Revista Electrónica de Ciencia Penal y Criminología
ISSN 1695-0194

RESEARCH ARTICLES
RECPC 27-13 (2025)

Applying Classical Criminological Theories to Cyberspace: A Scoping Review of Limits and Convergences

Isadora Barbosa Coelho*
Universidade Federal de Minas Gerais (UFMG), Brazil

Bráulio Figueiredo Alves da Silva
Universidade Federal de Minas Gerais (UFMG), Brazil

Barbosa Coelho, Isadora and Alves da Silva, Bráulio Figueiredo. Applying Classical Criminological Theories to Cyberspace: A Scoping Review of Limits and Convergences. *Revista Electrónica de Ciencia Penal y Criminología*. 2025, núm. 27-13, pp. 1-25.

Abstract: The accelerated growth of cybercrime in recent decades has established itself as one of the main contemporary challenges to public security, driven by the expansion of digital technology use, the anonymity of cyberspace, and the fragility of traditional social control mechanisms. Despite the increasing complexity of cybercrimes, it is noted that predominant approaches remain anchored in technical-legal responses, which reveals a gap in the analysis of the social, cultural, and behavioral dimensions that sustain these practices. Given this scenario, the present article aims to analyze to what extent classical criminological theories remain capable of explaining cybercrimes, highlighting their potential and limits when applied to the digital environment. Methodologically, the study adopts a qualitative approach of a theoretical nature, based on a scoping analysis and a narrative literature review, with a temporal scope between 2010 and 2024. Routine Activity Theory, Anomie Theory, Social Learning Theory, and Deterrence Theory are mobilized in a comparative manner. The results suggest that understanding cybercrime requires the articulation between the expansion of opportunities, normative deregulation, learning processes in digital subcultures, and the reduced perception of risk. It is concluded that classical criminology remains relevant for understanding cybercrimes, provided it is reinterpreted in light of the specificities of the contemporary digital context.

Keywords: Cybercrime, Classical Criminology, Theoretical Criminology, Sociology of Crime, Cyberspace, Cybercrime and Technology.

Received Date: 19 September 2025
Date of Publication in RECPC: 12 December 2025
Contact: barbosaisadora@hotmail.com

I. Introduction

1. *Between Algorithms and Norms: The Sociotechnical Context of Cybercrime*

In recent years, digital globalization and the intensification of information technology use have profoundly reshaped social, economic, and institutional interactions in our society[1,2,3]. The expansion of internet access and the incorporation of digital technologies into people's daily lives have broadened the possibilities for communication, consumption, and information flow, which has also resulted in the creation of new practices of illicit conduct[4]. In this scenario, cybercrimes have consolidated as one of the primary focuses in contemporary debates on public security, especially given the rise of technologies such as blockchain, the metaverse, and artificial intelligence, which characterize the Web 3.0 era[5].

Cybercrime, also known as computer crime, according to Holt and Bossler[6], is adopted to designate offenses that can occur in online environments. The authors justify this definition by arguing that technological evolution has allowed virtually all modern computing devices to have internet access, drastically increasing the potential for misuse of cyberspace and including criminal modalities such as deviations perpetrated through the digital network [7,8]. These activities range from the dissemination of malicious software, system intrusions, and denial-of-service attacks to crimes of an economic and informational nature, such as digital fraud, extortion, and the misappropriation of personal data. Such conducts exploit technical and behavioral vulnerabilities, favoring financial or symbolic gains[9] with a low risk of criminal accountability, primarily due to the decentralization and anonymity inherent to cyberspace[10].

Available data reinforce the relevance of this phenomenon. In Brazil, in 2022 alone, approximately 103 billion cyberattack attempts were recorded, representing about 30% of occurrences in all of Latin America and the Caribbean. On a global

[1] Kerr, O. S. (2003). Cybercrime's scope: Interpreting'access' and'authorization'in computer misuse statutes. *New York University Law Review*, *78*(5), 1596.
[2] Wall, D. (2021). The Transnational Cybercrime Extortion Landscape and The Pandemic: Ransomware and changes in offender tactics, attack scalability and the organisation of offending. *European Law Enforcement Research Bulletin*.
[3] Akers, R. (2017). *Social learning and social structure: A general theory of crime and deviance*. Routledge.
[4] Merton, R. K. (1970). *Social structure and anomie.* In Sociology: Theory and structure (M. Maillet, Trans.; pp. 197–228). Mestre Jou.
[5] McGuire, M. (2012). *Technology, Crime and Justice: The Question Concerning Technomia*. Routledge.
[6] Holt, T., & Bossler, A. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.
[7] Beccaria, C. (2016). *On crimes and punishments*. Transaction Publishers.
[8] Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and justice*, *42*(1), 199-263.
[9] Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, *8*(1), 1-20.
[10] Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity.

scale, the growth trend also exists, with the blocking of about 161 billion cyber threats in 2023, a number that indicates a significant increase compared to the previous year. These indicators demonstrate that cybercrimes have ceased to be isolated episodes to become one of the main contemporary challenges to public and institutional security[11].

Qualitatively, the nature of these threats has also worsened. Wall[12] points out that, along with ransomware, data theft has consolidated as one of the main global threats, recording a 160% increase since 2019. Such crimes are classified as "keystone cybercrimes" because they facilitate the commission of other future offenses through the sale of this information in illegal markets.

Although they often do not involve direct physical violence, cybercrimes impact health and public safety. Their consequences go beyond financial losses, affecting the psychological well-being of victims, trust in institutions, and the integrity of critical infrastructures. This scenario became even more evident during periods of intensified use of digital technologies, when essential institutions, such as those in the healthcare area, began to figure among the main targets of cyberattacks, demonstrating structural fragilities in digital protection[13].

Despite the complexity of the phenomenon, institutional and academic responses still prioritize technical-legal solutions, neglecting sociological, symbolic, and structural aspects[14]. Tackling the problem has prioritized the development of information security tools, digital defense systems, and the updating of legal frameworks, often without deepening the analysis of the social and behavioral dimensions that sustain the practice of these offenses. In this sense, it is possible to note a limitation in traditional approaches, which tend to treat cybercrime as a strictly technological or normative problem, neglecting its insertion in broader social dynamics.

It is at this point that classical criminology becomes relevant for understanding cybercrimes. Although formulated in historical contexts prior to the consolidation of the digital environment, classical criminological theories offer analytical instruments capable of explaining how social, cultural, and structural factors influence the occurrence of crime. The application of these theories to cyberspace allows for the understanding of the offense not only as a result of technical failures but as a product of social routines, fragilities in social control, learning processes,

[11] ABES – Brazilian Association of Software Companies. (2024). 2023 ends with 161 billion cyberattacks, in another record, according to a report by Trend Micro.

[12] Wall, D. (2021). The Transnational Cybercrime Extortion Landscape and The Pandemic: Ransomware and changes in offender tactics, attack scalability and the organisation of offending. *European Law Enforcement Research Bulletin*.

[13] Lourenço, A. C. G., Dos Santos, C. E. P., de Almeida, G. H., & de Castro, B. V. (2023). O aumento dos crimes cibernéticos durante a pandemia da Covid-19 e as dificuldades para combatê-los. *LIBERTAS DIREITO*, *4*(1).

[14] McGuire, M. (2012). *Technology, Crime and Justice: The Question Concerning Technomia*. Routledge.

and contexts of normative deregulation. The emergence of cybercrime, therefore, demands a need to understand the phenomenon as a product of a new form of organization of social life.

