
Cybercrime and computer criminal law: typologies, prosecution and challenges in contemporary digital environments.

Ciberdelincuencia y derecho penal informático: tipologías, persecución y desafíos en entornos digitales contemporáneos.

Cibercrime e direito penal informático: tipologias, perseguição criminal e desafios nos ambientes digitais contemporâneos.

Mohamed Messika

✉ : messika.mohamed@univ-bechar.dz

id : <https://orcid.org/0009-0002-3834-4645>

Kasdi Merbah University, Ouargla, Algeria

Cita sugerida (APA, séptima edición)

Messika, M. (2026). Cybercrime and computer criminal law: typologies, prosecution and challenges in contemporary digital environments. *Tribunal de Justicia, Revista de Investigación jurídica*. 3(2), 107-119. DOI: <https://doi.org/10.51247/tj.v3i2.974>

Abstract

This study aims to analyze cybercrime from the perspective of computer criminal law by identifying its main typologies, criminal prosecution mechanisms, and the challenges faced by legal systems in contemporary digital environments. The research was conducted using a qualitative approach with a narrative review design incorporating elements of a systematic review. Documentary methodology was applied through doctrinal, legal, and comparative analysis of scientific literature, legislation, and international legal instruments selected according to relevance, timeliness, and academic impact criteria. The findings showed that cybercrime has become a dynamic and transnational criminal phenomenon characterized by unlawful access to computer systems, computer fraud, data-related crimes, cyberbullying, and digital economic crimes. The review also revealed that protecting information, privacy, cybersecurity, and property requires updated legal frameworks, specialized investigative mechanisms, and stronger international cooperation. It is concluded that strengthening computer criminal law requires a comprehensive response integrating legislative modernization, technological innovation, specialized training for criminal justice operators, and coordinated preventive and punitive strategies to ensure the effective protection of fundamental rights and legal certainty in the face of the continuous evolution of digital crime.

Keywords: cybercrime; computer criminal law; computer crimes; criminal prosecution.

Resumen

El presente estudio tiene como objetivo analizar la ciberdelincuencia desde la perspectiva del derecho penal informático, identificando sus principales tipologías, los mecanismos de persecución penal y los desafíos que enfrentan los sistemas jurídicos en los entornos digitales contemporáneos. La investigación se desarrolló mediante un enfoque cualitativo con diseño de revisión narrativa y elementos de revisión sistemática. Se empleó la metodología

documental, sustentada en el análisis doctrinal, normativo y comparado de literatura científica, legislación e instrumentos internacionales seleccionados conforme a criterios de relevancia, actualidad e impacto académico. Los resultados evidenciaron que la ciberdelincuencia constituye un fenómeno criminal dinámico y transnacional, caracterizado por modalidades como el acceso ilícito a sistemas, el fraude informático, los delitos contra los datos, el ciberacoso y los delitos económicos digitales. Asimismo, se identificó que la protección de la información, la privacidad, la seguridad informática y el patrimonio demanda marcos normativos actualizados, mecanismos especializados de investigación y una cooperación internacional más eficiente. Se concluye que el fortalecimiento del derecho penal informático requiere una respuesta integral que combine la actualización legislativa, la innovación tecnológica, la capacitación de los operadores de justicia y la articulación de estrategias preventivas y represivas, con el propósito de garantizar la protección efectiva de los derechos fundamentales y la seguridad jurídica frente a la evolución constante de la criminalidad digital.

Palabras clave: ciberdelincuencia; derecho penal informático; delitos informáticos; persecución penal.

Resumo

O presente estudo tem como objetivo analisar a cibercriminalidade sob a perspectiva do direito penal informático, identificando suas principais tipologias, os mecanismos de persecução penal e os desafios enfrentados pelos sistemas jurídicos nos ambientes digitais contemporâneos. A pesquisa foi desenvolvida por meio de uma abordagem qualitativa com delineamento de revisão narrativa e elementos de revisão sistemática. Foi utilizada a metodologia documental, fundamentada na análise doutrinária, normativa e comparada da literatura científica, da legislação e dos instrumentos internacionais selecionados conforme critérios de relevância, atualidade e impacto académico. Os resultados demonstraram que a cibercriminalidade constitui um fenómeno criminoso dinâmico e transnacional, caracterizado por acesso ilícito a sistemas, fraude informática, crimes contra dados, ciberassédio e crimes económicos digitais. Também foi identificado que a proteção da informação, da privacidade, da segurança informática e do património exige marcos jurídicos atualizados, mecanismos especializados de investigação e maior cooperação internacional. Conclui-se que o fortalecimento do direito penal informático requer uma resposta abrangente baseada na atualização legislativa, na inovação tecnológica, na capacitação dos operadores da justiça e na implementação de estratégias preventivas e repressivas integradas, visando assegurar a proteção efetiva dos direitos fundamentais e da segurança jurídica diante da constante evolução da criminalidade digital.

Palavras-chave: cibercriminalidade; direito penal informático; crimes informáticos; persecução penal.

