprudential perspectives, provides valuable inputs for academia and the formulation of

public policies, by showing situations in which economic criminal law protects, protects and provides legal certainty, through the punishable normative set as a result of the systematic development of this aspect of law. Consequently, the gaps, gaps and challenges in the legislation will be identified in the face of the rise of this behavior and globalization; since its relevance lies in checking how the legal response has been insufficient to face the new forms of technological criminality and thus, contribute to the structuring of the methodological procedure proposed, so that it adds important input to advance socially in the emerging punitive identification within the cybernetic community, where the use of electronic and computer tools and devices of all kinds is essential.

The personal reasons that lead to the choice of this research topic consigned in the doctoral thesis in Economic and Business Law, is given thanks to the importance of raising awareness in the collective imagination of those who are interested in the impact and digital development in our territory, which managed to transform from the 90s, the physical and real social environment to become virtual, since electronic devices are part of the daily life of human beings and the use of them, which in most cases due to carelessness of users lead to generate threats and vulnerabilities, affecting their economic assets, companies and / or economic groups.

Methodology

In order to develop the parameters outlined and following the line of reasoning of the methodological approach, it is essential that the strategic framework of the research be coherent and practical to effectively address the problem and achieve the proposed objectives. In this sense, the research design is part of the qualitative paradigm, which focuses on understanding and exploring the punitive normative reality regarding the protection of information and data in accordance with the provisions of Title VII-bis Penal Code, in the context of Colombian economic criminal law between 1991 and 2021. From an interpretative and naturalistic perspective, the approach seeks to capture and describe social, cultural and human phenomena in their natural context, avoiding reducing them to numerical variables. Arias (2012), in the work: "The Research Project: Introduction to Scientific Methodology", argues that in documentary and bibliographic research, the basic analysis consists of breaking down the information into main and secondary ideas, to identify links and implications and, at the same time, to translate or decipher the meaning of these, perceiving the events in an accurate way. He also notes that bibliographic research is a documentary design that relies on secondary sources, such as books and articles, to systematically collect, select and analyze information. Along the same lines, Hernández-Sampieri, Fernández-Collado and Baptista-Lucio (2014) in the sixth edition of "Research Methodology" argue that the qualitative approach resorts to data collection without numerical measurement to discover or refine research questions in the process of interpretation. Consequently, within the research work, we will proceed to compile and analyze the normative instruments issued by the Colombian legislator with regard to the normative development of the protected legal right.

The non-experimental cross-sectional design selected in this process is appropriate and leads to define the paradigm of analysis that arises to understand the phenomena that

concern economic criminal law. An explanatory approach is adopted, aimed at identifying and analyzing the possible shortcomings of the ordinary criminal law that underlies the recognition and application of economic criminal law in the area of information and data protection. This type of research is relevant because it studies new or little explored phenomena, focusing on the details and particularities, so that finally, solid and determinant conclusions are generated on the issue under study.

As a complement to this methodological process, the application of the historical-legal and legal exploratory methods is added to this research, where the first one allows focusing the research question on the evolutionary succession of the general aspects of the normative development of the protected legal right "Of the Protection of Information and Data", analyzing the succession of legal provisions and other complementary norms typified in Title VII-Bis Penal Code (Law 599, 2000).

Thus, the historical-logical method is a tool that allows understanding the object of study in its historical evolution, highlighting its general aspects and development trends, which is essential to reveal the genesis and evolution of legal institutions and norms, as well as to understand the formation of legal systems, as Villabella (2020) points out, it is essential to understand the origin and evolution of legal institutions and norms, as well as to identify the trends and transformations that have shaped legal systems.

On the other hand, the legal exploratory method is oriented to the analysis of normative issues that have not been studied or are new, allowing the identification of gaps and aspects not previously addressed in the law, and providing a preliminary vision that can later be deepened by means of descriptive or explanatory approaches. This methodological combination will make it possible to unveil a comprehensive and critical view of the shortcomings, gaps or legal flaws that the standard may have when it comes to applying it to reality.

The target population of the research study comprises the set of regulations and their legislative development from 1991 to 2021 on the subject of information and data protection. In order to collect the data and information necessary to achieve the objectives set, we initially resorted to specialized sources such as academic databases, scientific journals, graduate papers and monographs, among others. In the same way, information was compiled from primary sources such as the Political Constitution of Colombia of 1991, Law 599 of 2000, Law 1273 of 2009 and Law 1581 of 2012 and other complementary norms, added to the Gazettes of the Congress of the Republic and bulletins of the Constitutional Court, from which the jurisprudence was extracted (Sentences or Rulings) as well as the Treaties and Conventions ratified by Colombia and the public policies related to data protection. All of the above, available and without restriction in accordance with the provisions of Law 1712 of 2014, which deals with transparency and the right of access to public information in Colombia. In addition, relevant information published on the websites of international, regional and local organizations that deal with issues related to economic criminal law and cybercrime will be consulted.