The transformations in daily activities, driven by the centrality of the internet in social life, exemplify this relationship. In Brazil, the average daily internet connection time exceeds nine hours, which significantly expands individuals' exposure to potentially insecure digital environments[15]. The migration of social, economic, and educational activities to the digital medium has altered criminal opportunities, reducing certain in-person offenses but favoring the emergence and growth of cybercrimes[16]. These changes highlight the relevance of criminological approaches that consider the reorganization of social routines and their implications for criminality.

Furthermore, the digital environment is characterized by high levels of anonymity and the fragility of social control mechanisms, elements that contribute to states of loosening social rules. The dissociation between physical identity and virtual identity weakens traditional social norms, favoring deviant behavior and reducing the perception of individual accountability[17]. This condition dialogues directly with the assumptions of Anomie Theory, by highlighting how the absence or insufficiency of effective norms in cyberspace creates fertile ground for digital criminality, especially in contexts marked by inequalities and pressures for material success[18].

In parallel, cyberspace also favors the learning processes of criminal behavior. Online communities, forums, and social networks function as socialization spaces where illicit techniques (concomitantly with socially accepted behaviors) are shared, normalized, learned, and reinforced. Exposure to delinquent digital subcultures enables not only the acquisition of technical knowledge but also the internalization of definitions favorable to crime, justifying and legitimizing illegal practices[19]. This scenario highlights the current relevance of Social Learning Theory for the understanding of cybercrime.

Despite the existence of studies that apply criminological theories to cybercrime, a significant gap is still observed regarding the comparative theoretical

[15] Kahn, T. (2023). Migration from violent street crimes to digital crimes. *Fonte Segura*.
[16] Figueiredo, B., & Miró Llinares, F. (2024). Digital life and crime trends in the global south: on the impact of increased Internet use on opportunities for crime. *Revista Espanola de Investigacion Criminologica*, *22*(2).
[17] Suxberger, A. H. G., & Pacheco, W. E. P. (2019). A TEORIA DA ANOMIA NOS CRIMES CIBERNÉTICOS: THEORY OF ANOMIE APPLIED TO CYBERCRIME. *Delictae Revista de Estudos Interdisciplinares sobre o Delito*, *4*(7), 104-125.
[18] Costa, D. B. d. (2022). Social structure and anomie: Aspects of contemporary criminality, analyzed from the works of Durkheim, Merton, and Young. *Journal of the Public Defender's Office of the State of Rio Grande do Sul*, *6*, 79–100.
[19] Aguiar, J. C., & Medeiros, M. A. (2024). The social learning theory of criminal behavior. *Brazilian Journal of Criminal Sciences*, *184*.

systematization of these approaches. A large part of academic production remains fragmented, addressing theories in isolation and without a consistent effort of analytical integration, which limits a holistic understanding of the phenomenon. To face this challenge, we adopted a methodological approach capable of mapping the field in a structured way based on the scoping analysis that will be detailed below.

In doing so, this article proposes a re-reading of the main classical criminological theories applied to cybercrime, discussing their explanatory potentials and limitations. By integrating situational, normative, interactional, and rational perspectives, we seek to demonstrate that classical criminology—although formulated and conceived for a context of events in the physical environment—still offers a robust theoretical framework,

redefined through the lens of digital criminology and adapted to the complexity of Web 3.0.

II. How we Read the Literature: Narrative Review and Scoping as an Analytical Strategy

This article employs a methodological approach of a qualitative and theoretical nature, with the central objective of analyzing the explanatory capacity of classical criminological theories regarding the phenomenon of cybercrime. An analytical-conceptual investigation was carried out, which does not seek to produce original empirical evidence, but rather to systematize, critically interpret, and compare consolidated theoretical models of criminology when applied to the contemporary digital context.

The adopted method consists of a scoping analysis, operationalized through a narrative literature review combined with a comparative analysis, which, according to Lijphart[20], constitutes a basic scientific method for discovering empirical relationships between variables and establishing general propositions. The choice of scoping analysis is justified by the need to map, organize, and broadly interpret how different classical criminological theories have been mobilized to explain cybercrime, identifying convergences, gaps, and explanatory limits. Unlike systematic reviews or meta-analyses, scoping analysis[21] allows for greater interpretive flexibility, being particularly suitable for theoretical fields in consolidation or marked by conceptual diversity, as is the case with the application of classical criminology to cybercrime.

The narrative review, adopted because it enables critical interpretation and the

[20] Lijphart, A. (1971). Comparative Politics and the Comparative Method. *American political science review*, *65*(3), 682-693.
[21] Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*, *8*(1), 19-32.

deepening of theoretical understanding beyond data aggregation[22], was conducted in a structured manner, focusing on identifying academic productions that simultaneously engaged with two central dimensions: classical criminological theories and the phenomenon of cybercrimes. Bibliographic searches were performed in recognized academic databases, including the CAPES Journals Platform, SciELO, Google Scholar, and DOAJ, prioritizing peer-reviewed articles, books, book chapters, theses, and technical reports. The temporal scope covered publications between 2010 and 2024, in Portuguese and English, in order to capture both consolidated contributions and more recent debates.

Eligibility criteria were defined based on the theoretical relevance of the publications to the study's objectives. Included were productions that discussed classical criminological theories applied directly or indirectly to the context of cybercrime, as well as works addressing digital crimes from a sociological, criminological, or behavioral perspective. Studies centered exclusively on technical-legal, technological, or computer engineering approaches without an interface with criminology were excluded, as were merely descriptive researches on cyberattacks that did not present a consistent theoretical dialogue.

The bibliographic search initially resulted in the identification of a broad set of publications, subsequently refined based on the previously defined theoretical eligibility criteria. Priority was given to studies establishing a direct dialogue between classical criminological theories and the phenomenon of cybercrime, forming an analytical selection aligned with the article's objectives. After reading the titles, abstracts, and, where relevant, the full texts, the final corpus was constituted by theoretical and empirical studies considered central to the proposed analysis.

This procedure follows the guidelines proposed by Arksey and O'Malley[23] for scoping studies, which emphasize conceptual mapping and the interpretive systematization of emerging theoretical fields over strict criteria of statistical exhaustiveness. The choice of this method allows for greater analytical flexibility, suited to the conceptual diversity that marks the application of classical criminology to the digital environment.

The selection of studies occurred in multiple stages. Initially, a broad survey was conducted using descriptors related to both cybercrime and classical criminological theories.

The figure illustrates the methodological decision process/stages. The initial search retrieved 179 documents. After the first screening (removal of duplicates, news, articles not relevant to the research), 120 works remained. The application of

[22] Greenhalgh, T., Thorne, S., & Malterud, K. (2018). Time to challenge the spurious hierarchy of systematic over narrative reviews? *European Journal of Clinical Investigation*, *48*(6), e12931.
[23] Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*, *8*(1), 19-32.

eligibility criteria (focus on the interface between cybercrime and criminological theory, excluding purely technical-legal approaches) reduced the sample to 47 articles. After full reading and verification of adherence to the variables of the analytical spreadsheet, 30 studies composed the final sample.