Introduction

The rapid expansion of digital technologies has profoundly reshaped social, economic, political, and legal dynamics on a global scale. The widespread adoption of the Internet, cloud computing, artificial intelligence, digital platforms, and ubiquitous connectivity has fostered new forms of communication, production, and information exchange. These developments have given rise to a highly digitalized society in which a substantial proportion of everyday activities is conducted within virtual environments. In this context, Buzai (2001) argued that the geotechnological paradigm has driven the emergence of an ever-expanding digital universe, redefining the relationship between physical space and cyberspace. Similarly, García-Machado and León-Santos (2021) emphasized that digitalization has evolved beyond commercial processes to become a structural pillar of contemporary development, while Saura (2025) identified digital technology as one of the principal drivers of economic, educational, and social transformation in the twenty-first century.

The accelerated growth of digital ecosystems has also generated unprecedented risks to legal certainty and the protection of fundamental rights. The widespread use of interconnected devices, the storage of massive volumes of personal data, and the automation of numerous processes have expanded opportunities for the commission of unlawful acts through technological means. Consequently, conventional criminal activities have evolved into increasingly sophisticated forms characterized by the exploitation of computer networks, digital systems, and anonymization technologies that hinder the identification of perpetrators. This transformation demonstrates that although technological innovation is indispensable for societal progress, it simultaneously intensifies the complexity of the challenges confronting contemporary criminal justice systems.

In this regard, Conde-Pumpido Tourón (2006) argued that criminal prosecution authorities must continuously adapt to emerging forms of crime arising from technological advancement. Likewise, Pardo Mateos (2013) explained that contemporary criminality has evolved from traditional offenses toward more complex manifestations in which information technologies reshape both the execution of criminal conduct and the strategies employed in criminal investigations. From this perspective, cybercrime encompasses a heterogeneous range of illicit activities, including unauthorized access to computer systems, electronic fraud, identity theft, malware dissemination, cyber extortion, attacks against critical infrastructure, and numerous other offenses committed through digital platforms.

Despite the sustained increase in these forms of criminal activity, many legal systems continue to exhibit significant limitations in responding effectively to rapidly evolving technological realities. The pace of technological innovation frequently exceeds the capacity of criminal and procedural legislation to adapt, creating regulatory gaps that facilitate impunity. Furthermore, the inherently transnational nature of cybercrime complicates the determination of jurisdiction, the collection and preservation of digital evidence, and international judicial cooperation among competent authorities. These challenges underscore the urgent need to strengthen legal frameworks and specialized investigative mechanisms capable of effectively addressing this increasingly complex phenomenon.

In relation to these issues, Acosta Sila et al. (2026) demonstrated that Ecuadorian legislation governing cybercrime still contains significant shortcomings that limit effective protection against emerging digital threats, particularly regarding the coordination between the *Comprehensive Organic Criminal Code* and the *Organic Law on Personal Data Protection*. Similarly, Gala Rodríguez (2026) observed that the fragmented regulatory landscape across several Latin American jurisdictions hinders the effective prosecution of cybercrime and contributes to substantial levels of impunity, particularly where criminal conduct transcends national borders and requires efficient mechanisms for international cooperation.

Against this backdrop, strengthening the legal protection of individual rights within digital environments has become imperative. Privacy, personal data integrity, confidentiality of communications, and cybersecurity constitute legally protected interests whose safeguarding requires criminal law responses that are consistent with ongoing technological developments. In this context, Santillán Molina and Vinuesa Ochoa (2020) argued that the private virtual environment should be recognized as a new dimension of human rights, requiring effective legal mechanisms for its protection. Likewise, Mora Pedreros, Gutiérrez, and Santiago Pajajoy (n.d.) maintained that virtual spaces have become essential environments for the production and dissemination of knowledge, thereby necessitating robust legal safeguards to preserve trust, security, and the effective exercise of fundamental rights.

Considering these premises, the present study aimed to analyze cybercrime from the perspective of cyber criminal law by identifying its principal typologies, examining the mechanisms of criminal prosecution, and assessing the challenges faced by contemporary legal systems in digital environments. To achieve this objective, the following research questions were formulated: What are the principal forms of cybercrime currently affecting

digital environments? and How does criminal law respond to these emerging forms of cybercrime, and what are the primary challenges to ensuring effective criminal prosecution?

Methodology

This study was conducted using a qualitative research approach, as it enabled an in-depth understanding and interpretation of cybercrime and the legal responses provided by cyber criminal law from doctrinal, normative, and critical perspectives. Packer (2018) argued that qualitative research facilitates the comprehensive analysis of complex phenomena through the systematic interpretation of their meanings and contextual dimensions. Furthermore, the study adopted a narrative literature review design incorporating elements of a systematic review, with the aim of integrating and critically examining the scientific and legal scholarship concerning the principal typologies of cybercrime, mechanisms of criminal prosecution, and the regulatory challenges emerging within contemporary digital environments.

Regarding the research methodology, documentary research was employed to facilitate the collection, organization, analysis, and interpretation of information derived from academic publications, legislative instruments, and judicial decisions. Botero Bernal (2003) maintained that documentary research represents an appropriate methodological strategy for legal scholarship because it enables the systematic construction of knowledge through the critical examination of specialized legal sources. Complementarily, Riofrío Martínez-Villalva (2018) emphasized that methodological selection in legal research must correspond to the nature of the object of study. Accordingly, the present investigation combined doctrinal analysis, normative analysis, and the comparative legal method to identify convergences, divergences, and emerging trends in the regulation of cybercrime across different legal frameworks.