The information collected was obtained through the analysis of primary and secondary documentary, bibliographic and electronic sources using tools called data recording cards, and then proceeded to directly observe the data, in accordance with Marshall and Rossman (1989), which implies a systematic observation of "events, behaviors and artifacts in the social scenario chosen to be studied". After the application of this

technique, we proceed to elaborate the structured templates that consolidate the clear and objective information, which will be processed, thus achieving the expected results that will be incorporated in the corresponding research work.

During the conduct of the research, probability sampling is used, resorting to the representative selection that has given rise to the normative development of the legal property related to the object of study, which offers a better opportunity to create a reliable and representative sample and thus achieve greater precision in the results, this, this is in accordance with Salamanca-Crespo and Martín-Crespo (2007) who state that probability sampling is "the best way to obtain data" since they are "decisions made in the field, since we want to reflect the reality and the diverse points of view of the participants, which are unknown to us at the beginning of the study". This approach allows a deep and contextualized understanding of the phenomena studied. In conclusion, the adequate and congruent selection of information on the population required in this research work, especially in relation to the legal field, requires careful consideration in the management of current regulations, since the legal framework establishes principles such as transparency and restricted circulation of data, ensuring that the collection, processing and use procedures respect fundamental rights and protect the privacy of individuals, which reinforces the ethical validity of the research product.

Results

In order to achieve the expected results in this qualitative research, we resorted to the process of categorizing the information collected, since this procedure allows us to identify relevant themes, recurring events and patterns of ideas within the data, facilitating their analysis and interpretation. Categories function as conceptual groupings that bring together elements with common characteristics, which helps to reduce, organize and structure the information in a way that makes it more manageable and understandable for the researcher. Thus, categorization is consolidated as an essential cognitive and organizational process, which involves classifying and grouping concepts or information according to shared criteria or characteristics, optimizing the approach and understanding of the phenomenon under study. This position is supported by Lakoff, (1987) in his work "Fundamental women, fire and dangerous things" who argues that categorization is an active and fundamental process for thought, perception, action and language, every time we understand or produce statements, we are using linguistic and conceptual categories, and in this dynamic, flexible and experience-dependent process, prototypes play an important role since they open a door to the complex and realistic understanding of the human mind.

Based on the above approach and considering the need to structure the analysis of the research development, the application of the categorization process is proposed in order to broadly address the regulatory, technological and legal aspects involved.

Categories

Category 1: Development of the protected legal right "of information and data protection" (1991-2021)

Subcategories:

a) *Constitutional Development*. This refers to the set of constitutional provisions designed to protect the guarantees and rights of individuals, especially with regard to possible violations of human dignity and other fundamental rights. It is provided for in Articles 15, 21, 42, 44 and 74 of the Magna Carta of 1991.

b) *Regulatory development*. It refers to the evolution of regulations such as Laws, Decrees and other provisions regarding the protection of information and personal data, driven by the need to adapt and appropriate laws to technological advances and new forms of crime, thus ensuring the protection of fundamental rights related to privacy and the handling of personal data. Other standards include: Law 527-1999; Law 599-2000; Law 679-2001; Law 962-2006; Law 1032-2006; Law 1266-2008; Law 1273-2009; Law 1336-2009; Law 1581-2012; Decree 1727-2009; Decree 2952-2010; Decree 1377 of 2013.

c) *Jurisprudential development*. It is materialized with the issuance of Rulings or Judgments of the Constitutional Court in judicial decisions, emphasizing the right to the protection of personal data and the right to Habeas Data, which has been decisive in defining the prerogatives of the holders of personal data to know, update and rectify their information in public and private databases. Some examples are: T-414/1992; SU-082/1995; C-748/2011; T-050-2016 among others.

d) *Development at the level of international treaties and agreements ratified by Colombia.* It reflects the commitment of the Colombian State to the protection of personal data and privacy by adapting its legislation to the demands of the contemporary global digital environment in the face of infringement by cybercriminal gangs, by adhering to the Budapest Convention, and thus guaranteeing respect for fundamental rights related to personal information in a global context.

e) *Development of internal public policies.* The development of Public Policies in Colombia, which refers to the issue of information and data protection (1991 and 2021) has evolved through the CONPES 3920-2018 documents that established the national policy for data exploitation (Big Data), the CONPES 3701-2011 "Policy guidelines for cybersecurity and cyber defense", the CONPES 3854-2016 that establishes the "National policy for digital security" and the CONPES 3995-2020 on the "National policy for trust and digital security in Colombia".

