International Journal of Multidisciplinary Research and Technology
ISSN 2582-7359, Peer Reviewed Journal, Impact Factor 6.325
www.ijmrtjournal.com

ROBBERY WITH VIOLENCE IN THE DIGITAL AGE AND LEGAL RESPONSES TO HYBRID PHYSICAL AND CYBER-ENABLED CRIME

[1]Rizki Adiputra, [2]Heni Siswanto, [3]Erna Dewi, [4]Ahmad Irzal Fardiansyah, [5]Rini Fathonah

[1]Graduate law student
[2,3,4,5]Lecturer of Law at the University of Lampung
Indonesia

Abstract

This article examines the evolving nature of robbery with violence in the digital age, where traditional physical acts of violence are increasingly facilitated by digital technologies. It analyzes the doctrinal challenges, evidentiary complexities, and victimological impacts of hybrid crimes that combine physical and cyber-enabled conduct. Through normative and comparative legal analysis, the study identifies significant gaps in existing criminal law frameworks and highlights the need for substantive and procedural legal reforms. The article concludes that an adaptive and rights-based legal response is essential to ensure the effectiveness, fairness, and legitimacy of criminal justice systems in addressing technologically facilitated violent crime.

Keywords: Robbery, Cyber, Crime

Background

The rapid development of information and communication technology has fundamentally transformed the structure of contemporary societies, reshaping the ways in which individuals interact, conduct economic activities, and engage with public and private institutions. Digitalization has significantly accelerated the circulation of information, enhanced global connectivity, and created new opportunities for social and economic advancement. At the same time, these technological advancements have generated novel forms of criminal behavior that challenge traditional legal frameworks. One of the most pressing phenomena in modern criminal law is the emergence of hybrid crimes, particularly robbery with violence that is increasingly facilitated and amplified through digital technologies (Wall, 2007).

Traditionally, robbery with violence has been understood as a property crime involving the taking of another person's property through the use of force or the threat of force against the victim. This offense has long been recognized across legal systems, including both civil law and common law traditions. However, the contemporary landscape of criminal behavior demonstrates a significant evolution in the modus operandi of such crimes. Offenders no longer rely solely on physical strength or direct intimidation but increasingly exploit digital platforms to gather personal information, track victims' movements, manipulate communication, and coordinate criminal activities in real time. This shift reflects a broader transformation in crime patterns, where physical and digital dimensions are no longer separate but deeply interconnected (McGuire and Dowling, 2013).

The integration of cyber capabilities into conventional crimes has led scholars to conceptualize a distinct category of criminal behavior referred to as "cyber-enabled crime." In this model, traditional offenses are not committed exclusively in cyberspace but are substantially facilitated by digital tools and online infrastructures. Robbery with violence represents a particularly illustrative example of this phenomenon. Perpetrators may use social media to identify potential victims, exploit data breaches to obtain sensitive personal information, or utilize encrypted messaging applications to coordinate complex criminal operations. These practices significantly enhance the efficiency, reach, and precision of criminal conduct, thereby increasing both the frequency and severity of harm to victims (UNODC, 2010).

From an institutional perspective, this development poses profound challenges to criminal justice systems. Many legal frameworks continue to conceptualize violent property crimes and cybercrimes as separate categories subject to distinct legal regimes. This structural separation often results in normative gaps and enforcement inefficiencies when confronting hybrid offenses. The absence of comprehensive legal definitions and integrated regulatory approaches limits the ability of law enforcement agencies to effectively investigate, prosecute, and adjudicate cases involving the convergence of physical violence and digital facilitation. Furthermore, procedural laws in many

jurisdictions remain ill-equipped to manage the complexities of digital evidence, including issues of authenticity, integrity, and admissibility (Brenner, 2010).

The transnational nature of digital infrastructures further complicates the legal response to digitally facilitated robbery. Digital communications, cloud-based data storage, and global social media platforms frequently operate across multiple jurisdictions, creating significant challenges related to territoriality and jurisdiction. As a result, acts that are planned digitally in one country may be executed physically in another, thereby undermining traditional principles of territorial criminal jurisdiction. International institutions have sought to address these challenges through various legal instruments, most notably the Council of Europe's Convention on Cybercrime (Budapest Convention, 2001). Nevertheless, while this convention provides a foundational framework for cooperation in cybercrime investigations, it primarily addresses offenses that occur within cyberspace and does not comprehensively regulate hybrid crimes that involve both physical violence and digital facilitation.

