Berajah Journal
Published by: CV Lafadz Jaya | ISSN: 2797-1805 | E-ISSN: 2797-1882

Volume 5 No.11 (2025)
Page: 445 – 458
https://ojs.berajah.com/index.php/go/

THE DEVELOPMENT OF CRIMINAL LAW IN ADDRESSING DIGITAL FRAUD AND CYBER OFFENSES

Iip Nurul Topani[1]*, Alan Yati[2]
UIN Raden Intan Lampung[1,2]
***Email Correspondence:** iipnurultofani@radenintan.ac.id

Abstract

The advancement of digital technology has facilitated economic activities, communication, and public services, yet it has simultaneously created new avenues for digital fraud and various forms of cybercrime. The cross-border and dynamic nature of technology-based crimes which exploit the anonymity and complexity of digital systems poses challenges for the evolution of criminal law. This study aims to analyze the development of criminal law in response to digital fraud and cyber offenses, specifically regarding the nature of these crimes, criminal liability, electronic evidence, and the need to align legal policies with technological advancements. The research employs a normative-juridical approach, analyzing relevant legislation, legal doctrines, and scholarly literature. The findings indicate that the evolution of digital crime necessitates a shift in criminal law from conventional approaches toward a legal framework that is more adaptive to the characteristics of technology. Strengthening regulations, clarifying the construction of criminal liability, optimizing the use of electronic evidence, enhancing the capacity of law enforcement officials, and fostering inter-agency and cross-border cooperation are crucial aspects of combating digital fraud and cyber offenses. Consequently, the development of criminal law should not focus solely on sanctioning perpetrators but also on establishing a law enforcement system capable of ensuring legal protection, certainty, and effectiveness in addressing the transformation of crime within the digital realm.

Keywords: Criminal Law, Digital Fraud, Cyber Offenses, Cybercrime, Electronic Evidence, Law Enforcement

INTRODUCTION

Advancements in information and communication technology have brought about fundamental changes in various aspects of societal life. Digitalization has not only enhanced efficiency in economic activities, communication, commerce, and public services but has also created new avenues for the emergence of various forms of crime. As public activity becomes increasingly reliant on the internet, digital applications, electronic banking services, online commerce, and social media, a significant portion of transactions and interactions now occur in environments that cannot be fully regulated by conventional legal mechanisms (Olukunle Oladipupo Amoo et al., 2024a). This situation creates opportunities for criminals to exploit technology as a means to commit offenses using increasingly complex and difficult-to-detect methods.

One form of crime that has seen significant growth is digital fraud—fraud facilitated by digital technology (Broadhurst, 2006). Such crimes can be perpetrated through various *modus operandi*, ranging from information manipulation, identity theft, phishing, and electronic transaction fraud to account misuse and social engineering that exploits the victim's trust. Unlike conventional fraud, digital fraud can be carried out using false identities, distributed communication networks, and technological systems that allow perpetrators to conceal their activity trails. The rapid spread of digital information also enables a single criminal scheme to reach numerous victims within a relatively short period. These shifting characteristics demonstrate that technological progress not only influences how people conduct their daily activities but also alters the patterns, methods, and impacts of criminal acts.

DOI: https://doi.org/10.47353/bj.v5i11.753

Beyond digital fraud, cyber offenses encompass a wide range of unlawful acts involving computer systems, internet networks, electronic data, and digital infrastructure. Cybercrimes can range from unauthorized system access, data interception, and the manipulation or destruction of electronic information to data theft, the dissemination of illegal content, and attacks on systems critical to society. Because cyber offenses can be committed without the perpetrator's physical presence at the scene, the processes of identification, investigation, and prosecution face challenges distinct from those associated with conventional crimes (Sinrod & Reilly, 1999). In some instances, the perpetrator and the victim may be located in different jurisdictions, while data related to the criminal offense is stored on systems or servers situated in another country.

This situation poses a challenge for criminal law in mounting an effective response to digital-based crimes. Fundamentally, criminal law serves to protect society by defining prohibited acts, establishing perpetrator liability, and imposing sanctions for legal violations. However, technological advancements outpace the processes of enacting and adapting regulations. Consequently, a potential mismatch arises between the characteristics of new crimes and existing legal frameworks. Ambiguities regarding the elements of the offense, the scope of perpetrator liability, jurisdiction, and the use of specific technologies in committing crimes can complicate law enforcement efforts.

Issues also arise regarding the evidentiary process. Digital crimes typically leave behind evidence in electronic form such as digital messages, transaction records, internet addresses, metadata, device data, system activity logs, and information from digital platforms. Such evidence differs in nature from conventional evidence because it can be easily moved, altered, deleted, or disseminated across various systems (Silalahi, 2023a). Therefore, the effectiveness of law enforcement against digital fraud and cyber offenses depends heavily on the ability of authorities to lawfully obtain, secure, examine, and present electronic evidence. Strengthening digital evidentiary mechanisms is crucial to ensuring that law enforcement processes uphold the principle of legal certainty while keeping pace with technological developments.

In Indonesia, legal developments regarding digital crime demonstrate an effort to establish a legal basis for various acts committed via electronic systems. Regulations concerning electronic information and transactions, alongside updates to criminal law, indicate that the national legal system continues to adapt to societal changes (Katyal, 2001). Nevertheless, existing regulations have not fully resolved all issues arising in practice. Technological advancements—such as artificial intelligence, digital financial services, e-commerce platforms, cloud computing, and various forms of digital communication—have spawned new criminal modalities that require responsive legal interpretations and policies.