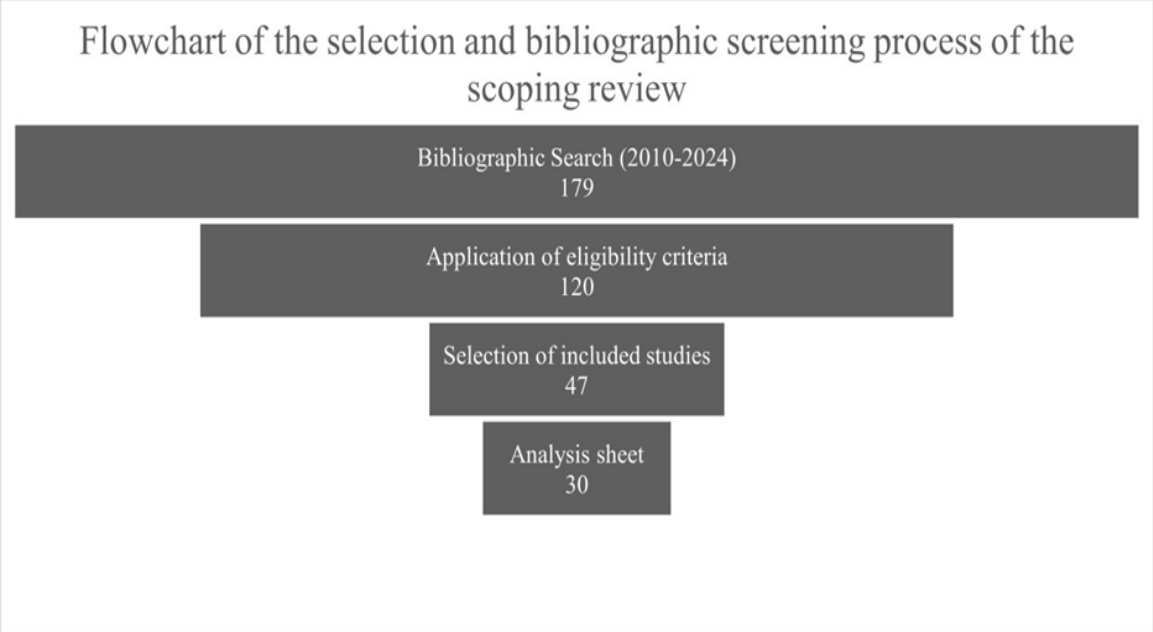

Figure 1: Sample Refinement: From Raw Search to Final Selection by Eligibility Criteria

After the selection stage of the eligible studies, the works included in the review were organized into analytical spreadsheets with the objective of systematizing information and enabling comparative analysis between the theoretical approaches mobilized. Each study was categorized based on five central axes:

(i) Predominant criminological theory, explicitly identifying which classical approach grounded the analysis.

(ii) Research problem, synthesizing the central question investigated by the author in the context of cybercrime.

(iii) Source of data, distinguishing studies of a theoretical, empirical, or mixed nature, as well as the type of material used (secondary databases, surveys, documentary analyses, case studies, or literature reviews).

(iv) Analytical variables, recording the main concepts, dimensions, or indicators mobilized to operationalize the theory in the digital environment. And, (v) modern studies and theoretical updates, indicating how each work dialogued with contemporary adaptations of classical theories or with recent contributions from digital criminology. This systematization allowed for the identification of recurring patterns, analytical convergences, and explanatory gaps, in addition to supporting the comparison between theories regarding their scope, limits, and capacity for adaptation to the context of cyberspace.

The methodological procedure adopted, from the bibliographic search to the comparative analysis of the studies, is synthesized in the flowchart presented in the figure below:

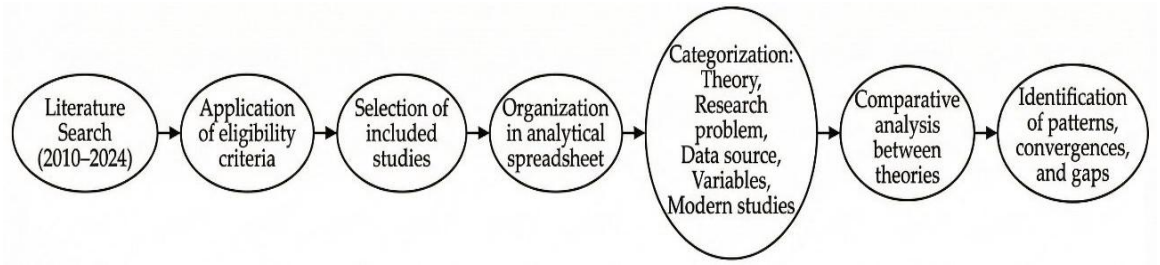

Figure 2: Flowchart of the Methodological Procedure and Analytical Organization of Studies

The data extraction and analysis followed a manual and interpretive procedure, guided by previously defined analytical categories. For each study included, elements such as the criminological theory addressed, the central concepts mobilized, the application context, the contributions to the understanding of cybercrime, and the theoretical limitations pointed out by the authors themselves were considered. These data served as the basis for the comparative analysis developed throughout the article, allowing for an evaluation of how each theory explains certain aspects of cybercrime and which dimensions remain insufficiently addressed.

The evaluation of the methodological quality of the studies did not follow standardized protocols, such as risk-of-bias assessment instruments used in empirical research, since this is essentially a theoretical investigation. Instead, a critical-interpretive criterion was adopted, based on conceptual relevance, internal coherence of arguments, the timeliness of contributions, and the suitability of the studies to the article's objectives. It is recognized, however, that methodological limitations exist, especially related to the dependence on specific keywords, linguistic scope, and the involuntary exclusion of productions in other languages.

Finally, the synthesis of the results was carried out through a qualitative comparative analysis, articulating the four selected theories based on their main explanatory axes. The decision to work only with Routine Activity Theory, Anomie Theory, Social Learning Theory, and Deterrence Theory stems from their recurrence in the literature and their explanatory potential regarding the dynamics of cybercrime, verified by the extraction of the selected articles. The empirical limitations of the study are reflexively acknowledged, as a characteristic of the scoping analysis itself, whose main objective is to broaden theoretical understanding and support future research, especially of an empirical or mixed-methods nature.

Table 1: Comparative Framework of Criminological Theories Applied to Cybercrime.

Theory	Focus and Central Concept	Practical Application to Cybercrime (Study Findings)	Limits & Relevant and Current Studies
Anomie	Normative deregulation. The dissociation between real and virtual identity weakens norms and favors deviance.	The dissociation between real and virtual identity (anonymity) eliminates moral restraints. Digital crime becomes an acceptable "shortcut" to achieve financial success and status that are unattainable through legal means.	Limits: Ignores technology as a mediator. Ref: Suxberger & Pacheco[24].
Routine Activity	Situational opportunity. Convergence of: Offender + Victim - Guardian.	Hyperconnectivity generates continuous exposure to risk. Crime has migrated from the street to the network. The lack of "guardians" (effective software/laws) stands out.	Limits: Difficult to define a digital "guardian." Ref: Figueiredo Alves Silva & Miró-Llinares[25].
Social Learning	Cultural transmission. Crime is learned in subcultures through interaction and reinforcement.	Forums and the dark web function as "crime schools." The offense is redefined as a "technical challenge" or "game" (gamification), which neutralizes guilt and normalizes conduct among peers.	Limits: Original focus was face-to- face, not anonymous. Ref: Aguiar & Medeiros[26].
Deterrence	Rational Calculation. Cost vs. Benefit. The certainty of punishment inhibits crime.	Rational calculation favors crime: the cost of the attack is low and the profit is high (asymmetry). The certainty of punishment is almost nil due to the technical difficulty of identifying the perpetrator (anonymity/proxies).	Limits: Technical impunity nullifies the fear of the law. Ref: Nagin[27]; Jones[28].