The selection of sources was based on criteria of thematic relevance, currency, scientific rigor, and academic impact. Priority was given to peer-reviewed journal articles indexed in internationally recognized databases, specialized legal monographs, national and international legal instruments, and authoritative doctrinal publications, with particular emphasis on recent contributions while also incorporating seminal works essential to the theoretical foundation of the study. Subsequently, the collected materials were subjected to qualitative content analysis and critical comparative examination, enabling the identification of conceptual categories, criminal typologies, models of criminal prosecution, and the principal legal challenges associated with cybercrime. Consistent with Contreras López (2019), the analysis of contemporary cybercriminality required a multidisciplinary perspective integrating contributions from criminal law, criminology, and information sciences in order to provide a comprehensive understanding of cybercrime within the modern digital ecosystem.

Development

Cybercrime

Cybercrime represents one of the most significant manifestations of criminal activity within the digital society, as information and communication technologies have substantially expanded the environments in which unlawful conduct can be perpetrated. Unlike conventional criminality, cybercrime is executed through computer systems, communication networks, and electronic devices that enable perpetrators to operate with remarkable speed, anonymity, and transnational reach. Mateos Pascual (2013) defined cybercrime as the set of criminal offenses committed through digital technologies or directed against computer systems, emphasizing that its rapid expansion is intrinsically linked to the widespread diffusion of the Internet and the digitalization of human activities.

From a legal perspective, cybercrime encompasses conduct that infringes legally protected interests through the use of technological tools or directly targets computer systems, digital data, or technological infrastructures. In this regard, Arteaga González (2021) argued that cyber criminal law emerged as a legal response to the necessity of protecting new forms of

social interaction developed within cyberspace by incorporating specific criminal offenses capable of addressing forms of unlawful conduct absent from traditional models of criminality. This evolution demonstrates that technological advancement has transformed not only the methods through which crimes are committed but also the mechanisms required for their legal protection.

The defining characteristics of cybercrime include its capacity to operate beyond geographical boundaries, the ease with which offenders can conceal their identities, and its reliance on continuously evolving technologies. These features considerably complicate criminal investigations while facilitating the rapid emergence of increasingly sophisticated forms of cybercriminal activity. Peña Labrin (2023) explained that cybercrime is characterized by high levels of technical specialization, continuous innovation, and significant adaptability to governmental control mechanisms, circumstances that necessitate strengthening both preventive and enforcement capacities within the institutions responsible for safeguarding digital security.

Another distinguishing characteristic of cybercrime is the substantial economic profitability associated with many illicit activities conducted in cyberspace. Cyberattacks may be simultaneously directed against thousands of victims located across multiple jurisdictions while requiring relatively limited operational resources and presenting a low probability of immediate detection or identification. Moreover, the automation of attacks through malicious software significantly increases the capacity to compromise critical infrastructures, public institutions, private organizations, and individual users. These circumstances have positioned cybercrime among the most complex threats to the legal and technological security of contemporary States.

The evolution of cybercrime has closely paralleled the rapid advancement of digital technologies. During its earliest manifestations, cybercriminal activities primarily involved unauthorized access to computer systems and acts of digital vandalism. Subsequently, however, increasingly sophisticated forms of criminal conduct emerged, including financial fraud, large-scale data theft, ransomware-based extortion, data manipulation, and cyberattacks targeting strategic national infrastructures. Catá del Palacio (2014) observed that this technological evolution has required a fundamental reassessment of traditional models of criminal prosecution through the incorporation of specialized investigative tools capable of combating criminal organizations operating across globally distributed digital platforms.

Consequently, cybercrime is no longer perceived merely as a technological phenomenon but rather as a multidimensional challenge encompassing legal, economic, social, political, and geopolitical dimensions. The growing dependence on digital services has substantially increased the vulnerability of individuals, businesses, and public administrations to increasingly sophisticated cyberattacks. Accordingly, legal scholarship broadly recognizes that effective governmental responses must integrate preventive public policies, enhanced international cooperation, institutional capacity building, and the continuous modernization of criminal legislation in order to ensure the effective protection of fundamental rights within the digital environment.

Typologies of Cybercrime

The diversity of conduct constituting cybercrime has given rise to multiple doctrinal and legal classifications. Broadly speaking, cyber offenses may be categorized according to the legally protected interest affected, the means employed to perpetrate the offense, or the objective pursued by the offender. Del Pino (2016) argued that these typologies facilitate a comprehensive understanding of the complexity of digital criminality while supporting the development of differentiated legal responses tailored to each category of offense. The accurate identification of these classifications also promotes the proper legal characterization of criminal conduct within contemporary criminal justice systems.

One of the most prevalent forms of cybercrime is unauthorized access to computer systems, commonly referred to as hacking. This offense consists of gaining unauthorized entry into computers, networks, or databases with the purpose of obtaining information, manipulating digital systems, or facilitating the commission of subsequent criminal acts. Unauthorized access frequently serves as the initial stage of numerous cyberattacks because it compromises the confidentiality, integrity, and availability of digitally stored information. Macías-Lara et al. (2022) identified this offense as one of the most recurrent forms of cybercrime in Ecuador, emphasizing the need to strengthen preventive mechanisms and enhance specialized cybercrime investigation capabilities.