The implications of digitally facilitated violence are particularly significant from a victimological perspective. Victims of modern robbery with violence are often subjected not only to physical harm and financial loss but also to privacy violations and psychological trauma associated with the misuse of their personal data. The concept of "double victimization" has been widely discussed in contemporary victimology, referring to situations in which individuals are harmed both through digital exploitation and physical violence (Walklate, 2017). This duality of victimization raises fundamental questions regarding the adequacy of existing victim protection mechanisms, compensation schemes, and restorative justice approaches within current legal systems.

Another critical dimension of this phenomenon concerns evidentiary challenges. The successful prosecution of hybrid crimes often depends on the ability to establish a causal link between digital activities and physical acts of violence. This requires the effective collection, preservation, and analysis of digital evidence, including communication records, metadata, geolocation data, and system logs. However, the standards governing digital forensic practices vary considerably across jurisdictions, leading to inconsistencies in the treatment of electronic evidence during judicial proceedings. Without the harmonization of digital forensic standards, courts face significant difficulties in ensuring the reliability and probative value of such evidence, thereby jeopardizing the fairness and effectiveness of criminal trials (Casey, 2011).

In developing countries, these challenges are further exacerbated by disparities in technological capacity and institutional resources. The rapid expansion of internet access and smartphone usage in regions such as Southeast Asia, Africa, and Latin America has not been accompanied by a corresponding development in legal and technical infrastructure. According to data published by the International Telecommunication Union, global digital connectivity has expanded dramatically over the past two decades, particularly in emerging economies (ITU, 2020). While this expansion has supported economic growth and social inclusion, it has simultaneously increased societal vulnerability to technology-facilitated crime. National criminal codes in many jurisdictions continue to rely on traditional formulations of robbery and theft without adequately addressing the digital dimension of contemporary criminal conduct.

From a human rights perspective, the failure to effectively regulate and prevent hybrid forms of violence raises serious concerns regarding the state's obligation to protect fundamental rights. The right to personal security, the right to property, and the right to privacy are core elements of international human rights law. When legal systems are unable to respond adequately to technologically facilitated violence, states may be considered to have failed in fulfilling their positive obligations to protect individuals from foreseeable harm. The intersection between criminal justice policy and human rights standards has been extensively analyzed in international legal scholarship, emphasizing that effective protection against modern forms of violence is an essential component of the rule of law in democratic societies (Nowak, 2003).

In light of these developments, scholarly attention toward the regulation of hybrid crimes has intensified. However, existing literature often remains fragmented, focusing either on cybercrime or on traditional violent offenses without sufficiently examining their convergence. This gap in the literature underscores the necessity for comprehensive legal research that integrates doctrinal analysis, comparative legal perspectives, and policy-oriented evaluation. The present study seeks to contribute to this emerging field by examining how different legal systems conceptualize and regulate robbery with violence in contexts where digital technologies play a facilitating role.

This research is based on the premise that conventional criminal law doctrines require reconceptualization in order to remain effective in the digital age. The rigid distinction between physical and cyber domains is increasingly untenable in a reality where criminal conduct transcends traditional boundaries. By analyzing the limitations of existing legal frameworks and examining international best practices, this study aims to propose normative and institutional reforms capable of addressing the complex nature of cyber-enabled violent crime. Such reforms are not only necessary to enhance the effectiveness of law enforcement but also to strengthen public trust in the criminal justice system.

Ultimately, the urgency of this research is grounded in the recognition that legal systems must evolve in tandem with technological developments. Without timely and coherent legal responses, the gap between the sophistication of criminal methods and the capacity of legal institutions will continue to widen. This study, therefore, seeks to provide a conceptual and normative foundation for the development of more responsive and resilient criminal justice policies in addressing robbery with violence in the digital age, thereby contributing to the broader discourse on the modernization of criminal law in the twenty-first century.

Research Methodology

This study adopts a doctrinal (normative) legal research method with a qualitative analytical approach. The research primarily examines statutory regulations, judicial decisions, and legal doctrines concerning robbery with violence and cyber-enabled crime. A comparative legal approach is employed to analyze how selected jurisdictions regulate hybrid crimes involving physical violence and digital facilitation. Data are collected through library research, focusing on primary legal materials (criminal codes, conventions, and court rulings) and secondary materials (scholarly articles, textbooks, and official reports). The data are analyzed using statutory interpretation and conceptual analysis to identify normative gaps and propose legal reforms relevant to contemporary criminal justice systems.