The application of this methodological strategy of scoping analysis resulted in the selection of a representative set of studies dealing with cybercrime through the lens of classical criminological theories. By mapping this literature, we identified the recurring presence of four theoretical traditions that, although distinct in their foundations, have been mobilized to understand the dynamics of crime in digital environments: a) Routine Activity Theory; b) Anomie Theory; c) Social Learning Theory; and d) Deterrence Theory. In the following chapter, we explore how each

[24] Suxberger, A. H. G., & Pacheco, W. E. P. (2019). A TEORIA DA ANOMIA NOS CRIMES CIBERNÉTICOS: THEORY OF ANOMIE APPLIED TO CYBERCRIME. *Delictae Revista de Estudos Interdisciplinares sobre o Delito*, *4*(7), 104-125.
[25] Figueiredo, B., & Miró Llinares, F. (2024). Digital life and crime trends in the global south: on the impact of increased Internet use on opportunities for crime. *Revista Espanola de Investigacion Criminologica*, *22*(2).
[26] Aguiar, J. C., & Medeiros, M. A. (2024). The social learning theory of criminal behavior. *Brazilian Journal of Criminal Sciences*, *184*.
[27] Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and justice*, *42*(1), 199-263.
[28] Jones, S. (2021). The evolution of cybersecurity in the face of cybercrime. *Cybersecurity Research Journal*.

of these approaches has been reinterpreted and applied to the context of cyberspace, highlighting their explanatory potentials, analytical limits, and ways of articulating with one another.

III. Classical Criminological Theories in Debate: Theoretical Rereadings to Understand Digital Crime

In this article, we propose to consolidate the concept of digital criminology, understood as the emerging field that seeks to understand criminality in contexts mediated by digital technologies, considering not only the technical means of the offense but also the cultural, identity, symbolic, and social dynamics that structure cyberspace. Such a perspective implies overcoming purely technical or legal explanations, while simultaneously inviting us to a rereading of classical criminological theories in light of the transformations introduced by the interactional logic of Web 3.0, characterized by decentralization, anonymity, the algorithmization of daily life, and normative volatility. In this context, digital criminology consolidates itself as a theoretical field that rescues, updates, and applies classical models to interpret digital criminality as a multifaceted, transversal phenomenon adaptable to contemporary technological dynamics[29].

The understanding of cybercrime requires theoretical approaches capable of going beyond strictly technical or normative explanations, incorporating social, cultural, and behavioral dimensions that structure criminal practice in the digital environment. In this sense, classical criminological theories remain relevant, provided they are reinterpreted in light of the transformations imposed by the nature of what cyberspace is.

This article adopts four central theoretical perspectives: Routine Activity Theory, Anomie Theory, Social Learning Theory, and Deterrence Theory. The choice of these approaches was due to their explanatory capacity regarding the contemporary dynamics of cybercrime, especially concerning the reorganization of social routines, the weakening of normative control in the digital environment, the formation of online subcultures, and the reduced perception of risk by offenders. Rather than a historical reconstruction of the theories, the adopted focus prioritizes their analytical application to cyberspace, highlighting interpretive potentials and limits.

1. *Digital Routines and Criminal Opportunities: Cyberspace as a Risk Ecology*

Routine Activity Theory, emphasizes the convergence of three elements for the occurrence of an offense: a motivated offender, a potential victim, and the absence of a capable guardian. By shifting the focus from individual motivation to

[29] McGuire, M. (2012). *Technology, Crime and Justice: The Question Concerning Technomia*. Routledge.

situational conditions, this approach proves especially useful in

the analysis of cybercrime, as the reorganization of daily routines in the digital environment, intensified by the dynamics of Web 3.0, structurally expands opportunities for illicit conduct. This rereading, within the scope of digital criminology, points to the need to understand crime not as an isolated event, but as an expression of interactive patterns and social habits mediated by technology.

The incorporation of the internet into daily activities has profoundly transformed how individuals interact, consume information, and conduct transactions. The constant presence in the digital environment, associated with the frequent sharing of personal data and the use of often insecure systems, creates a scenario conducive to the actions of motivated offenders. The continuous exposure of users, combined with the fragility of protection mechanisms, highlights how cyberspace is configured as a risk environment in which criminal opportunities are constantly produced. In this context, cyberspace presents itself as a structured risk environment, where criminal opportunities not only exist but are produced and reproduced by the architecture of digital interaction itself[30].

In the Brazilian context, this dynamic becomes even more evident when observing the high average daily time connected to the internet, which exceeds nine hours[31]. This pattern of intensive use increases the probability of contact between potential offenders and victims in the virtual environment, satisfying one of the central conditions pointed out by the theory. Unlike physical space, where the convergence between offender and victim depends on spatial proximity, in cyberspace this encounter occurs permanently and in a decentralized manner, exponentially expanding criminal opportunities.

Recent studies indicate that the migration of social, economic, and leisure activities to the digital environment has produced significant changes in the configuration of criminality[32]. Conventional crimes have shown a reduction, while cybercrimes grow consistently, confirming the shift of criminal opportunities to the online environment. This evidence reinforces the timeliness of Routine Activity Theory by demonstrating that changes in social routines directly impact the patterns and formats of crime in the digital society.

A decisive aspect for the application of Routine Activity Theory to cyberspace refers to the absence of "capable guardians." In the digital environment, this function is weakened by factors such as the lack of normative standardization, low control capacity, and the difficulty of identifying authors, which contribute as a whole to reducing the risks

[30] Yar, M. (2006). Cybercrime and Society. *SAGE Publications*.
[31] Kahn, T. (2023). Migration from violent street crimes to digital crimes. *Fonte Segura*.
[32] Figueiredo, B., & Miró Llinares, F. (2024). Digital life and crime trends in the global south: on the impact of increased Internet use on opportunities for crime. *Revista Espanola de Investigacion Criminologica*, *22*(2).

perceived by offenders. The anonymity and decentralization of networks make it difficult to identify those responsible and weaken formal social control, creating favorable conditions for the proliferation of cybercrimes. Thus, the theory allows for the understanding of cybercrime as a result of the convergence between victim exposure, the presence of motivated offenders, and the absence of adequate protection.

However, the application of this theory to the digital world is not without conceptual challenges. According to Majid Yar[33], cyberspace imposes a kind of 'spatio-temporal disorganization' that subverts the logic of physical proximity necessary for classical convergence. In the virtual environment, interaction no longer depends on geographic coordinates but manifests at zero distance, where the target is permanently within reach of a click. This fluidity suggests that cybercrime is not just a new guise for old crimes, but a phenomenon that alters the very architecture of opportunity by collapsing traditional barriers of geographic friction.

Although Routine Activity Theory is particularly effective in demonstrating how the reorganization of daily practices in the digital environment structurally expands opportunities for crime, its limits become evident when seeking to understand why such opportunities are exploited systematically and socially tolerated in certain contexts. The situational emphasis of the theory, centered on the convergence of offender, target, and absence of guardians, explains little about the broader normative processes that shape the disposition for deviance. In this sense, it becomes necessary to shift the analysis from the plane of opportunity itself to a structural-normative level, capable of illuminating how the weakening of rules, values, and social expectations in cyberspace creates conditions conducive to the legitimation of criminal behavior. It is precisely at this point that Anomie Theory offers a complementary explanatory contribution.

2. ***Fragile Structures, Fluid Identities: Anomie and Online Crime***

Anomie Theory, originally developed by Émile Durkheim[34] and later reformulated by Robert K. Merton, explores the effects of normative deregulation and the tension between cultural goals and the legitimate means to achieve them. In the digital environment, especially under the decentralized logic of Web 3.0, these conditions intensify: anonymity, the dissociation between physical and virtual identity, and the absence of consolidated norms produce a scenario of weakened social control and a partial collapse of moral regulation[35,36].