These changes demonstrate that developing criminal law requires more than merely adding new types of offenses or increasing penalties. Legal approaches must also consider the characteristics of the technology, fair liability mechanisms, victim protection, and the capacity of law enforcement agencies to handle digital evidence and criminal modalities. Criminal laws that are overly rigid risk becoming obsolete when confronted with constantly evolving forms of crime. Conversely, laws that are overly broad and lack clear boundaries can raise issues regarding legal certainty and the protection of individual rights. Therefore, a balance must be struck between the effective eradication of digital crime and respect for fundamental criminal law principles.

Addressing digital fraud and cyber offenses also requires stronger cooperation, given that cybercrime transcends geographical boundaries. Law enforcement efforts may involve digital service providers,

DOI: https://doi.org/10.47353/bj.v5i11.753

financial institutions, law enforcement agencies, government bodies, and authorities from other countries. Information exchange and inter-agency coordination are crucial for rapidly identifying perpetrators, securing electronic evidence, tracing fund flows, and preventing the recurrence of criminal acts. Consequently, the development of criminal law must be situated within a broader framework: one that not only strengthens criminal norms but also establishes a law enforcement system capable of responding to the unique characteristics of the digital realm (Tawil & Tarawneh, 2026a). Given these circumstances, it is relevant to examine the evolution of criminal law in addressing digital fraud and cyber offenses. This study aims to understand how criminal law evolves in response to changing forms of digital crime, issues regarding criminal liability and electronic evidence, and the strategies required to strengthen law enforcement. The study is expected to make an academic contribution to understanding the trajectory of criminal law in the digital era, while also offering perspectives for strengthening legal policies that are adaptive and effective, and that ensure legal certainty and justice for the public.

LITERATURE REVIEW

Concepts of Digital Fraud and Cyber Offenses

Digital fraud and cyber offenses are two forms of crime that have evolved alongside the increasing use of information technology in society. Digital fraud generally refers to fraudulent acts that utilize digital devices, networks, applications, or platforms to obtain illicit gains. Modus operandi include phishing, identity theft, electronic transaction manipulation, online commerce fraud, account misuse, and social engineering—whereby victims are induced to voluntarily provide information or access. The defining characteristic of digital fraud lies in the use of technology as a means to manipulate victims, acquire data, or misappropriate assets (Graham & Smith, 2024).

Meanwhile, cyber offenses encompass a broader scope, covering various unlawful acts committed using computers, networks, electronic systems, or digital data—whether as the means or the target of the crime. Forms of such offenses include unauthorized system access, data theft or manipulation, network disruption, the dissemination of malicious software, and other illegal activities leveraging digital infrastructure. Thus, digital fraud can be understood as a specific type of cyber offense, particularly when technology is employed to commit fraud or secure unlawful benefits.

The distinct characteristics distinguishing digital crimes from conventional crimes have significant implications for criminal justice systems. In conventional crimes, perpetrators and victims can generally be identified based on location and relatively clear event dynamics. Conversely, digital crimes can be perpetrated from locations far removed from the victim, using identities that do not correspond to the actual person, and utilizing multiple platforms and devices simultaneously. These conditions complicate the process of tracking perpetrators and establishing jurisdiction. Furthermore, evidence of the crime often exists in the form of electronic data that can be rapidly altered, deleted, or relocated (Tawil & Tarawneh, 2026b).

Technological advancements also cause the patterns of digital fraud and cyber offenses to constantly evolve. Perpetrators not only exploit vulnerabilities in technological systems but also capitalize on human factors through psychological manipulation and the abuse of trust. The use of artificial intelligence, automation, and increasingly sophisticated communication technologies has the potential to render criminal methods more convincing and harder to detect. Consequently, understanding the concepts of digital fraud and cyber offenses requires considering both technological and legal dimensions—specifically regarding prohibited acts, elements of culpability, victim losses, and perpetrator liability (Saghir & Kafteranis, 2022).

DOI: https://doi.org/10.47353/bj.v5i11.753

From a criminal law perspective, these characteristics highlight the need for an approach that adapts to the evolution of digital crime. Regulations must go beyond merely establishing prohibitions and sanctions; they must also provide certainty regarding the boundaries of criminally punishable conduct, mechanisms for utilizing electronic evidence, and the scope of authority for law enforcement agencies in conducting investigations and enforcement actions. A clear conceptual understanding of digital fraud and cyber offenses serves as a vital foundation for formulating criminal policies that protect the public while upholding the principles of legality, legal certainty, proportionality, and the protection of individual rights.

The Evolution of Criminal Law in the Digital Era

The development of digital technology has encouraged changes in crime patterns as well as influenced the direction of criminal law development. Activities that were previously carried out in person can now be carried out via electronic devices and internet networks, resulting in forms of criminal acts that have a different character from conventional crimes. Crimes such as digital fraud, data theft, illegal access to systems, manipulation of electronic information, and various forms of cyberattacks show that criminal law needs to have the ability to respond to technological change on an ongoing basis (Maagbeh, 2026).

The development of criminal law in the digital era is not only related to the creation of new norms, but also to the adjustment of existing legal concepts. The principle of legality requires that an act can be categorized as a criminal act based on applicable legal provisions. In a digital context, this principle becomes important because technological developments can produce new modes that have not been specifically formulated in regulations (Silalahi, 2023b). Therefore, legislators need to ensure that digital crime regulations have clear formulations, do not have multiple interpretations, and are able to provide legal certainty for the public and law enforcement officials.

In Indonesia, the development of digital criminal law can be seen from the increasingly strong regulations regarding acts carried out through electronic systems. Regulations regarding information and electronic transactions have become an important basis for dealing with various forms of technology-based crime. These developments then need to be harmonized with national criminal law reforms so that regulations regarding digital crime have a harmonious relationship with the criminal law system as a whole. Harmonization is important to avoid overlapping norms, unclear authority, and differences in interpretation in the law enforcement process (Asli, 2023).