Category 2: Analysis of the legal protection of information and data

Subcategories:

a) *Protection of information and data*. It is the set of skills, measures and regulations to protect personal and sensitive information against unauthorized access, theft and in general any act of insecurity or compromise of personal or business information. The above, in order to take measures to protect its integrity against manipulation or attacks with malware or computer viruses.

b) *Data classification*. Process by which personal data or data of a private or public organization are organized and categorized according to their level of sensitivity, confidentiality, importance or relevance. This is fundamental for information management and cybersecurity, allowing to determine which protection measures should be applied to each type of data, with regulatory compliance and international standards that ultimately mitigates and identifies the risk associated with loss or unauthorized access to information.

c) *Data security*. It is the practice of protecting digital information against unauthorized access, theft and in general other threats throughout its life cycle, since its purpose is to identify who can see or manipulate the data, limiting access to authorized persons through authentication and authorization, thus safeguarding the integrity, confidentiality and availability of the data.

d) *Technology and crime*. They refer to the confluence between criminal activities and technological advances insofar as they may affect the security, privacy, intellectual property or assets of individuals, companies or States. This makes it necessary to develop regulations and research protocols to prevent and combat vulnerabilities in computer systems and interconnection networks.

Category 3: Economic crimes

Subcategories:

a) *Analysis of economic crimes related to technology.* The analysis identifies common crimes committed for economic purposes with the intermediation of technological devices to affect the assets of third parties, highlighting the need to develop effective strategies to combat such criminal behavior in an increasingly digitalized world.

b) *Impact of economic crimes on economic assets.* This refers to the negative impact they can have at the moment of affecting both the microeconomic and macroeconomic levels, so that these actions have consequences on the assets of individuals, companies and States, as well as the economy in general, leading to a lack of confidence in financial institutions and in the economic system and, at the same time, having repercussions on direct and indirect foreign investment.

c) *Influence of globalization on the emergence of new crimes.* It occurs within the processes of globalization and the way they have facilitated the creation and expansion of new forms of criminality, with the intervention of ICTs which have provided spaces for the growth of organized criminal networks operating internationally through the Internet, where globalization has created new markets for illicit goods and services, such as drugs, weapons and human organs trafficking, among others.

Category 4: Economic criminal law

Subcategories:

a) *Contextualization of economic criminal law in the Colombian legal framework.* It focuses on the protection of supra-individual legal assets, such as the economic and social order, through criminal sanctions, achieving through economic criminal law, the guarantee and security in commercial interactions between individuals and sometimes between the State and other actors, against situations

related to criminal activities against the economic heritage, the economic and social order and public administration.

b) *Relationship of economic criminal law with computer crimes and/or cybercrimes.* It is based on the confluence between criminal activities that affect the economic and social order and those committed through the use of ICTs, which ultimately have a direct impact on the economic assets of individuals, companies and the State, making it necessary to develop effective, efficient and relevant legislation.

c) *Influence of economic criminal law on globalization and technology.* It manifests itself in how economic criminal law must protect the economic order in general against the threats (unfair and fraudulent practices) posed by both globalization and ever-evolving technologies, which must include legal regulation of economic activities and protection against those forces that have transformed the criminal landscape as the world has become more interconnected and digitized.

Data Analysis

In order to achieve the objectives outlined in this research, the documentary review and analysis technique was implemented as the main method for the collection of information. According to Corbetta (2007), who states that documentary analysis is one of the most appropriate tools for data collection in documents or judicial material, due to its nature, since "a document is an informative material about a certain social phenomenon that exists independently of the researcher". This technique enables a systematic and rigorous approach to the reality studied, facilitating the interpretation and understanding of the facts through the analysis of primary and secondary sources, which is especially relevant when dealing with legal or institutional issues. Marshall and Rossman (1989) define data analysis as "the systematic description of events, behaviors and artifacts in the social setting chosen to be studied". Therefore, it follows that once the corresponding technique focused on exploring the legal implications aimed at observing the regulatory changes is applied, the corresponding records containing clear and objective information will be prepared in order to achieve the goals set.

The following steps were carried out:

First. Compilation and organization of data and information, which consists of relating the constitutional precepts; as well as the regulations (laws and decrees) issued by the legislator and the national government, before and after the enactment of the Political Constitution of 1991; the relevant jurisprudence; public policy documents (CONPES documents); and the treaties and agreements signed by the Colombian State. These contextual and normative aspects are extracted from primary sources such as the Political Constitution of Colombia, Colombian Penal Code, complementary laws, jurisprudential review of the Constitutional Court, which will serve to support the present proposal and the methodological planning with which a chronological classification will be elaborated, with the purpose of organizing the data collected in a timeline, identifying the most important legislative and jurisprudential milestones.