Another widely recognized category is computer fraud, characterized by the manipulation of electronic systems to obtain unlawful financial benefits. Such conduct includes fraudulent bank transfers, manipulation of financial platforms, unauthorized use of electronic payment cards, digital commerce scams, and social engineering techniques designed to obtain users' authentication credentials. Acosta et al. (2020) observed that the growing digitalization of commercial activities has significantly increased the exposure of businesses and financial institutions to these offenses, resulting in substantial economic losses and creating new challenges for corporate risk management and internal control systems.

Data-related offenses constitute another particularly significant category because they directly affect one of the most valuable assets of the digital economy: information. These offenses include the unauthorized alteration, destruction, copying, extraction, or disclosure of personal, corporate, or institutional data. The legal protection of digital information has become increasingly important given that a substantial proportion of social, financial, and governmental activities now depends upon digital infrastructures. Ponce Tubay (2024) highlighted that Ecuadorian legislation has progressively strengthened the criminal protection of digital data, although important challenges remain concerning technological modernization and effective international cooperation.

Cyber harassment represents another rapidly expanding category of cybercrime, largely driven by the widespread adoption of social media platforms and digital communication technologies. Such conduct encompasses threats, harassment, stalking, the non-consensual dissemination of intimate content, persistent intimidation, and various forms of psychological abuse perpetrated through electronic means. Although many of these behaviors have traditional criminal counterparts, the digital environment significantly amplifies their reach, permanence, and capacity to infringe fundamental rights such as human dignity, privacy, and personal integrity. Consequently, preventing cyber harassment requires not only effective criminal sanctions but also comprehensive educational policies that promote the responsible and ethical use of digital technologies.

Finally, digital economic crimes encompass a broad spectrum of illicit activities involving money laundering through virtual platforms, cryptocurrency-related attacks, transnational financial fraud, illicit trade within the dark web, and the use of digital assets to conceal proceeds derived from organized crime. Bascur and Sepúlveda (2022) explained that the legislative developments observed across numerous jurisdictions demonstrate the necessity of continuously adapting criminal legislation to address emerging forms of cybercriminal activity that exploit technological innovation. Accordingly, the classification of cyber offenses continues to evolve alongside technological advancements, consolidating cybercrime as one of the most dynamic fields of contemporary criminal law.

Legally Protected Interests

Cyber criminal law seeks to safeguard those legally protected interests whose infringement jeopardizes the security and proper functioning of the digital society. The integration of information technologies into virtually every sphere of social life has expanded the traditional catalogue of legally protected interests to include the integrity of computer systems, the availability of digital data, and trust in electronic communications. Araúz Ulloa (2003) argued

that the concept of the legally protected interest constitutes the foundation of criminal law intervention because it legitimizes State protection against conduct capable of producing significant social harm or endangerment. Consequently, cybercrime requires a dynamic interpretation of legally protected interests that reflects the evolving realities of the digital environment.

Among the most significant legally protected interests is information, understood as a strategic asset indispensable for the functioning of public institutions, private organizations, and individual citizens. Digital information possesses economic, legal, and social value that extends far beyond the physical media on which it is stored. Therefore, its unauthorized alteration, destruction, or appropriation may generate severe consequences for both individuals and society as a whole. García Arroyo (2022) explained that the evolution of criminal law has fostered the recognition of supra-individual legal interests, whose protection has become essential for preserving the effective functioning of contemporary societies, particularly in contexts characterized by high levels of technological dependence.

Cybersecurity constitutes another fundamental legally protected interest because it guarantees the confidentiality, integrity, and availability of digital systems. The protection of computer networks, databases, and critical infrastructures ensures the continuity of essential services, including electronic banking, telecommunications, healthcare systems, public administration, and digital commerce. From this perspective, cyber offenses affect not only individual proprietary interests but also the stability of services whose disruption may seriously compromise collective welfare. The accelerating process of digital transformation has consequently elevated cybersecurity to a fundamental component of both national security and sustainable economic development.

Property remains one of the legally protected interests most frequently targeted by cybercrime, particularly through electronic fraud, digital scams, the unlawful appropriation of virtual assets, and attacks against financial systems. Simultaneously, privacy has acquired enhanced legal significance within digital environments owing to the enormous volume of personal data collected, processed, and stored electronically. Navarro (2005) emphasized that the protection of collective legal interests requires criminal law mechanisms capable of addressing risks that extend beyond individual harm, whereas Gil (2009) argued that criminal legal protection must continuously evolve in response to new forms of injury arising from societal transformation. Accordingly, cyber criminal law simultaneously protects both individual and supra-individual legal interests that sustain public trust in the digital ecosystem.

Criminal Investigation and Prosecution

The investigation of cybercrime presents distinctive challenges arising from the intangible nature of digital evidence and the speed with which it can be altered, concealed, or permanently deleted. Unlike conventional criminal investigations, the collection of evidence in cybercrime cases requires specialized expertise in digital forensics, electronic evidence preservation, and the forensic analysis of digital records. Cuadrado Salinas (2010) argued that criminal investigations must be conducted through rigorous procedural frameworks that ensure both the legality of investigative actions and the evidentiary admissibility of the materials obtained throughout the proceedings.