Discussion

1. Doctrinal and Practical Challenges of Robbery with Violence in the Digital Age

Robbery with violence has historically been conceptualized as a crime involving the unlawful taking of property through force or the threat of force. This traditional legal construction presumes a direct physical confrontation between perpetrator and victim, a model that reflected social realities in pre-digital societies (Wall, 2007). However, the digital transformation of social life has fundamentally altered the way violent property crimes are planned, executed, and concealed.

In the contemporary context, offenders frequently utilize digital platforms to facilitate the commission of robbery. Social media is used to identify potential victims, track personal routines, and assess the value of targeted property (McGuire and Dowling, 2013). Encrypted messaging applications enable real-time coordination between perpetrators, while leaked or illegally acquired databases provide detailed personal information that allows criminals to minimize operational risk and maximize their success rate.

This development creates a serious doctrinal dilemma for criminal law. Many jurisdictions continue to regulate robbery as a purely physical offense, while cyber activities are treated as separate and often subordinate forms of criminality. This artificial separation no longer reflects empirical reality, as digitally facilitated robbery constitutes a hybrid crime combining elements of violence and cyber-enabled conduct (National Academies, 2014). As a result, legal systems struggle to attribute full criminal responsibility for preparatory digital acts that are essential to the commission of the offense.

The evidentiary structure of modern robbery cases has also undergone profound change. Traditional forms of proof, such as eyewitness testimony and physical traces, are now supplemented or even replaced by digital evidence. Communication metadata, geolocation records, cloud-based storage logs, and platform activity histories play a critical role in reconstructing criminal behavior (Casey, 2011). These forms of evidence introduce technical challenges related to authenticity, integrity, and chain of custody that traditional procedural frameworks were not designed to address.

The risk of digital manipulation further complicates judicial assessment. Advances in artificial intelligence have increased the feasibility of fabricating audio-visual materials, thereby weakening courts' confidence in the

reliability of electronic evidence (National Institute of Justice, 2016). At the same time, many legal systems lack standardized protocols for digital forensic examinations, resulting in wide disparities in evidentiary practices and judicial outcomes.

From a victimological perspective, robbery with violence in the digital age produces harms that extend far beyond physical injury and material loss. Victims are often subjected to prolonged privacy violations, including online surveillance and unauthorized use of personal data prior to the violent incident (Walklate, 2017). This dual experience of informational and physical harm has been conceptualized as "double victimization," highlighting the inadequacy of traditional compensation and support mechanisms in addressing the full spectrum of victim suffering.

Law enforcement responses to digitally facilitated robbery raise additional concerns in relation to privacy and human rights. To counter technologically sophisticated criminals, investigative authorities increasingly rely on expansive surveillance tools, bulk data collection, and remote digital access techniques. While these measures may be operationally effective, they carry significant risks of disproportionate interference with individual rights if implemented without strict legal safeguards and judicial oversight (Nowak, 2003).

Taken together, these doctrinal, evidentiary, and victimological challenges reveal a widening gap between the realities of contemporary violent crime and the capacities of existing legal frameworks. Robbery with violence can no longer be effectively understood or regulated as a purely physical act. Instead, it must be conceptualized as a socio-technical phenomenon that requires a rethinking of fundamental assumptions within criminal law theory and practice.

2. Comparative Legal Responses and Future Directions for Regulating Hybrid Violent Robbery

Comparative legal analysis demonstrates that states have adopted divergent strategies in responding to the phenomenon of digitally facilitated robbery with violence. Some jurisdictions have undertaken explicit legislative reforms to recognize the role of digital technologies as an aggravating factor in violent crime, while others continue to rely on traditional statutory language that makes no reference to cyber-enabled conduct (Council of Europe, 2001).

The Budapest Convention on Cybercrime represents the most influential international effort to harmonize legal responses to technologically mediated crime. Although primarily focused on cyber-dependent offenses, the procedural mechanisms introduced by the Convention, such as expedited data preservation and international mutual legal assistance, have significant relevance for the investigation of hybrid crimes involving physical violence and digital facilitation (Brenner, 2010). Nevertheless, the Convention does not provide a comprehensive doctrinal framework for integrating violent and cyber-enabled offenses, resulting in uneven national implementation.

Future regulatory models must therefore move beyond a rigid separation between traditional violent crime and cybercrime. Substantive criminal law should be modernized to explicitly recognize digital facilitation as a relevant component of the offence structure of robbery with violence. This can be achieved through legislative techniques such as aggravating clauses or the creation of hybrid offense categories that clearly define the role of digital conduct in the commission of physical violence (McGuire and Dowling, 2013).