Another challenge relates to the nature of digital crime which can transcend national borders. The perpetrator can be in one country, the victim in another country, while the data needed for proof is stored on a server in a different jurisdiction. This condition means that the application of criminal law cannot only rely on a national approach. International cooperation, information exchange, and mutual legal assistance mechanisms are becoming increasingly important to ensure that digital criminals can be processed effectively in accordance with applicable legal provisions ("Criminal Behavior in the Digital Environment," 2025).

Apart from regulatory aspects, the development of criminal law is also closely related to electronic evidence. Digital evidence can be in the form of electronic communications, transaction data, system activity records, device information, or other data relevant to criminal acts. The nature of evidence that is easily changed or deleted requires collection and security procedures that can maintain its authenticity and integrity. Therefore, the ability of law enforcement officers in the field of digital forensics is an important part of the development of the criminal justice system in the technological era.

DOI: https://doi.org/10.47353/bj.v5i11.753

Criminal Liability in Cybercrime

Criminal liability in cybercrime is a critical issue because the nature of digital offenses differs from that of conventional crimes. Cybercrimes can be committed via digital devices and networks with masked identities, where the perpetrator is geographically distant from the victim, and technology enables rapid, repetitive actions. These circumstances necessitate precisely determining who bears criminal liability, the nature of the culpability involved, and the causal link between the perpetrator's actions and the resulting harm (Baker & Robinson, 2020).

In criminal law, liability is fundamentally based not only on the commission of a prohibited act but also on the perpetrator's culpability. Elements such as intent or other forms of fault are crucial in determining criminal liability. In the context of cybercrime, proving these elements can be complex, as digital acts are often carried out using fake accounts, third-party devices, or manipulated systems. Consequently, law enforcement agencies must link the perpetrator's identity to the digital activity using legally admissible evidence.

Issues of liability also arise when crimes are committed by exploiting third parties or specific technologies. Perpetrators may use bank accounts, user accounts, devices, or digital infrastructure belonging to others to mask their activities. In such situations, the presence of a specific identity or device in digital evidence does not automatically prove that the owner is the perpetrator. Law enforcement must distinguish between those who knowingly commit or assist in a crime and those who are merely victims of identity or device misuse. Such precision is essential to uphold justice and prevent the wrongful criminalization of innocent parties (Sari, 2025).

Technological advancements also expand the potential for various parties to be involved in a digital offense. Beyond the primary perpetrator, there may be parties who provide the means, profit from the proceeds of the crime, or intentionally facilitate the commission of the offense. Therefore, the framework for criminal liability must consider the nature of each party's involvement based on their specific roles and degrees of culpability. This approach is crucial to ensure that sanctions are not excessive and remain proportionate to the offense committed (L, 2023). The cross-border nature of cybercrime further complicates the determination of criminal liability. Perpetrators can conduct illicit activities from jurisdictions different from where the victims suffer harm. Disparities in legal systems, evidentiary rules, and the authority of law enforcement agencies across nations can impede identification and prosecution processes (Nadaradjan, 2025). Consequently, international cooperation and information-sharing mechanisms are vital to ensuring that perpetrators cannot exploit territorial boundaries to evade legal accountability. Thus, addressing criminal liability in cybercrime requires an approach that integrates fundamental criminal law principles with the unique characteristics of digital technology. Identifying perpetrators must rely on valid evidence, a clear causal link between the act and its consequences, and proof of culpability. Strengthening digital investigation capabilities, enhancing the competence of law enforcement personnel, and harmonizing regulations are essential steps to ensure effective cybercrime enforcement while upholding legal certainty, fairness, and the protection of all parties' rights.

DOI: https://doi.org/10.47353/bj.v5i11.753

METHOD

This study employs a normative-juridical method utilizing both statutory and conceptual approaches. The statutory approach is used to analyze legal provisions concerning digital fraud, cyber offenses, criminal liability, and electronic evidence, while the conceptual approach is used to understand the evolution of criminal law concepts in response to the characteristics of digital technology-based crimes. The research data consists of primary, secondary, and tertiary legal materials obtained through a literature review. Primary legal materials comprise relevant legislation, whereas secondary materials include books, scholarly journal articles, research findings, and academic documents addressing criminal law and cybercrime.

The analysis of legal materials is conducted qualitatively by identifying, classifying, and interpreting provisions and legal concepts relevant to the research focus. The collected materials are then analyzed using a descriptive-analytical method to outline the evolution of criminal law in addressing digital fraud and cyber offenses, including issues of criminal liability, electronic evidence, jurisdiction, and law enforcement challenges. Finally, the analysis results are synthesized to gain an understanding of the need to strengthen and adapt criminal law so that it can effectively respond to the evolution of digital crime while upholding the principles of legality, legal certainty, justice, and the protection of the public's legal rights.

RESULTS AND DISCUSSION

Digital Transformation of Fraud and Cyber Offenses

The digital technology transformation has shifted the nature of crime from traditional patterns to acts that leverage electronic devices, networks, and systems. This shift is evident in the rise of digital fraud and cyber offenses, which have evolved alongside the adoption of the internet, digital financial services, e-commerce, social media, and various communication platforms. While technology facilitates daily activities, it simultaneously creates opportunities for perpetrators to exploit system vulnerabilities and user behaviors. Consequently, digital crime has become an evolving legal issue that demands a more adaptive response (Rawat et al., 2021).