Digital investigative techniques encompass the forensic examination of electronic devices, the recovery of deleted data, Internet Protocol (IP) address tracing, analysis of connection logs, server inspections, and the use of specialized digital forensic tools. These investigative measures must strictly adhere to the principles of legality, proportionality, and due process, thereby preventing unjustified interference with the fundamental rights of individuals under investigation. Pérez Gil (2018) maintained that technologically assisted investigative measures require a continuous balance between the effectiveness of criminal prosecution and the protection of the right to privacy, particularly when they involve access to digitally stored personal information.

Electronic evidence has become one of the cornerstone elements in criminal proceedings involving cybercrime. Emails, browsing histories, digital files, metadata, communications exchanged through virtual platforms, and evidence extracted from electronic devices constitute evidentiary materials whose authenticity and reliability must be guaranteed through appropriate technical protocols. Romero Sánchez (2015) emphasized that the admission of digital evidence requires procedural mechanisms capable of ensuring an unbroken chain of custody and preserving the integrity of electronic information throughout every stage of the criminal investigation, thereby preventing alterations that could undermine its evidentiary value.

The transnational nature of cybercrime makes international cooperation among judicial authorities, law enforcement agencies, and specialized institutions indispensable. Many cyberattacks are orchestrated simultaneously across multiple jurisdictions, significantly complicating offender identification and the collection of admissible evidence. Doreste Armas (2017) highlighted that international judicial cooperation constitutes an essential instrument for combating criminal organizations operating through globally interconnected digital networks by promoting mutual legal assistance, information sharing, and legislative harmonization aimed at enhancing the effectiveness of criminal prosecution.

Regulatory Framework

The legal framework governing cybercrime comprises domestic criminal legislation, international legal instruments, and technical standards designed to safeguard the security of digital systems. The continuous evolution of digital technologies requires States to update their legal frameworks periodically in order to incorporate emerging forms of cybercrime and strengthen investigative mechanisms. Salazar Mendoza (2023) argued that an effective legal response to cybercrime requires a comprehensive regulatory framework integrating prevention, criminal prosecution, and international cooperation as the fundamental pillars of contemporary criminal policy.

At the domestic level, numerous jurisdictions have enacted specific criminal offenses addressing unauthorized access to computer systems, unlawful interception of communications, data manipulation, electronic fraud, and attacks against critical infrastructure. Nevertheless, considerable disparities persist among national legal systems, thereby hindering the development of a consistent legal response to offenses of a transnational nature. Guerrero Pérez and Toro Álvarez (2026) observed that Latin American criminal justice systems continue to face substantial challenges in harmonizing their legal frameworks with the rapid evolution of digital criminality and the increasing demands arising from international judicial cooperation.

At the international level, the Budapest Convention on Cybercrime constitutes the principal legal instrument for the harmonization of cybercrime legislation, promoting the standardized criminalization of unlawful conduct while strengthening international cooperation among States. Concurrently, international cybersecurity and data protection standards complement criminal law responses through preventive policies designed to reduce technological vulnerabilities. Vilchez Limay (2020) emphasized that international legal instruments acquired particular significance during the COVID-19 pandemic due to the substantial increase in criminal activities perpetrated through digital environments. Likewise, Bazurto Mecías et al. (2024) underscored that the protection of personal data has become one of the fundamental pillars of the contemporary regulatory framework addressing digital criminality.

Contemporary Challenges

The continuous evolution of digital technologies presents persistent challenges for cyber criminal law and for the institutions responsible for combating cybercrime. The anonymity provided by numerous digital platforms, the widespread use of virtual private networks (VPNs), encryption technologies, and decentralized systems significantly complicate the

identification of offenders while reducing the effectiveness of traditional investigative methods. Soriano Silva (2025) argued that the increasing technological sophistication of criminal organizations necessitates the development of more flexible prosecution strategies supported by specialized technical expertise and sustained international cooperation.

Another major challenge stems from the inherently transnational character of cybercrime, as a single cyberattack may simultaneously involve victims, servers, financial intermediaries, and perpetrators located in multiple jurisdictions. This reality generates jurisdictional conflicts, complicates the acquisition of digital evidence, and often delays international mutual legal assistance procedures. Tenorio Pereyra (2018) explained that State accession to international legal instruments, particularly the Budapest Convention on Cybercrime, strengthens coordination among competent authorities and facilitates a more effective response to cyber offenses with global reach.

The rapid expansion of cryptocurrencies, digital assets, and decentralized financial platforms has also created new opportunities for money laundering, electronic fraud, and other forms of economic crime. At the same time, artificial intelligence, automation, and other emerging technologies continuously expand the possibilities for increasingly sophisticated forms of cybercriminal conduct. Játiva Aguirre et al. (2025) argued that twenty-first-century criminology must adopt interdisciplinary approaches capable of explaining the complex interaction between technological innovation and criminal behavior. Along similar lines, Carrillo (2023) maintained that digital transformation simultaneously creates unprecedented opportunities for social and economic development while posing significant challenges to public security. Consequently, effective responses require dynamic criminal policies, continuously updated legislation, strengthened institutional capacities, and enhanced international cooperation to ensure the effective protection of fundamental rights and cybersecurity within contemporary digital environments.