Procedural reform is equally essential. The effectiveness of any substantive legal reform depends on the existence of clear, predictable, and technologically informed rules governing the collection and evaluation of electronic evidence. Standardized forensic protocols, judicial training in digital evidence assessment, and the establishment of specialized forensic units are increasingly viewed as necessary institutional prerequisites for effective prosecution (Casey, 2011).

Institutional capacity building emerges as a central theme in comparative experiences. Countries that have successfully improved their responses to cyber-enabled violent crime have invested heavily in specialized law enforcement units, inter-agency cooperation mechanisms, and international partnerships. These investments are particularly important in developing jurisdictions that face high exposure to digital crime but lack sufficient technical infrastructure (UNODC, 2019).

Victim protection policies also require significant recalibration. Existing legal systems often fail to provide adequate remedies for informational harm suffered by victims of hybrid crime. Comparative victimology research suggests that criminal justice systems should expand restitution frameworks to include compensation for data-

related harm and provide specialized psychological support services adapted to the realities of digital exposure (Walklate, 2017).

At the international level, the transnational nature of digitally facilitated robbery necessitates stronger mechanisms of cooperation. Traditional mutual legal assistance procedures are frequently too slow to preserve volatile digital evidence. Emerging models of rapid cooperation and direct communication between competent authorities offer a potential path forward, but their effectiveness depends on political will and legal harmonization among states (UNODC, 2010).

Ultimately, the regulation of robbery with violence in the digital age requires a balanced approach that integrates technological awareness with fundamental principles of criminal justice. While legislatures must expand the scope of liability to address digital facilitation, such expansion must remain constrained by the principles of legality, proportionality, and legal certainty to prevent overreach and protect fundamental rights (Nowak, 2003).

In conclusion, comparative analysis indicates that the most effective legal responses to hybrid violent robbery are those that combine substantive doctrinal reform, procedural modernization, institutional strengthening, and victim-centered policies. As digital technologies continue to evolve, criminal law must maintain adaptive capacity while preserving its foundational commitments to justice, fairness, and the protection of human dignity.

Conclusion

Robbery with violence in the digital age demonstrates a profound transformation of violent property crime, as traditional physical acts of force are increasingly preceded and facilitated by digital technologies. The convergence of online and offline criminal conduct exposes significant doctrinal, evidentiary, and institutional gaps within existing legal frameworks. Effective legal responses therefore require the modernization of substantive criminal law, the strengthening of digital evidence procedures, and the enhancement of institutional capacity, while simultaneously safeguarding fundamental rights and providing comprehensive protection for victims. Without adaptive and coherent reforms, criminal justice systems will remain ill-equipped to address the growing complexity of hybrid violent crime in contemporary society.

References

1. Brenner, S. W. (2010). *Cybercrime and the law: Challenges, issues, and outcomes*. Boston: Northeastern University Press.
2. Casey, E. (2011). *Digital evidence and computer crime* (3rd ed.). London: Academic Press.
3. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. Strasbourg: Council of Europe.
4. International Telecommunication Union (ITU). (2020). *Measuring digital development: Facts and figures*. Geneva: ITU.
5. McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. London: Home Office Research Report No. 75.
6. National Academies of Sciences, Engineering, and Medicine. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Washington, DC: National Academies Press.
7. National Institute of Justice. (2016). *Electronic crime scene investigation: A guide for first responders* (2nd ed.). Washington, DC: U.S. Department of Justice.
8. Nowak, M. (2003). *Introduction to the international human rights regime*. Leiden: Martinus Nijhoff Publishers.
9. United Nations Office on Drugs and Crime (UNODC). (2010). *The globalization of crime: A transnational organized crime threat assessment*. Vienna: United Nations.
10. United Nations Office on Drugs and Crime (UNODC). (2019). *Comprehensive study on cybercrime*. Vienna: United Nations.
11. Walklate, S. (2017). *Handbook of victims and victimology*. London: Routledge.
12. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity Press.

Use for Citation: Rizki Adiputra, Heni Siswanto, Erna Dew, Ahmad Irzal Fardiansyah, Rini Fathonah. (2025). ROBBERY WITH VIOLENCE IN THE DIGITAL AGE AND LEGAL RESPONSES TO HYBRID PHYSICAL AND CYBER-ENABLED CRIME. International Journal of Multidisciplinary Research and Technology, 6(12), 49–53. https://doi.org/10.5281/zenodo.17935449