Digital fraud has evolved from simple scams into complex activities that simultaneously involve technology, data manipulation, and social engineering. Perpetrators do not always attack systems directly; instead, they may exploit human vulnerabilities by crafting convincing communications. Phishing, identity theft, online transaction fraud, account misuse, and information manipulation are examples of how technology is used for illicit gain. These patterns demonstrate that the evolution of digital fraud depends not only on technological sophistication but also on the perpetrator's ability to exploit victims' habits, trust, and limited digital literacy (Rossy & Ribaux, 2020).

This transformation is further complicated by the digital environment, which allows perpetrators to utilize multiple platforms within a single sequence of actions. For instance, a victim's information might be obtained via social media, communication conducted through messaging apps, and the proceeds of the crime laundered through digital financial services. Each stage can involve different devices or accounts, making tracing and investigation significantly more difficult. This situation highlights the flexible nature of digital fraud and its ability to adapt to technological changes; when a platform's security is strengthened, perpetrators tend to seek new methods to exploit technological loopholes or user vulnerabilities (Dupuis et al., 2021).

Meanwhile, cyber offenses have expanded in scope, as technology serves not only as a tool for committing crimes but also as a target of attacks. Cybercrime encompasses unauthorized system access, data

DOI: https://doi.org/10.47353/bj.v5i11.753

theft, the manipulation of electronic information, network disruption, the misuse of digital identities, the distribution of malicious software, and attacks on digital infrastructure. This evolution reflects a shift from crimes targeting physical objects to those targeting data, information, accounts, systems, and networks. The economic and strategic value inherent in data makes it a key target in the landscape of cybercrime (Dobrovolska et al., 2024).

A defining characteristic of the transformation of cyber offenses is the ability of perpetrators to execute actions rapidly and on a vast scale. A single attack can impact numerous users or systems within a short timeframe. Furthermore, perpetrators can mask their identities using various techniques and leverage digital infrastructure distributed across multiple regions. These factors make it increasingly difficult to distinguish between local and transnational crimes. In practice, perpetrators, victims, devices, service providers, and data storage locations may all be situated in different jurisdictions. This cross-border nature is a primary reason why addressing cybercrime requires enhanced coordination among authorities (Financial Crime and Fraud in the Age of Cybersecurity, n.d.).

The advancement of artificial intelligence and automation has expanded the potential for the digital transformation of fraud and cyber offenses. These technologies can be leveraged to generate more convincing communications, automate large-scale activities, and enhance the capabilities of perpetrators in carrying out digital manipulation. These developments necessitate the continuous updating of crime detection methods, as attack patterns can shift more rapidly than in the past. From a criminal law perspective, this situation poses challenges in defining the specific acts that constitute criminal offenses and in establishing how perpetrator liability can be proven.

The transformation of digital crime also impacts the evidentiary process. Evidence related to criminal offenses may consist of electronic messages, transaction records, device data, internet addresses, metadata, account activity, or information derived from digital systems. Unlike conventional evidence, electronic data is easily copied, transferred, altered, or deleted (Nourelhouda, 2024). Consequently, the processes of collecting and securing evidence must be executed with great care to ensure the data's authenticity and integrity remain intact. The ability of law enforcement officials to understand technology and conduct digital examinations is a crucial factor in the success of law enforcement efforts.

In the context of criminal law, the digital transformation of fraud and cyber offenses demonstrates that legal approaches cannot rely solely on conventional concepts of crime. The law must be capable of identifying the characteristics of acts committed via electronic systems while clearly defining the actions for which liability can be imposed. The principle of legality remains the fundamental basis ensuring that any imposition of criminal penalties rests on a clear legal foundation. However, the application of this principle must be accompanied by regulatory updates that are responsive to technological advancements, thereby preventing a gap between evolving criminal methods and the law's capacity to provide protection.

Beyond normative aspects, the transformation of digital crime highlights the importance of preventive approaches. Law enforcement should not merely react after losses have occurred; rather, it must be complemented by efforts to enhance digital literacy, strengthen security systems and data protection, and raise public awareness regarding fraudulent schemes. In cases of digital fraud, users often constitute a critical link in the security chain, as a victim's decision to disclose information, access a link, or execute a transaction can be exploited by perpetrators (Undale & Shinde, 2024). Consequently, mitigation strategies must involve the government, law enforcement agencies, digital service providers, financial institutions, and the public.

DOI: https://doi.org/10.47353/bj.v5i11.753

Based on this analysis, the evolution of digital fraud and cyber offenses demonstrates that technological advancements have altered the methods of committing crimes, the targets involved, and the mechanisms for enforcement. Crimes are increasingly dynamic, rapid, anonymous, and transnational in nature, while the resulting evidence relies heavily on electronic data. These conditions necessitate the evolution of criminal law moving beyond a mere focus on sanctions to a framework capable of establishing clear liability, strengthening evidentiary mechanisms, and protecting the public from the various risks associated with digital crime.

Thus, the transformation of digital fraud and cyber offenses serves as a crucial foundation for reforming criminal law policy. The legal system must evolve adaptively through the harmonization of regulations, capacity building for law enforcement, the use of technology in investigations, enhanced inter-agency and international cooperation, and strengthened victim protection. A balanced response is required to ensure criminal law keeps pace with technological advancements without compromising the principles of legality, legal certainty, proportionality, and the protection of individual rights. Such an approach will bolster the criminal justice system's capacity to address the increasingly complex nature of digital crime.