[33] Yar, M. (2006). Cybercrime and Society. *SAGE Publications*.
[34] Durkheim, E. (2023). The division of labour in society. In *Social theory re-wired* (pp. 15-34). Routledge.
[35] Costa, D. B. d. (2022). Social structure and anomie: Aspects of contemporary criminality, analyzed from the works of Durkheim, Merton, and Young. *Journal of the Public Defender's Office of the State of Rio Grande do Sul*, *6*, 79–100.
[36] Suxberger, A. H. G., & Pacheco, W. E. P. (2019). A TEORIA DA ANOMIA NOS CRIMES

The rapid technological evolution and the transformation of social interactions in cyberspace have created a context in which traditional norms lose effectiveness, while new rules are still in the process of consolidation. This structural normative gap favors a state of anomie: disorganization. In which individuals begin to act with less reference to shared social standards. In cyberspace, this condition is intensified by the possibility of concealing identity, which reduces the perception of accountability and weakens the links between the individual and society, favoring the occurrence of deviance in de- institutionalized digital spaces[37]

The dissociation between physical and virtual identity constitutes one of the pillars for understanding digital criminality. By acting under fictitious or anonymous identities, individuals experience a loosening of the moral and social controls that regulate behavior in the offline world. This dissociation weakens the internalization of social norms and increases the disposition for deviant behavior, creating an environment conducive to the practice of crimes such as digital fraud, online stalking, and identity theft[38].

The perspective of anomie also aligns with Merton's contributions, highlighting the tension between socially valued goals and the legitimate means available to achieve them. In the digital context, the pursuit of financial and media success, recognition, and status can be intensified by the dynamics of contemporary capitalism, while unequal access to legitimate means increases the propensity to use illicit strategies. This discrepancy favors deviant adaptations, in which cybercrime emerges as a viable alternative to achieve culturally prescribed goals[39].

By constituting its own social reality, mediated by technologies and marked by fragile bonds, cyberspace promotes a dissociation between action and accountability. The consequences of criminal acts rarely fall upon the physical identity of the offender, which intensifies the sensation of impunity. Such dissociation reinforces states of social deregulation and normalizes deviance. In this scenario, Anomie Theory remains crucial for understanding the process of digital normative erosion as fertile ground for online criminality.

The reading of cybercrime through Anomie Theory allows for the understanding of how normative deregulation, anonymity, and the dissociation between physical and virtual identity weaken traditional mechanisms of social control, creating a favorable

structural background for deviance. However, while this approach explains why norms lose effectiveness in the digital environment, it still does not fully answer

CIBERNÉTICOS: THEORY OF ANOMIE APPLIED TO CYBERCRIME. *Delictae Revista de Estudos Interdisciplinares sobre o Delito*, *4*(7), 104-125.

[37] Ibid.

[38] Ibid.

[39] Costa, D. B. d. (2022). Social structure and anomie: Aspects of contemporary criminality, analyzed from the works of Durkheim, Merton, and Young. *Journal of the Public Defender's Office of the State of Rio Grande do Sul*, *6*, 79–100.

how concrete criminal practices are learned, diffused, and normalized among individuals. Anomie, in itself, does not produce criminal techniques, justifications, or routines; it creates the context in which such practices can emerge and stabilize. To advance the understanding of these micro-social processes of transmission and legitimation of crime in cyberspace, it is necessary to incorporate a perspective focused on socialization and the learning of deviance, assumed here by reflecting on the explanatory potentials offered by Social Learning Theory.

3. *Culture, Codes, and Connections: Learning About Crime in Cyberspace*

Social Learning Theory proposes that deviant behavior is learned through social interaction, in contexts where there is repeated exposure to definitions favorable to the violation of the norm [40]. In the digital environment, this dynamic is enhanced by the existence of online communities, forums, and social networks that also operate as spaces for criminal socialization. Such environments function as digital subcultures, where deviant practices not only circulate but are reinforced, normalized, and reinterpreted under the logic of technicality and symbolic transgression.

By connecting to specific digital environments, individuals can learn illicit techniques, share experiences, and legitimize criminal practices through interaction with users who are already involved in illegal activities. These interactions constitute what the authors call differential associations, in which definitions favorable to crime are transmitted and reinforced[41]. Learning occurs not only on a technical level but also on a symbolic level, through the construction of narratives that minimize the severity of the offense or justify its practice[42]. In the context of digital criminology, certain communities or pathways, such as the dark web, operate as deviant learning ecosystems.

Exposure to criminal models in the digital environment plays a central role in this process. The observation of deviant behaviors that are rewarded, whether financially or symbolically, reinforces the imitation and repetition of these conducts. In the context of cybercrimes, practices such as hacking, digital fraud, and malware dissemination can be presented as challenges, games, or demonstrations of technical skill, a process that contributes to the normalization of deviance and the reduction of moral barriers[43].

In this sense, the internalization of definitions favorable to crime allows individuals to perceive their actions as less reprehensible. In the digital

[40] Akers, R. (2017). *Social learning and social structure: A general theory of crime and deviance*. Routledge.
[41] Ibid.
[42] Aguiar, J. C., & Medeiros, M. A. (2024). The social learning theory of criminal behavior. *Brazilian Journal of Criminal Sciences*, *184*.
[43] Ibid.

environment, it is common to build discourses that delegitimize victims or justify offenses based on criticisms of large corporations or institutions, reinforcing neutralization mechanisms. These rationalizations facilitate the continuity of criminal behavior and highlight the relevance of Social Learning Theory for understanding cybercrime.

This learning dynamic gains even more complex contours when we observe the professionalization of criminal organizations in the digital environment, as contemporary cybercrime is structured in networks of high functional specialization. According to Broadhurst et al.[44], these structures operate with an almost industrial division of labor, encompassing roles ranging from programmers and data distributors to money mules and executives who manage the operation. Such a scenario requires that learning theory consider not only the transmission of individual techniques but also immersion in criminal ecosystems where illicit knowledge is shared in a modular and highly coordinated manner.

Thus, the adaptation of Social Learning Theory to the cyberspace context reveals that the internet is not just a means for the offense, but a formative and relational field. Digital criminology, by incorporating this interactional dimension, allows for an understanding of how online deviant subcultures not only reproduce illegal behaviors but also construct their own identities, bonds, and legitimacies. This perspective contributes to a broader reading of the socio-cultural roots of criminality in cyberspace.

By highlighting the role of digital subcultures, networked interactions, and the transmission of definitions favorable to crime, Social Learning Theory contributes decisively to understanding how cybercrime reproduces and becomes professionalized in the digital environment. However, the learning of deviance does not occur in a decision- making vacuum: individuals do not only internalize techniques and legitimizing narratives, but also continuously evaluate the risks and benefits associated with criminal practice. The digital subcultures themselves actively participate in the collective construction of these perceptions, sharing experiences of success, failure, and impunity. Thus, to understand why learned behavior converts into repeated action, it becomes

necessary to incorporate an approach that examines the offender's rational calculation and the effectiveness (or fragility) of social (and criminal) control mechanisms in cyberspace, as proposed by Deterrence Theory.

4. *Low Cost, Invisible Risk: Rationality and Crime in the Digital Environment*

Deterrence Theory starts from the premise that criminal behavior is the result of a rational decision, in which the individual evaluates costs and benefits before

[44] Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, *8*(1), 1-20.

acting[45,46].

In this sense, the effectiveness of criminal control would depend on the perception that punishment is probable, swift, and severe enough to outweigh the advantages of the offense[47,48]. However, when placed in the context of cyberspace, this logic faces structural limitations that weaken its deterrent potential. The technical and organizational characteristics of the digital environment alter the offender's rational calculation, reducing the perception of risk associated with criminal practice.