Second. A content analysis was performed, where the legal precepts of each relevant law or ruling were examined in detail, identifying changes and developments in the protection of information and data.

Third. The trends, progress and normative development in terms of the legally protected good were analyzed and identified.

Fourth. A comparison was made with international standards, where Colombian regulations were contrasted with instruments ratified by Colombia regarding data protection, information and computer crimes.

Fifth. A statistical analysis was carried out, where descriptive data on the application of these norms in the context of economic criminal law in Colombia were examined.

Sixth. The interpretation of results and evaluation of the findings in the context of Colombian economic criminal law was carried out, analyzing the effectiveness and implications of the regulatory changes until 2021, achieving through the analysis with a qualitative approach to know how the new criminal types were implemented in the punitive legislation, in order to verify if they have responded effectively to counteract the criminal actions in our territory.

Conclusions

The implications of this doctoral thesis highlight the need to strengthen and update the Colombian regulatory framework to meet the challenges of cybercrime and data protection in the digital era, which requires revising legislation and adopting international standards that allow more effective and coordinated responses. The research also highlights the need to articulate public policies, international cooperation and criminal strategies that adapt to technological dynamics, providing valuable inputs for academic debate and training in economic criminal law, motivating legal operators and legislators to rethink the role of economic criminal law as a tool for social and economic protection in a context of future digital and global transformation.

Thus, the product of the investigation evidences the normative development of the protected legal right: "Of the Protection of Information and Data" in the context of Colombian economic criminal law, from 1991 to 2021, which has undergone a progressive evolution aimed at addressing the challenges of cybercrime, however, the growing global and local concern about the increase in cybercrime, suggests the need for a continuous review and strengthening of the legal framework to adequately protect fundamental rights and the economic structure of organizations, as there are still significant challenges that can be exploited by organized crime, which has prompted the creation of standards and mechanisms for the protection of personal information and data, as well as challenges arising from the rapid evolution of ICTs, artificial intelligence and the massification of electronic devices. Despite these challenges, the protection of rights such as privacy, good name and Habeas Data are constitutionally guaranteed and regulated by norms that require the proper handling of information in both the public and private sectors.

It is concluded that the regulatory development around the protection of information and data, shows that it has evolved in a limited way in legal response to the challenges posed by cybercrime, as it needed the jurisprudential way and constant interpretations to achieve reach the challenges presented and the new illicit modalities, this is reflected in the socio-legal study (2019) ten years after the enactment of the Law on computer crimes in Colombia (Law 1273 of 2009) where it is shown that, although this law represented a step forward in

the protection against cybercrime, there is still a need to continuously update and strengthen the legal framework to ensure effective protection against new forms of crime, thus consolidating the role of the law as an essential instrument for the defense of fundamental rights and the stability of the economic order in the digital environment.

Finally, it is important to highlight that the comparative analysis of regulatory frameworks for the protection of personal data in Latin America reveals that, in the digital era, this issue has acquired an unprecedented relevance, driving the countries of the region to develop and strengthen specific regulations aimed at safeguarding the privacy and rights of their citizens in the face of technological challenges and new threats in the handling of personal information, as Argentina was a pioneer with Law 25.326 of 2000, which is being revised to align with the European General Data Protection Regulation (GDPR). Brazil enacted the General Data Protection Law (LGPD) in 2018, inspired by the GDPR, and elevated data protection to a fundamental right in its Constitution in 2022. Chile is reforming its legislation to adapt to international standards. Ecuador implemented the Organic Law on Personal Data Protection in 2021. In Mexico, there are two fundamental laws that regulate the protection of personal data, each focused on different areas, a Federal Law for the Protection of Personal Data in Possession of Private Parties (LFPDPPP of Jul-5-2010) and another, General Law for the Protection of Personal Data in Possession of Obligated Subjects (LGPDPPSO of 2017), Peru, has the Law for the Protection of Personal Data (LDPD) No.29733 of 2011 (effective-2013). Paraguay implemented Law 6.534 of 2020 "On Protection of Personal Credit Data" (effective Oct-28-2020). Uruguay has Law No. 18.331 on Personal Data Protection and "Habeas Data" Action. Venezuela presents a particular case, since it does not have a specific law for the protection of personal data. However, it does have the Law on the Protection of Privacy of Communications, which seeks to protect the privacy, confidentiality, inviolability and secrecy of communications between persons.

References

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.secretariasenado.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 Cifuentes Muñoz. 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 Cifuentes Muñoz. 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 Trasnacionales 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_redes.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