Discussion

The findings of this study demonstrate that cybercrime constitutes a profound transformation of traditional criminality, driven by the rapid advancement of digital technologies and society's increasing reliance on information systems. The analyses of Mateos Pascual (2013) and Peña Labrin (2023) converge in recognizing that technological innovation has significantly increased both the prevalence and the complexity of cyber offenses, thereby requiring more dynamic and adaptive criminal law responses. These findings are consistent with the arguments advanced by Arteaga González (2021), who maintained that cyber criminal law must evolve continuously to address emerging forms of criminal conduct that develop at a pace exceeding that of conventional legislative processes.

Another significant finding concerns the broad diversity of cybercrime typologies identified through the literature review. Offenses involving unauthorized access to computer systems, computer fraud, personal data breaches, cyber harassment, and digital economic crimes demonstrate that cybercrime can no longer be regarded as an isolated phenomenon but rather as a complex spectrum of highly specialized criminal activities affecting multiple legally protected interests. In this regard, the contributions of Macías-Lara et al. (2022), Ponce Tubay (2024), and Bascur and Sepúlveda (2022) underscore that the continuous modernization of criminal legislation is essential for addressing emerging forms of cybercriminality resulting from technological innovation and the expansion of digital services.

The review also revealed broad doctrinal consensus regarding the expansion of the legally protected interests safeguarded by cyber criminal law. Whereas criminal law traditionally focused primarily on the protection of property, contemporary legal frameworks increasingly recognize the importance of safeguarding information, privacy, cybersecurity, and the integrity of digital systems. In this context, Araúz Ulloa (2003) argued that criminal law intervention derives its legitimacy from the protection of legally protected interests that are

essential to social coexistence, while García Arroyo (2022) explained that technological development has fostered the recognition of supra-individual legal interests whose protection is indispensable for ensuring the effective functioning of the digital society. This evolution demonstrates that cybercrime extends far beyond economic harm, directly threatening fundamental rights associated with human dignity, individual liberty, and personal security.

Regarding criminal investigation and prosecution, the findings indicate that the effectiveness of judicial proceedings depends largely on the incorporation of specialized technical capabilities for the management and analysis of digital evidence. The contributions of Cuadrado Salinas (2010), Romero Sánchez (2015), and Pérez Gil (2018) consistently emphasize that the collection, preservation, authentication, and evaluation of electronic evidence constitute decisive factors in ensuring criminal proceedings that simultaneously respect due process guarantees and effectively address technologically sophisticated criminal organizations. Similarly, Doreste Armas (2017) highlighted that international judicial cooperation has become an indispensable component of cybercrime investigations, particularly where offenses and perpetrators are dispersed across multiple jurisdictions.

With respect to the regulatory framework, the present study found that although numerous countries have strengthened their legislation addressing cybercrime, substantial regulatory disparities continue to hinder effective criminal prosecution. The analyses of Salazar Mendoza (2023) and Guerrero Pérez and Toro Álvarez (2026) demonstrate that legislative reforms remain insufficient to keep pace with the rapid evolution of digital threats. Furthermore, Vilchez Limay (2020) emphasized the significance of the Budapest Convention on Cybercrime as the principal international benchmark for legislative harmonization, while Bazurto Mecías et al. (2024) identified personal data protection as one of the fundamental pillars of contemporary cybersecurity and crime prevention policies.

Finally, the review indicates that the future challenges confronting cyber criminal law will be closely associated with the expansion of emerging technologies, the increasing use of cryptocurrencies, artificial intelligence, online anonymity, and the consolidation of transnational criminal organizations. Within this context, Tenorio Pereyra (2018), Játiva Aguirre et al. (2025), and Soriano Silva (2025) concur that governmental responses cannot be limited solely to strengthening criminal legislation but must also incorporate preventive strategies, international cooperation, continuous professional training for criminal justice practitioners, and the development of specialized technological capabilities. Consistent with Carrillo (2023), public security in the twenty-first century will largely depend upon the capacity of States to adapt their criminal policies to the pace of technological innovation while simultaneously safeguarding fundamental rights and ensuring the effective prosecution of cybercrime within increasingly complex digital environments.

Conclusions

Cybercrime has emerged as one of the most significant threats to legal certainty within the digital society owing to the continuous evolution of information and communication technologies. Its dynamic, transnational, and highly specialized nature has fundamentally transformed traditional patterns of criminality, creating new risks for individuals, organizations, and States alike. Consequently, cyber criminal law must evolve continuously to respond effectively to emerging forms of cybercrime and to ensure adequate protection of the legally protected interests affected by digital criminal activity.

The analysis conducted in this study identified unauthorized access to computer systems, electronic fraud, data-related offenses, cyber harassment, and digital economic crimes as the principal categories of cybercrime. These forms of criminal conduct demonstrate that information, privacy, cybersecurity, and property constitute essential legally protected interests whose effective safeguarding requires continuously updated legal frameworks,

specialized investigative procedures, and the proper incorporation and management of electronic evidence within criminal proceedings.