In the context of cybercrimes, the certainty of punishment is compromised by the nature of the system. The difficulty of attributing authorship, enhanced by the use of anonymization mechanisms, fake digital identities, and decentralized infrastructures, hinders the identification of those responsible for attacks. This fragility in detection directly impacts the offender's decision-making process, who begins to perceive the application of punishment as unlikely or distant. As a consequence, punishment ceases to operate as a relevant cost in the rational calculation, making it insufficient to contain criminal practice[49,50].

Another central aspect for the application of Deterrence Theory to cybercrime concerns the relationship between operational cost and expected return. Unlike traditional crimes, many illicit digital practices demand minimal investment and can be performed remotely, with tools that are widely available and easily accessible. This asymmetry between effort employed and potential gain reinforces the attractiveness of cybercrime, as the "benefit of the crime" tends to vastly outweigh the "evil of the punishment," according to the utilitarian logic of deterrence[51].

The literature points out that the dynamics of cybercrime are governed by a deep asymmetry: while defense mechanisms require massive investments, offensive costs are comparatively negligible, reaching an estimated ratio of 1 to 1,000 in favor of the attacker

[52]This economic advantage, combined with a 'hyperbolic discounting' of risk, where the threat of punishment is perceived as so temporally distant that it becomes irrelevant, creates an environment favorable not only to recidivism but to the continuous expansion of digital criminality.

---

[45] Beccaria, C. (2016). *On crimes and punishments*. Transaction Publishers.
[46] Bentham, J. (1879). *The principles of morals and legislation*. Clarendon Press.
[47] Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and justice*, *42*(1), 199-263.
[48] Paternoster, R. (2010). How much do we really know about criminal deterrence? *Journal of Criminal Law and Criminology*, *100*(3), 765-824.
[49] Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and justice*, *42*(1), 199-263.
[50] Paternoster, R. (2010). How much do we really know about criminal deterrence? *Journal of Criminal Law and Criminology*, *100*(3), 765-824.
[51] Bentham, J. (1879). *The principles of morals and legislation*. Clarendon Press.
[52] Brantly, A. F. (2018). The cyber deterrence problem. In *2018 10th International Conference on Cyber Conflict (CyCon)* (pp. 31-54). NATO CCD COE Publications.

Furthermore, automation and the possibility of carrying out large-scale attacks deepen these limitations of traditional deterrence when we consider a broader and more current context. The use of bots, scripts, and distributed networks allows a single agent, or even loosely structured groups, to cause extensive damage to multiple targets simultaneously. In these cases, individual punishment loses part of its symbolic and preventive effect, since authorship is diluted in complex and often transnational networks[53]. This complexity aggravates what Brantly[54] defines as the 'attribution problem', where the use of proxies and layers of anonymity prevents the precise identification of the aggressor, making the immediate application of the law unfeasible.

The application of the theory allows us to demonstrate that the problem does not lie exclusively in the absence of punishment, but in the inability to make that punishment perceptible, probable, and relevant in the digital context. In this sense, modern literature highlights the need to adapt deterrent mechanisms to the specificities of cyberspace, expanding the focus beyond traditional punishment. Strategies that increase uncertainty regarding the success of attacks tend to directly impact the offender's rational calculation, increasing the perception of risk associated with criminal practice[55].

The construction of a culture of accountability, combined with educational initiatives and the promotion of ethical standards of online conduct, contributes to redefining the symbolic and social costs of cybercrime. By acting on social norms and collective expectations, these strategies complement classic criminal deterrence, reinforcing the idea that crime control in cyberspace requires a combination of sanction, prevention, and social regulation[56]. In this way, Deterrence Theory remains relevant not as an isolated model, but as part of a broader explanatory set capable of illuminating the limits and possibilities of confronting cybercrime.

Despite its historical relevance and wide use in contemporary criminology, Deterrence Theory, as well as approaches derived from the rational choice perspective, has been the target of recent criticism questioning the assumption of a full and stable rationality on the part of offending agents. Steinmetz and Pratt[57] argue that rational criminological

[53] Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats. (2021). Cyber deterrence: A case study on Estonia's policies and practice (Hybrid CoE Paper 8).
[54] Brantly, A. F. (2018). The cyber deterrence problem. In *2018 10th International Conference on Cyber Conflict (CyCon)* (pp. 31-54). NATO CCD COE Publications.
[55] Jones, S. (2021). The evolution of cybersecurity in the face of cybercrime. *Cybersecurity Research Journal*.
[56] Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats. (2021). Cyber deterrence: A case study on Estonia's policies and practice (Hybrid CoE Paper 8).
[57] Steinmetz, K. F., & Pratt, T. C. (2024). Revisiting the tautology problem in rational choice theory: What it is and how to move forward theoretically and empirically. *European Journal of Criminology*, *21*(4), 513-532.

theory faces a problem of logical tautology, insofar as it defines criminal behavior as rational whenever the perceived benefits outweigh the costs, making the explanation circular and limiting its explanatory and predictive capacity regarding criminal decision- making.

According to the authors, this rationality is often constructed in a post-hoc manner, that is, inferred from the observed behavior itself rather than explaining it beforehand. Such a formulation tends to obscure the complexity of actual decision-making processes, especially in contexts marked by social, emotional, structural, or situational pressures, which are central characteristics of the digital environment. Recognizing these limitations demonstrates the need to integrate Deterrence Theory with approaches that consider cognitive, social, and contextual dimensions of criminal action, expanding its analytical capacity in the face of the complexity of contemporary cybercrime.

The analysis of the limitations of Deterrence Theory in the context of cyberspace highlights that the offender's rational calculation is deeply shaped by the structural, situational, and interactional factors discussed in the previous sections. The low perception of risk does not emerge solely from technical failures in attribution, but from a social ecosystem in which expanded opportunities, weakened norms, and collective learning processes converge to reduce the symbolic and material weight of punishment. Thus, the four analyzed theories should not be understood as competing explanations, but as complementary analytical levels of the same phenomenon. In the following section, these perspectives are integrated in a comparative manner, allowing for an understanding of cybercrime as an articulated and multi-level social process.

IV. **Results: A Multi-Level Digital Criminogenic Ecosystem**

The comparative analysis of the four classical criminological theories indicates that, although formulated in contexts prior to the advent of cyberspace, these approaches maintain explanatory capacity for cybercrimes when reinterpreted in light of the transformations promoted by digital technologies. The main result of this study is not the sufficiency of an isolated theory, but the realization that cybercrime arises from the articulation between expanded opportunities, normative weaknesses, social learning processes mediated by digital networks, and a reduced perception of punitive risk.

Routine Activity Theory proved relevant in understanding how the reorganization of social routines in the digital environment structurally expanded criminal opportunities.

The constant presence of individuals in cyberspace, combined with the absence of effective guardians, creates a scenario in which the convergence between offender, target, and absence of control occurs continuously rather than

episodically. The results reinforce the idea of a shift in criminal opportunities from physical to digital space, evidencing that the growth of cybercrime is less associated with new motivations and more with the transformation of situational risk conditions.

A critical aspect emerging from this analysis is the influence of gender on the construction of the "potential target" in the virtual environment. As pointed out by Holt and Bossler[58], victimization in cyberspace is not neutral: women face significantly higher risks of online harassment, often regardless of their preventive behavior or level of technical skill. This occurs because digital interaction can replicate patterns of hostility and aggression that identify the target based on sociodemographic aspects rather than just technical vulnerabilities. Thus, "target attractiveness" in digital criminology must be understood beyond financial value, incorporating cultural patterns of exclusion and hostility that structure cyberspace.