Adaptation and Criminal Law Accountability in the Digital Era

Adapting criminal law essentially concerns the capacity of legal norms to address evolving forms of crime. Digital fraud and cyber offenses possess distinct characteristics, as the acts can be committed rapidly and anonymously, involve the use of false identities, and span multiple systems simultaneously. These conditions create challenges when an act is not yet specifically regulated or when existing provisions are limited in their ability to account for the nature of specific technologies (Olukunle Oladipupo Amoo et al., 2024b). Consequently, legal reform must be undertaken cautiously, adhering to the principle of legality to ensure that the expansion of criminalization does not create uncertainty for the public. In the context of Indonesian criminal law, adaptation to digital crime is evident in the evolution of regulations governing activities and actions within electronic systems. Provisions regarding electronic information and transactions provide a legal basis for addressing various acts committed via digital media. However, rapid technological advancements necessitate continuous evaluation of regulations to maintain their relevance. Harmonizing general criminal provisions with specific digital-sector regulations is crucial to avoid overlapping rules and to ensure clarity regarding the elements of the offense and applicable sanctions (Faisal & Ulya, 2026).

Adapting criminal law also involves determining criminal liability. Under criminal law, a person cannot be punished solely because a specific consequence has occurred; there must be a basis for linking the act to the perpetrator's culpability. This principle remains relevant when addressing digital crime. Even though activities are conducted via electronic devices or systems, law enforcement must still prove the involvement and culpability of the alleged perpetrator. This is vital because an account, device, internet address, or bank account used in a crime does not automatically indicate that the owner is the perpetrator (Hartomi et al., 2026).

These issues become increasingly complex when perpetrators use the identities or devices of others. In the practice of digital crime, perpetrators may hijack accounts, use victims' identity data, or utilize third-party devices to commit criminal acts. Therefore, the law enforcement process must distinguish between perpetrators who knowingly commit a criminal act and parties who fall victim to the misuse of technology. Determinations of liability must be grounded in a clear relationship between the perpetrator, the act, the tools employed, and the objective of the action (Sihombing & Nuraeni, 2023).

DOI: https://doi.org/10.47353/bj.v5i11.753

Criminal liability in the digital realm also requires consideration of the nature of each party's involvement. Cybercrimes are not always committed by a single individual acting alone. In certain instances, other parties may play roles such as providing the means, assisting in the commission of the act, managing the proceeds of the crime, or intentionally facilitating illegal activities. These varying roles must be analyzed in accordance with applicable criminal law provisions to ensure that sentencing is proportionate. This approach is essential to ensure the law does not merely target those who directly commit the act but also reaches other parties who knowingly contributed to the commission of the crime.

The evidentiary aspect is inseparable from criminal liability in the digital era. Criminal activities can leave traces in the form of electronic data such as messages, digital documents, transaction information, system logs, device data, and account activity. Such evidence can serve as the basis for linking an individual to a criminal offense (Osman et al., 2025). However, the nature of digital data which is easily copied, transferred, modified, or deleted necessitates collection and examination mechanisms capable of preserving its authenticity and integrity. Errors in evidence management can compromise its probative value and potentially impede judicial proceedings.

Therefore, the adaptation of criminal law must be accompanied by capacity building for law enforcement officials. Investigators, public prosecutors, and judges require an adequate understanding of digital technology and the characteristics of electronic evidence. Such capabilities are essential not only for identifying perpetrators but also for assessing the relationship between digital data and the elements of a criminal offense. The use of digital forensic technology, data security procedures, and human resource development are crucial components in establishing a law enforcement system capable of keeping pace with the evolution of cybercrime (Tarantang & Pelu, 2024).

Issues of accountability become increasingly complex when criminal offenses are committed across borders. Perpetrators may be located in a different jurisdiction than the victim, while the data or services utilized are stored on digital infrastructure in another country. In such scenarios, law enforcement faces challenges regarding jurisdiction, access to evidence, and disparities between national legal systems (Johnson et al., 2020). Consequently, the adaptation of criminal law must be supported by international cooperation, information exchange, and legal assistance mechanisms to prevent perpetrators from exploiting jurisdictional differences to evade legal proceedings. Conversely, technological advancements must not serve as a pretext for diminishing the protection of individual rights. Law enforcement actions against digital crime must uphold the principles of due process, legal certainty, and personal data protection. The collection of digital evidence, access to devices, and data examination must be conducted based on clear legal authority and accountable procedures. Striking a balance between law enforcement needs and the protection of public rights is vital to ensure that efforts to combat cybercrime do not give rise to new forms of legal violations (Irhamdessetya, 2025).

Thus, the adaptation of criminal law and the determination of criminal liability in the digital era are interconnected aspects. Adaptation is necessary to ensure that criminal legal norms keep pace with evolving forms of crime, while accountability is essential to ensure that penalties are imposed only on parties with proven involvement and culpability. Both aspects require support through clear regulations, robust mechanisms for handling electronic evidence, adequate official capacity, and inter-agency as well as international cooperation. Ultimately, criminal law in the digital era must be developed into a system that is both adaptive and grounded in fundamental legal principles. Regulatory reform should aim not only to expand the scope of criminal offenses but also to clarify the elements of the act, forms of culpability, liability,

DOI: https://doi.org/10.47353/bj.v5i11.753

jurisdiction, and the use of electronic evidence. Such an approach will facilitate effective law enforcement against digital fraud and cyber offenses while upholding legal certainty, fairness, proportionality, and the protection of public rights within the digital environment.

Strengthening Law Enforcement against Cybercrime

The first aspect requiring reinforcement is a legal framework capable of keeping pace with technological advancements. Regulations concerning cybercrime must clearly define prohibited acts, the elements of the offense, perpetrator liability, and applicable sanctions. Normative clarity is essential to provide legal certainty for the public while facilitating investigations and prosecutions by authorities. Legal updates must also address emerging *modus operandi*, such as digital platform-based fraud, identity theft, data manipulation, the misuse of electronic systems, and various other crimes exploiting technological developments (Assessing Law Enforcement's Cybercrime Capacity and Capability, n.d.).