Furthermore, the study concludes that the effectiveness of criminal prosecution depends not only on the strengthening of domestic legislation but also on enhanced international cooperation, legislative harmonization, and the development of specialized technical expertise among criminal justice professionals. The challenges posed by online anonymity, cryptocurrencies, artificial intelligence, and transnational cybercriminal organizations require comprehensive public policies integrating prevention, investigation, prosecution, sanction, and digital education. In this context, strengthening cyber criminal law constitutes an indispensable prerequisite for ensuring legal certainty, protecting fundamental rights, and fostering a secure, trustworthy, and resilient digital environment capable of addressing the technological challenges of the twenty-first century.

Study Limitations

The primary limitation of this study lies in its documentary nature, as the analysis was based exclusively on the review of scientific literature, legal doctrine, and the applicable regulatory framework. Consequently, it did not incorporate empirical evidence derived from field research or the application of quantitative or qualitative methodologies involving stakeholders engaged in the investigation and prosecution of cybercrime.

Future Research

Future research should prioritize empirical and comparative studies assessing the effectiveness of criminal justice systems in addressing cybercrime. Particular attention should be devoted to examining the impact of artificial intelligence, cryptocurrencies, and other emerging technologies on the evolution of cyber offenses, as well as their implications for the continuous adaptation of national and international legal frameworks.

Acknowledgments

The author expresses sincere gratitude to the scholars and experts in criminal law, cyber law, and cybersecurity whose academic and scientific contributions enriched the development of this research. The author also acknowledges the valuable work of fellow researchers, peer reviewers, and the authors of the scholarly publications consulted, whose contributions strengthened the critical analysis of cybercrime and the contemporary challenges confronting cyber criminal law.

Declaration of Conflict of Interest

The author expressly declares that there are no personal, professional, academic, institutional, or financial conflicts of interest that could have influenced the design, conduct, analysis, interpretation of the findings, or publication of this scientific article.

Referencias

- Acosta Sila, C. D. R., Jácome Veliz, G. D. L., & Morejón Llanos, S. P. (2026). La Debilidad Normativa en Delitos Informáticos en Ecuador: Un Análisis Crítico del Coip y Lopdp. *ASCE MAGAZINE*, 5(2), 2747-2765.
- Acosta, M. G., Benavides Benalcázar, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia: RVG*, 25(89), 351-368.
- Araúz Ulloa, M. (2003). El bien jurídico protegido. *Revista de Derecho*, (6), 105-119.
- Arteaga González, C. D. (2021). Ciberdelincuencia: a propósito del derecho penal informático en Colombia. *Episteme. Revista de Estudios Socioterritoriales*, 13(1), 38-47.

- Bascur, G., & Sepúlveda, R. P. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, primera parte. *Revista de Estudios de la Justicia*, (37).
- Bazurto Mecias, C. J., Jurado Cabello, Y. K., Sifa Mueses, L. M., & Reinoso Paredes, A. G. (2024). La ciberdelincuencia y la protección de datos personales. *Sinergia Académica*, 7(Especial 5), 594-612. DOI: <https://doi.org/10.51736/sjq7b043>
- Botero Bernal, A. (2003). La metodología documental en la investigación jurídica: alcances y perspectivas. *Opinión Jurídica* vol. 2, No. 4 pp. 109-116
- Buzai, G. D. (2001). Paradigma Geotecnológico, Geografía Global y CiberGeografía, la gran explosión de un universo digital en expansión. *GeoFocus. International Review of Geographical Information Science and Technology*, (1), 24-48.
- Carrillo, R. M. (2023). Retos de la Seguridad Pública ante los Cambios Digitales: Una Nueva Era de Oportunidades y Desafíos Public Safety Challenges in the Face of Digital Changes: A New Era of Opportunities and Challenges. *La investigación: para resolver un problema, antes hay que identificarlo*.
- Catá del Palacio, A. (2014). Ciberdelincuencia. Desarrollo y persecución tecnológica. [Tesis de Grado, Universidad Politécnica de Madrid]. <https://oa.upm.es/34795/>
- Conde-Pumpido Tourón, C. (2006). El Ministerio Fiscal frente a la nueva criminalidad. *Eguzkilore: cuaderno del Instituto Vasco de Criminología*, (26).
- Contreras López, R. E. (2019). El estudio multidisciplinario del fenómeno criminal: necesidad de una metodología desde la investigación jurídica. *Derecho Penal y Criminología*, 40(108), 159-179.
- Cuadrado Salinas, C. (2010). *La investigación en el proceso penal*. La Ley.
- Del Pino, S. A. (2016). Delitos informáticos: generalidades. [Tesis de grado, Universidad de San Marcos]. URI: <localhost/xmlui/handle/11506/2374>
- Doreste Armas, D. C. (2017). El espacio judicial europeo y la fiscalía europea como órgano de investigación y persecución penal; versus modelo procesal español. *Diario La Ley*, (8981), 1.
- Gala Rodríguez, L. A. (2026). La cibercriminalidad en México: entre la dispersión normativa y la impunidad digital. *Revista Multidisciplinar Epistemología De Las Ciencias*, 3(1), 399-429. <https://doi.org/10.71112/d3625c91>
- García Arroyo, C. (2022). Sobre el concepto de bien jurídico. Especial consideración de los bienes jurídicos supraindividuales-institucionales. *Revista electrónica de ciencia penal y criminología*, 24.
- García-Machado, E., & León-Santos, M. (2021). ¿Evolución o expansión? Del marketing tradicional al marketing digital. *Alcance*, 10(26), 37-52.
- Gil, A. D. (2009). Sobre el bien o bienes jurídicos protegidos en los denominados delitos contra la Administración pública. *Anuario de derecho penal y ciencias penales*, (1), 357-424.
- Goscilo, A. (1981). Los bienes jurídicos penalmente protegidos. *Lecciones y Ensayos*, (46-01), 25-39.
- Guerrero Pérez, C., & Toro Álvarez, M. D. G. (2026). Ciberdelincuencia y criminalidad digital: retos del sistema penal colombiano. [Tesis de grado, Universidad Libre de Colombia]. <https://hdl.handle.net/10901/32341>
- Játiva Aguirre, S. E., Hernández Córdova, H. E., Rojas Barros, N., Villalta León, J. A., & Palacios Duarte, S. A. (2025). Criminología del Siglo XXI: delincuencia, perfiles criminales y nuevos desafíos globales. *Editorial Tecnocientífica Americana*, 300, 1-126. DOI: <https://doi.org/10.51736/91>