However, the explanatory limits of this approach become evident when considering that the expansion of opportunities does not, by itself, explain why certain individuals engage in cybercrime while others, exposed to the same conditions, do not. It is at this point that Anomie Theory contributes complementarily. The results indicate that cyberspace operates as an environment marked by high normative deregulation, in which the weakening of traditional social control mechanisms and the dissociation between real and virtual identity reduce the strength of shared norms[59]. This condition favors states of anomie that make deviance more likely, especially in contexts of structural inequalities in access to legitimate means to achieve socially valued goals.

Social Learning Theory, in turn, allows for progress in understanding the mechanisms of diffusion and normalization of cybercrime. The results reveal that online communities and digital subcultures act as privileged spaces for deviant socialization, in which illicit practices are learned, legitimized, and reinforced. The most relevant result of this perspective is to show that cybercrime is not sustained only by opportunities or structural tensions, but also by symbolic processes of normalizing deviance, in which crime is presented as a technical skill, a challenge, or a source of social recognition. This aspect helps explain the persistence and expansion of these practices, even in the face of known legal risks.

From the perspective of Deterrence Theory, the results indicate that cyberspace weakens one of the central pillars of criminal control: the certainty of punishment. Anonymity, the difficulty of attributing authorship, and the automation of illicit practices significantly reduce the perception of risk, making sanctions less relevant

[58] Holt, T., & Bossler, A. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

[59] Suxberger, A. H. G., & Pacheco, W. E. P. (2019). A TEORIA DA ANOMIA NOS CRIMES CIBERNÉTICOS: THEORY OF ANOMIE APPLIED TO CYBERCRIME. *Delictae Revista de Estudos Interdisciplinares sobre o Delito*, *4*(7), 104-125.

in the offender's rational calculation. In this context, the problem lies not only in the formal existence of punishment but in the inability to make it visible, credible, and immediate in the digital context.

The integrated reading of this article allows us to further clarify that the theories mobilized do not describe parallel dimensions of cybercrime, but rather distinct analytical levels that are articulated within the same social process. Cybercrime does not result from the simple sum of isolated factors but emerges from the dynamic overlap between weakened normative structures, specific situational configurations, interactional socialization processes, and rational decisions shaped by this context. Each theory illuminates a different plane of this process, which develops in a linked and cumulative manner.

At the structural-normative level → with Anomie: The starting point of the process lies in the weakening of normative references in the digital environment. Cyberspace intensifies the dissociation between action and accountability, producing a context in which social norms and expectations of sanction lose regulatory density. This normative weakening operates as an abstract background and reconfigures how individuals perceive the limits, obligations, and consequences of their conduct, creating favorable conditions for social tolerance of deviance.

At the situational/opportunity level → with Routine Activities: This structural deregulation projects direct effects here. The reorganization of daily practices in the digital environment occurs in a space where fragile norms and diffuse controls allow the convergence between potential offenders, targets, and the absence of guardians to become continuous. Anomie, by reducing normative brakes, enhances the exploitation of these opportunities, making exposure to risk the norm rather than the exception in digital interactions.

At the interactional-cultural level → with Social Learning: The expansion of opportunities, in turn, creates conditions for advancement here. In an environment marked by weak regulation and high availability of targets, illicit practices occur and begin to be

shared, taught, and legitimized in digital networks. Cyberspace favors the formation of interaction sites where deviance is reinterpreted, normalized, and incorporated as a technical competence or legitimate strategy. This learning process ranges from the transmission of techniques to the construction of meanings that neutralize moral disapproval and reinforce the continuity of criminal conduct.

At the decision/rationality level → with Deterrence Theory: This collective learning directly affects this level by shaping the calculation of costs and benefits associated with crime. The offender's rational calculation is socially formulated through narratives, shared experiences, and collectively constructed perceptions regarding risk, punishment, and reward. As the digital environment reinforces the

idea of low accountability and high offense efficiency, punishment loses its centrality as an inhibiting factor, weakening the classic deterrent effect and feeding back into the cycle of crime.

This chain of events shows that cybercrime develops as a circular process:

Anomie favors the reorganization of digital routines → these routines expand opportunities → opportunities sustain deviant learning processes → and learning reconfigures the rational calculation, reducing the effectiveness of deterrence and deepening the initial normative fragility. It is, therefore, a dynamic of continuous feedback in which each level reinforces the others.

Based on this processual reading, it becomes possible to understand cyberspace as a digital criminogenic ecosystem. This ecosystem operates simultaneously as an environment that produces opportunities from digital routines, weakens norms through structural deregulation, socializes deviance in its own interactional circuits, and reduces the perceived costs of crime by compromising the logic of deterrence. Cybercrime, in this sense, is not just a point-specific deviance nor exclusively technical; it becomes an emergent product of the interaction between multiple levels of social organization that intertwine in the daily functioning of the digital environment.

Such findings suggest that enforcement strategies based exclusively on technical or punitive solutions tend to be insufficient due to the nature of the offenses. Understanding cybercrime requires approaches that combine opportunity reduction, strengthening the perception of risk, promoting social norms in the digital environment, and addressing structural inequalities. In this sense, classical criminology, far from being obsolete,

reveals itself as fundamental for constructing critical and integrated analyses of crime in the contemporary digital context.

V. **Final Considerations: Contributions of Classical Criminology to the Digital Age**

This article aimed to analyze the current relevance of classical criminological theories in the face of the challenges imposed by cybercrimes in the context of digital society. Based on a comparative theoretical approach, the results indicate that such theories remain relevant, provided they are reinterpreted in light of the specificities of cyberspace, such as anonymity, decentralization, and the reconfiguration of social interactions promoted by Web 3.0. Cybercrime does not emerge as a radically new phenomenon, but as a reconfiguration of traditional crime dynamics in a space marked by new forms of social interaction, anonymity, and the expansion of criminal opportunities.

The findings of this study point to the need for theoretical advances that move beyond the isolated application of classical theories, promoting multi-level and

intersectional explanatory models. The overlap of structural (anomie), situational (routine), interactional (learning), and rational (deterrence) elements suggests that cybercrime can be better understood as a hybrid phenomenon, which requires integrated theoretical frameworks. Future research could focus on constructing more robust and composite analytical models capable of capturing the complexity of digital deviant practices based on interactions between normative contexts, socialization networks, and anonymity technologies. Investing in theoretical approaches of this nature may further contribute to the development of more refined typologies of digital offenses, overcoming the limitations of classical models when applied in isolation.

In this sense, Table 2 synthesizes, in a comparative manner, the main scopes, limits, and possibilities for adapting the analyzed theories to the context of cyberspace.

Table 2 (a): Comparative Analysis of the Conceptual and Structural Adequacy of Crime Theories to the Virtual Environment

Theory	Explanatory Scope at the Structural Level	Conceptual Adequacy to the Digital Environment	Main Weaknesses in Cyberspace	Margin for Theoretical Adaptation
Routine Activity Theory	High capacity to interpret changes in criminal opportunities resulting from the digitalization of social routines, considering continuous exposure, virtualization of interactions, and weakening of surveillance.	High degree of compatibility, provided that classic elements (target, offender, and guardian) are reinterpreted in light of technical, institutional, and algorithmic mediations.	Tendency to excessively prioritize situational factors, with limited incorporation of symbolic, cultural, and motivational dimensions specific to cybercrime.	Ample possibility for updating, especially through the redefinition of surveillance mechanisms (human, technical, and normative) and digital routines.
Social Learning Theory	Strong explanatory potential for understanding the diffusion, normalization, and	High conceptual coherence, since processes of differential association,	Less attention to the effects of technological mediation, such as algorithms,	High adaptation potential by incorporating anonymity, digital reputation,
	maintenance of illicit conduct in digital environments mediated by continuous interaction.	reinforcement, and definitions favorable to deviant conduct are intensified in online communities.	platforms, and gamification systems, in the criminal learning process.	symbolic reinforcements, and the centrality of platforms as spaces for socialization.
Anomie Theory	Intermediate to high explanatory capacity when addressing processes of normative weakening, fragmentation of rules, and tensions between means and ends in the digital context.	Moderate compatibility, as classic concepts of norm and control remain relevant, although they demand adjustments in the face of the fluidity and instability of the online environment.	Insufficient attention to informal digital norms, algorithmic logics of regulation, and the internal dynamics of virtual communities.	Consistent possibility of reformulation by shifting the focus from normative absence to processes of reconfiguration and norm disputes in the digital space.