Regulatory strengthening must be harmonized with the criminal justice system as a whole. Provisions governing digital activities must clearly align with general criminal law to avoid overlaps or conflicting interpretations. Such harmonization is crucial to ensuring that law enforcement remains grounded in the principles of legality, legal certainty, and proportionality. Consequently, legal reform should not merely focus on increasing criminal penalties but also on clarifying enforcement mechanisms and legal protections for all parties involved (Gustryan & Sulaiman, 2025). Beyond regulation, strengthening the capacity of law enforcement personnel is a critical factor. Cybercrime requires specialized knowledge regarding information technology, computer networks, cybersecurity, digital transactions, and digital forensics. Investigators must understand how crimes are committed and how digital footprints can be utilized to identify perpetrators. Public prosecutors and judges also require an adequate understanding of the nature of electronic evidence to assess its relevance and probative value during judicial proceedings. Competence can be enhanced through education, continuous training, certification, and the development of specialized units with expertise in cybercrime (Kuswardani et al., 2026).

Strengthening law enforcement also necessitates the use of technology in inquiry and investigation processes. Digital forensic technology enables law enforcement to acquire, secure, and analyze data related to criminal offenses. The use of such technology must be accompanied by clear procedures to ensure that the evidence obtained retains its integrity and stands up to scrutiny in court. The process of collecting digital evidence must account for data authenticity, the chain of custody, and the legal authority to obtain information (Zulyadi et al., 2025). With appropriate mechanisms in place, electronic evidence can serve as a crucial tool in solving cybercrimes. In cases of digital fraud, law enforcement efforts must also focus on tracing the flow of funds and recovering victims' losses. Digital fraud frequently involves fund transfers across various bank accounts, digital wallets, or electronic payment services. Perpetrators can rapidly move the proceeds of their crimes, making the tracing process dependent on coordination between law enforcement agencies and financial service providers. A swift response is essential to ensure that assets linked to the crime can be promptly traced and—provided there is a legal basis—subjected to action in accordance with established procedures. This approach demonstrates that law enforcement regarding digital crime focuses not only on apprehending perpetrators but also on protecting and restoring the rights of victims.

The cross-border nature of cybercrime necessitates enhanced international cooperation. Perpetrators can commit offenses from other countries, utilize digital infrastructure located in different jurisdictions, or exploit the services of globally operating companies. In such scenarios, national law enforcement agencies

DOI: https://doi.org/10.47353/bj.v5i11.753

face limitations in obtaining data or taking legal action outside their own jurisdictions. Cooperation through information exchange, mutual legal assistance, and inter-agency coordination is crucial to overcoming these obstacles. Effective international cooperation can accelerate the identification of perpetrators and the securing of digital evidence (Frimpong et al., 2026).

Law enforcement efforts must also engage digital platform providers and the private sector. Many digital activities take place on social media platforms, e-commerce sites, communication services, and digital financial systems managed by non-governmental entities. Service providers possess the data and technical capabilities to help detect suspicious activity and support law enforcement processes in accordance with applicable regulations. However, such cooperation must respect the limits of authority, data protection, and user privacy rights. Mechanisms for requesting and providing data must operate transparently and be grounded in a clear legal framework.

Beyond a reactive approach, strengthening law enforcement requires complementary prevention strategies. The public plays a vital role in fostering a safe digital environment. Low digital literacy increases the risk of falling victim to fraud, identity theft, and various forms of cybercrime. Consequently, the government and relevant institutions must enhance public education regarding account security, personal data protection, the recognition of fraud schemes, and the safe use of digital services. Preventive measures can reduce the likelihood of crimes occurring while simultaneously improving the public's ability to report suspicious activity (Syahfallah et al., 2025).

Ultimately, strengthening law enforcement against cybercrime requires an integrated approach. Adaptive regulations must be supported by competent personnel, adequate investigative technology, robust mechanisms for handling electronic evidence, inter-agency coordination, and international cooperation. These elements are interconnected, as a weakness in one aspect can diminish the overall effectiveness of countermeasures. Effective law enforcement must also strike a balance between the need to combat crime and the protection of public rights ("Expanding the Potential of the Preventive and Law Enforcement Function of the Security Police in Combating Cybercrime in Ukraine and the EU," 2020).

Consequently, strengthening law enforcement against cybercrime is not merely a matter of enhancing the capacity of authorities to apprehend perpetrators; it is a process of building a legal ecosystem that is responsive to technological changes. An approach combining regulatory reform, human resource development, the use of digital forensics, victim protection, cross-sector collaboration, and digital literacy-based prevention will provide a more robust foundation for addressing the evolution of cyber offenses. Such a strategy is expected to foster law enforcement that is more effective and adaptive, while upholding legal certainty, justice, and the protection of public rights in the digital era.

CONCLUSION

The advancement of digital technology has brought about significant transformations in the nature and characteristics of crime, particularly regarding digital fraud and cyber offenses. A normative-juridical study employing both statutory and conceptual approaches reveals that digital crimes are characterized by their dynamic, anonymous, and rapid nature, as well as their ability to transcend jurisdictional boundaries. These conditions pose challenges for criminal law, specifically concerning the definition of offenses, perpetrator liability, electronic evidence, and the determination of jurisdiction. The study indicates that criminal law must continuously adapt to ensure legal certainty and public protection without compromising the principles of legality, justice, proportionality, and the protection of individual rights.