- Macías-Lara, R. A., Andrade, M. F. B., Angulo, F. Q., Loor, J. J. M., Estupiñan-Troya, G., & Vizuite, J. D. R. (2022). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. *Sapientia: International Journal of Interdisciplinary Studies*, 3(2), 231-243.
- Mateos Pascual, I. (2013). *Ciberdelincuencia: desarrollo y persecución tecnológica*. [Tesis de Grado, Universidad Politécnica de Madrid]. <https://oa.upm.es/22176/>
- Mora Pedreros, P. A., Gutiérrez, D., & Santiago Pajajoy, M. J. Los entornos virtuales: un escenario de producción, acción y protección del conocimiento. *LIBRO DE RESÚMENES*, 597.
- Navarro, S. S. (2005). Concreción y lesión de los bienes jurídicos colectivos. *Anuario de derecho penal y ciencias penales*, (3), 887-918.
- Packer, M. (2018). *La ciencia de la investigación cualitativa*. Universidad de los Andes. Colombia, <https://repositorio.uniandes.edu.co/login>
- Pardo Mateos, R. J. (2013). Fenomenología del delito: delincuencia tradicional y nuevas formas de delincuencia. *Investigación policial y sus consecuencias jurídicas*, 97-138.
- Peña Labrin, D. E. (2023). Ciberdelitos y criminalidad informática: Rol de la prevención en la expansión de la ciberdelincuencia. *Informática y Derecho: Revista Iberoamericana de Derecho Informático (segunda época)*, (13), 57-72.
- Pérez Gil, J. (2018). Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución. In *Informatica giuridica e informatica forense al servizio della società della conoscenza: scritti in onore di Cesare Maioli* (pp. 187-198). Aracne.
- Ponce Tubay, M. A. (2024). Delitos informáticos: Caso Ecuador. *Revista San Gregorio*, 1(58), 119-123. <https://doi.org/10.36097/rsan.v1i58.2667>
- Riofrío Martínez-Villalva, J. (2018). La selección del método en la investigación jurídica. 100 métodos posibles. *Revista de educación y derecho = Education and law review*. No 12, 87-113
- Romero Sánchez, A. (2015). Proceso penal, privacidad y autodeterminación informativa en la persecución penal de la delincuencia organizada: un análisis desde la perspectiva del derecho procesal penal alemán. *Criminalidad*, 57(2), 319-333.
- Salazar Mendoza, J. A. (2023). Ciberdelincuencia; marco normativo y respuesta policial. [Trabajo de grado, Universidad Pontificia Comillas]. <http://hdl.handle.net/11531/69396>
- Santillán Molina, A. L., & Vinuesa Ochoa, N. V. (2020). El entorno virtual íntimo y privado como Derecho Humano de nueva generación. *Revista Uniandes Episteme*, 7, 1034-1047. Recuperado a partir de <https://revista.uniandes.edu.ec/ojs/index.php/EPISTEME/article/view/2280>
- Saura, G. (2025). El capital, la tecnología digital y la educación. *Revista Española de Educación Comparada*, (48), 11-30.
- Soriano Silva, A. (2025). La evolución de la ciberdelincuencia en España. Retos y tendencias actuales. [Tesis de grado, Universidad Europea]. URI: <https://hdl.handle.net/20.500.12880/13770>
- Tenorio Pereyra, J. E. (2018). Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia. [Tesis de Master, Universidad Diplomática del Perú, Javier Pérez de Cuellar]. <http://repositorio.adp.edu.pe/handle/ADP/71>
- Vilchez Limay, R. C. (2020). La ciberdelincuencia en el contexto de la pandemia del coronavirus: una aproximación desde el marco convencional. *AIS: Ars Iuris Salmanticensis*: 8, 2, 2020, 21-25.