Table 2 (b): Comparative Analysis of the Conceptual and Structural Adequacy of Crime Theories to the Virtual Environment

Theory	Explanatory Scope at the Structural Level	Conceptual Adequacy to the Digital Environment	Main Weaknesses in Cyberspace	Margin for Theoretical Adaptation
Deterrence Theory	Low to moderate explanatory capacity, especially in contexts marked by anonymity, low risk perception, and the transnationalization of criminal practices.	Limited conceptual compatibility, since classic assumptions of punishment, cost, and rationality lose effectiveness when applied in a traditional manner.	Reduced practical effectiveness of criminal punishment, combined with structural difficulties in investigation, tracking, and international cooperation.	Moderate adaptive potential, especially if articulated with technical deterrence strategies, digital barriers, and non-penal normative mechanisms.

Furthermore, from a theoretical-analytical standpoint, the results reinforce the importance of moving beyond unidimensional explanations and adopting integrated approaches in contemporary criminology, celebrating multidisciplinarity. The articulation between structural and situational theories allows for an understanding of how inequalities, normative deregulation, and the daily dynamics of cyberspace combine to facilitate criminal practices. This theoretical integration contributes to the advancement of the academic debate by highlighting that crime in the digital environment is the product of multiple levels of analysis, and not merely of individual or technological failures. Digital criminology, in this scenario, emerges as a promising field, capable of articulating theoretical tradition and analytical innovation to interpret the challenges of crime in the information society.

From a methodological standpoint, this article reinforces the importance of systematic mapping and interpretive scopes as a foundation for future empirical investigations in digital criminology. There is a fertile field for research that combines quantitative surveys of digital criminality patterns with qualitative analyses of deviant networks, including online ethnographies, content analysis in forums, data scraping in specific areas of the deep web, where forums with less public visibility and restricted access operate, and case studies involving emerging technologies. Such studies can contribute to validating or revising the findings of this article, in addition to exploring discursive and symbolic constructions of deviance in digital environments. In this sense, digital criminology benefits from mixed methodological designs that integrate computational social science techniques with the theoretical frameworks discussed in this article.

Finally, the implications of the study point to the need for coping strategies that go beyond exclusively technical or punitive responses. More effective prevention policies must combine the reduction of opportunities, the strengthening of risk perception, the dissemination of social norms in the digital environment, and the

tackling of structural inequalities. In this sense, classical criminology reaffirms its relevance by offering analytical tools capable of guiding more comprehensive and consistent responses to the challenges imposed by crime in the contemporary digital context.

By proposing a critical rereading of classical criminological theories through the lens of the digital age, this article contributes to strengthening the field of digital criminology in the international debate. By recognizing the continuity of theoretical principles amidst the transformation of the means and contexts of crime, the research offers analytical and

conceptual support for deepening the academic debate, formulating public policies, and developing future empirical and multidisciplinary investigations.

VI. **Acknowledgment**

This research was supported by the Foundation for Research Support of the State of Minas Gerais (FAPEMIG), through the Universal Demand call – Category B (Group Projects), Process No. APQ-02174-25. This article constitutes one of the products planned within the scope of the aforementioned project.

References

ABES – Brazilian Association of Software Companies. (2024). 2023 ends with 161 billion cyberattacks, in another record, according to a report by Trend Micro.

Aguiar, J. C., & Medeiros, M. A. (2024). The social learning theory of criminal behavior. *Brazilian Journal of Criminal Sciences*, *184*.

Akers, R. (2017). *Social learning and social structure: A general theory of crime and deviance*. Routledge.

Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*, *8*(1), 19-32.

Beccaria, C. (2016). *On crimes and punishments*. Transaction Publishers.

Bentham, J. (1879). *The principles of morals and legislation*. Clarendon Press.

Brantly, A. F. (2018). The cyber deterrence problem. In *2018 10th International Conference on Cyber Conflict (CyCon)* (pp. 31-54). NATO CCD COE Publications.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, *8*(1), 1-20.

Costa, D. B. d. (2022). Social structure and anomie: Aspects of contemporary criminality, analyzed from the works of Durkheim, Merton, and Young. *Journal of the Public Defender's Office of the State of Rio Grande do Sul*, *6*, 79–100.

Durkheim, E. (2023). The division of labour in society. In *Social theory re-wired* (pp. 15-34). Routledge.

Figueiredo, B., & Miró Llinares, F. (2024). Digital life and crime trends in the global south: on the impact of increased Internet use on opportunities for crime. *Revista Espanola de Investigacion Criminologica*, *22*(2).

Greenhalgh, T., Thorne, S., & Malterud, K. (2018). Time to challenge the spurious hierarchy of systematic over narrative reviews? *European Journal of Clinical Investigation*, *48*(6), e12931.

Holt, T., & Bossler, A. (2015). *Cybercrime in progress: Theory and prevention of technology-*

enabled offenses. Routledge.
Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats. (2021). Cyber deterrence: A case study on Estonia's policies and practice (Hybrid CoE Paper 8).
Jones, S. (2021). The evolution of cybersecurity in the face of cybercrime. *Cybersecurity Research Journal*.
Kahn, T. (2023). Migration from violent street crimes to digital crimes. *Fonte Segura*.
Kerr, O. S. (2003). Cybercrime's scope: Interpreting'access' and'authorization'in computer misuse statutes. *New York University Law Review*, *78*(5), 1596.
Lijphart, A. (1971). Comparative Politics and the Comparative Method. *American political science review*, *65*(3), 682-693.
Lourenço, A. C. G., Dos Santos, C. E. P., de Almeida, G. H., & de Castro, B. V. (2023). O aumento dos crimes cibernéticos durante a pandemia da Covid-19 e as dificuldades para combatê-los. *LIBERTAS DIREITO*, *4*(1).
McGuire, M. (2012). *Technology, Crime and Justice: The Question Concerning Technomia*. Routledge.
Merton, R. K. (1970). *Social structure and anomie.* In Sociology: Theory and structure (M. Maillet, Trans.; pp. 197–228). Mestre Jou.
Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and justice*, *42*(1), 199-263.
Paternoster, R. (2010). How much do we really know about criminal deterrence? *Journal of Criminal Law and Criminology*, *100*(3), 765-824.
Steinmetz, K. F., & Pratt, T. C. (2024). Revisiting the tautology problem in rational choice theory: What it is and how to move forward theoretically and empirically. *European Journal of Criminology*, *21*(4), 513-532.
Suxberger, A. H. G., & Pacheco, W. E. P. (2019). A TEORIA DA ANOMIA NOS CRIMES CIBERNÉTICOS: THEORY OF ANOMIE APPLIED TO CYBERCRIME. *Delictae Revista de Estudos Interdisciplinares sobre o Delito*, *4*(7), 104-125.
Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity.
Wall, D. (2021). The Transnational Cybercrime Extortion Landscape and The Pandemic: Ransomware and changes in offender tactics, attack scalability and the organisation of offending. *European Law Enforcement Research Bulletin*.
Yar, M. (2006). Cybercrime and Society. *SAGE Publications*.