Strengthening law enforcement against cybercrime requires an integrated approach involving the updating and harmonization of regulations, enhancing the competence of law enforcement personnel, optimizing digital forensic technologies, bolstering electronic evidentiary mechanisms, and fostering inter-agency and cross-border cooperation. Countermeasures must also be accompanied by preventive efforts, such as improving digital literacy and protecting the public as technology users. Through this approach, criminal law is expected not only to respond to crimes that have already occurred but also to establish a law enforcement system that is adaptive to technological advancements and capable of addressing various forms of digital crime in the future.

REFERENCES

Asli, M. R. (2023). Digital Trends of Criminology and Criminal Justice of the 21st Century. *Journal of Digital Technologies and Law*, *1 (eng)*(1). https://cyberleninka.ru/article/n/digital-trends-of-criminology-and-criminal-justice-of-the-21st-century

Assessing Law Enforcement's Cybercrime Capacity and Capability. (n.d.). FBI: Law Enforcement Bulletin. Retrieved August 19, 2026, from https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability-

Baker, D. J., & Robinson, P. H. (2020). *Artificial Intelligence and the Law: Cybercrime and Criminal Liability*. Routledge.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal*, *29*(3), 408–433. https://doi.org/10.1108/13639510610684674

Criminal Behavior in the Digital Environment: Historical Foundations and a Sociological Perspective. (2025). *Revista Universitară de Sociologie*, *XXI*(2), 10–20. https://www.ceeol.com/search/article-detail?id=1408294

Dobrovolska, O., Rozhkova, M., & NULL. (2024). The Impact of Digital Transformation on the Anti-Corruption and Cyber-Fraud System. *Business Ethics and Leadership*, *8*(3), 231–252. https://armgpublishing.com/journals/bel/volume-8-issue-3/article-15/

Dupuis, D., Smith, D., & Gleason, K. (2021). Old frauds with a new sauce: Digital assets and space transition. *Journal of Financial Crime*, *30*(1), 205–220. https://doi.org/10.1108/JFC-11-2021-0242

Expanding the Potential of the Preventive and Law Enforcement Function of the Security Police in Combating Cybercrime in Ukraine and the EU. (2020). *TEM Journal*, *9*(2), 460–468. https://www.ceeol.com/search/article-detail?id=869809

Faisal, F., & Ulya, I. R. (2026). Transformation of Legal Communication in the Criminal Justice System in the Digital Era. *Realism: Law Review*, *4*(1), 22–53. https://doi.org/10.71250/rlr.v4i1.101

Financial crime and fraud in the age of cybersecurity. (n.d.).

Frimpong, S., Udechukwu, C. C., Adeoba, M. I., Mensah, T. K., & Mensah, D. (2026). Assessing the Effectiveness of Cybercrime Laws in Africa: A Systematic Review of Enforcement Barriers and Policy Reform Options. *Current Research in Interdisciplinary Studies*, *5*(4), 1. https://doi.org/10.58614/cris541

Graham, R. S., & Smith, 'Shawn K. (2024). *Cybercrime and Digital Deviance*. Taylor & Francis.

Gustryan, M., & Sulaiman, A. (2025). The Urgency of Regulatory Reformulation and Strengthening the Capacity of Law Enforcers in Combating Cybercrime Through a Criminal Law Approach in Indonesia. *Greenation International Journal of Law and Social Sciences*, *3*(2), 221–229. https://doi.org/10.38035/gijlss.v3i2.416

Hartomi, Sunggara, M. A., & Sukrisno, W. H. (2026). Criminal Liability For Algorithmic Manipulation in The Dissemination of Information in The Digital Era. *KRTHA BHAYANGKARA*, *20*(2), 555–574. https://doi.org/10.31599/krtha.v20i2.5544

Irhamdessetya, H. (2025). Criminal Policy on Digital Crime in Building Smart and Sustainable Communities in the Age of Disruption. *The Virtual International Conference on Economics, Law and Humanities*, *4*(1), 335–341. https://callforpaper.unw.ac.id/index.php/ICOELH/article/view/1807

Johnson, D., Faulkner, E., Meredith, G., & Wilson, T. J. (2020). Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts. *The Journal of Criminal Law*, *84*(5), 427–450. https://doi.org/10.1177/0022018320952559

Katyal, N. K. (2001). Criminal Law in Cyberspace. *University of Pennsylvania Law Review*, *149*(4), 1003–1114. https://doi.org/10.2307/3312990

Kuswardani, K., Kurnianingsih, M., Prakosa, A. L., & Fairuzzaman, F. (2026). Cybercrime Growth and Law Enforcement Challenges in Indonesia: A Cybercriminology Perspective. *Journal of Mathematics Instruction, Social Research and Opinion*, *5*(1), 991–1006. https://doi.org/10.58421/misro.v5i1.1315

L, I. (2023). CRIMINAL LIABILITY FOR CYBERCRIMES IN THE BRICS COUNTRIES. *BRICS Law Journal*, *10*(1), 59–87. https://cyberleninka.ru/article/n/criminal-liability-for-cybercrimes-in-the-brics-countries

Maagbeh, M. M. F. A. (2026). Crime, Justice, Administration, and the Transformation of Society in the Digital Era. *Journal of Intelligent Decision Making and Information Science*, *3*(6s), 1313–1322. https://doi.org/10.59543/jidmis.v3.1501

Nadaradjan, C. (2025). Criminal Liability in the Digital Age: A Comparative and Behavioural Framework for Cybercrime in an AI-Driven World. *International Journal of Engineering Science & Humanities*, *15*(1), 123–128. https://www.ijesh.com/j/article/view/451

Nourelhouda, M. (2024). CYBER FRAUD IN THE CONTEXT OF DIGITAL TRANSFORMATION IMPLICATIONS AND SOLUTIONS. *Russian Law Journal*, *12*(2), 2343–2353. https://cyberleninka.ru/article/n/cyber-fraud-in-the-context-of-digital-transformation-implications-and-solutions

Olukunle Oladipupo Amoo, Akoh Atadoga, Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Femi Osasona, & Benjamin Samson Ayinla. (2024a). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*, *21*(2), 205–217. https://doi.org/10.30574/wjarr.2024.21.2.0438

Olukunle Oladipupo Amoo, Akoh Atadoga, Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Femi Osasona, & Benjamin Samson Ayinla. (2024b). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*, *21*(2), 205–217. https://doi.org/10.30574/wjarr.2024.21.2.0438

Osman, Y. H. M., John, D. J., Ahmed, D. A., Mohamed, R. M. A., & Ali, R. M. S. A. (2025). Criminal Responsibility in the Age of AI: Rethinking Legal Accountability. *African Journal of Law and Justice System*, *4*(3), 179–199. https://doi.org/10.31920/2753-3123/2025/v4n3a9

Rawat, R., Mahor, V., Rawat, A., Garg, B., & Telang, S. (2021). Digital Transformation of Cyber Crime for Chip-Enabled Hacking. In *Handbook of Research on Advancing Cybersecurity for Digital Transformation* (pp. 227–243). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-7998-6975-7.ch012

Rossy, Q., & Ribaux, O. (2020). Orienting the Development of Crime Analysis Processes in Police Organisations Covering the Digital Transformations of Fraud Mechanisms. *European Journal on Criminal Policy and Research*, *26*(3), 335–356. https://doi.org/10.1007/s10610-020-09438-3

Saghir, W., & Kafteranis, D. (2022). The Applicable Law on Digital Fraud. In N. Mansour & L. M. Bujosa Vadell (Eds.), *Finance, Law, and the Crisis of COVID-19: An Interdisciplinary Perspective* (pp. 221–235). Springer International Publishing. https://doi.org/10.1007/978-3-030-89416-0_14

Sari, R. M. P. (2025). Criminal Responsibility in Cybercrime: An Analysis of Phishing Crimes in Indonesia. *Jurnal Hukum Dan Keadilan*, *2*(5), 49–55. https://doi.org/10.61942/jhk.v2i5.418

Sihombing, L. A., & Nuraeni, Y. (2023). Norms and Ethics in Criminal Justice: Assessing Contemporary Legal Policy. *Jurnal Info Sains : Informatika Dan Sains*, *13*(03), 1088–1099. https://ejournal.seaninstitute.or.id/index.php/InfoSains/article/view/3693

Silalahi, J. A. S. (2023a). The Application of Criminal Law in the Digital Age: A Literature Review of Challenges and Opportunities. *Innovative: Journal Of Social Science Research*, *3*(2), 3658–3668. https://j-innovative.org/index.php/Innovative/article/view/678

Silalahi, J. A. S. (2023b). The Application of Criminal Law in the Digital Age: A Literature Review of Challenges and Opportunities. *Innovative: Journal Of Social Science Research*, *3*(2), 3658–3668. https://j-innovative.org/index.php/Innovative/article/view/678

Sinrod, E. J., & Reilly, W. P. (1999). Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws. *Santa Clara Computer and High-Technology Law Journal*, *16*, 177. https://access.heinonline.com/HOL/Page?handle=hein.journals/sccj16&id=185&div=&collection=

Syahfallah, Z. A., Razak, A., & Salle, S. (2025). The Effectiveness of Law Enforcement on Cybercrime: A Case Study of Online Fraud in South Sulawesi. *SIGn Jurnal Hukum*, *7*(2), 1116–1130. https://doi.org/10.37276/sjh.v7i2.557

Tarantang, J., & Pelu, I. E. A. S. (2024). Neo-Digitalism in the Legal System: Adapting Law to Technological Developments. *Jurnal Ilmu Hukum Tambun Bungai*, *9*(2), 519–530. https://doi.org/10.61394/jihtb.v9i2.495

Tawil, S., & Tarawneh, A. (2026a). Technology and the Law: Countering Cybercrime and Fraud in the Digital Age. In N. Al-Ramahi, A. M. A. Musleh Al-Sartawi, & M. Kanan (Eds.), *Artificial Intelligence in the Digital Era: Economic, Legislative and Media Perspectives* (pp. 1095–1105). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-89771-9_79

Tawil, S., & Tarawneh, A. (2026b). Technology and the Law: Countering Cybercrime and Fraud in the Digital Age. In N. Al-Ramahi, A. M. A. Musleh Al-Sartawi, & M. Kanan (Eds.), *Artificial Intelligence in the Digital Era: Economic, Legislative and Media Perspectives* (pp. 1095–1105). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-89771-9_79

Undale, P. S., & Shinde, V. (2024). Digital Transformation and Cyber Security: Unveiling Awareness. *Humanities & Language: International Journal of Linguistics, Humanities, and Education*, *1*(3), 191–197. https://doi.org/10.32734/ayr9wh15

Zulyadi, R., Maswandi, Kusbianto, Tarmizi, & Frensh, W. (2025). Cybercrime Investigation on Social Media: Implementation of Community Policing Moderated by Law Enforcement in the Indonesian National Police. *International Journal of Criminal Justice Sciences*, *20*(1), 36–49. https://www.ijcjs.com/menu-script/index.php/ijcjs/article/view/1017