Criminal Policy on Digital Crime in Building Smart and Sustainable Communities in the Age of Disruption

Hani Irhamdessetya[1]
Master of Law, Universitas Ngudi Waluyo, Indonesia[2].
Email Correspondence: haniirhamdessetya@unw.ac.id

Abstract

The rapid growth of digital technology has fostered data-driven smart communities while simultaneously intensifying complex and transnational digital crime. This article examines the ideal direction of criminal policy in addressing digital crime to support smart, sustainable, and just communities. Using a normative juridical method with a criminal policy approach, it analyzes legal frameworks, doctrines, and policy instruments. The study finds that conventional punitive policies are inadequate to address the evolving nature of digital crime. An adaptive, rights-based criminal policy is required, balancing effective enforcement with the protection of privacy, data protection, and freedom of expression. Such policy should integrate legal reform, institutional strengthening, preventive measures, and participatory governance. From a sustainable development perspective, adaptive criminal policy supports SDG 16, SDG 11, and SDG 9 by positioning criminal law as a strategic instrument in smart community governance.

Keywords: Criminal Policy; Digital Crime; Smart Governance.

Introduction

The rapid advancement of digital technology has fundamentally transformed social interaction, economic activity, and public governance.(Milakovich, 2012) Digital platforms, artificial intelligence, and data driven systems have become integral to the development of smart communities by enhancing efficiency, accessibility, and innovation in public services.(Criado & Gil-Garcia, 2019) Through digitalization, governments are increasingly able to provide responsive, transparent, and participatory services that support sustainable urban and community development. However, alongside these transformative benefits, digital disruption has simultaneously generated new forms of crime and intensified the complexity of conventional criminal behavior, commonly referred to as digital or cybercrime.

Digital crime including online fraud, data breaches, identity theft, cyber harassment, and the misuse of digital platforms pose serious threats to public trust, social security, and community resilience.(Godase, 2025) These crimes not only result in economic losses but also undermine the sense of safety and inclusiveness that is essential for building smart and sustainable communities.(Andriani et al., 2022) In digital environments where public services, social interaction, and economic activities increasingly depend on technology, the persistence of digital crime can weaken citizen confidence and discourage participation in digital governance initiatives. Without effective criminal law responses, technological progress risks exacerbating social vulnerability rather than improving public welfare.(Lestari et al., 2023)

Criminal policy plays a pivotal role in addressing digital crime by shaping how the state formulates, implements, and enforces penal measures(Ariyanti, 2019). Through criminalization, procedural regulation, and institutional enforcement, criminal policy serves as a primary instrument for safeguarding public interests in the digital sphere. Nevertheless, traditional criminal law frameworks often struggle to respond effectively to digital crime due to jurisdictional constraints, evidentiary challenges, rapid technological change, and the inherently transnational nature of cyber offenses.(McCusker, 2017) These structural limitations raise fundamental questions regarding the adaptability and effectiveness of existing criminal policies in protecting communities within an increasingly digitalized society.(Cahyono et al., 2025)

Based on these challenges, this paper addresses the following research problem, which also serve as the analytical framework of the discussion: How does the existing criminal policy respond to digital crime in the context of building smart communities in the age of digital disruption, What is the ideal direction of criminal policy in addressing digital crime to support the development of smart, sustainable, and just communities.

Using normative juridical approach with a criminal policy perspective, this study aims to highlight the strategic role of criminal law in safeguarding public security, enhancing legal certainty, and strengthening social trust in the digital era.

Research Urgency and Gap. Despite the growing body of literature on cybercrime and digital regulation, most existing studies remain fragmented and predominantly focus on technical dimensions of cyber offenses, law enforcement challenges, or isolated statutory analyses.(Brown, 2015) There is a notable lack of comprehensive research that situates criminal policy on digital crime within the broader framework of smart and sustainable community development.(Powell et al., 2018) Moreover, limited attention has been given to examining criminal law as a governance instrument that simultaneously addresses crime control, fundamental rights protection, and community resilience. This research in therefore urgent to fill the normative and conceptual gap by offering an integrated criminal policy analysis that aligns digital crime regulation with the objectives of smart community governance.(Simmler et al., 2023) By addressing this gap, the study provides a timely contribution to legal scholarship and policy discourse in responding to digital disruption in an increasingly technology driven society.

Novelty and Contribution. This study offers a distinctive contribution by positioning criminal policy on digital crime not merely as a law enforcement mechanism, but as a strategic instrument for building smart and sustainable communities.(Losavio et al., 2018) Unlike existing studies that predominantly focus on technical aspects of cybercrime or isolated legal provisions, this paper integrates criminal law policy analysis with the concept of smart community development. It introduces an adaptive, rights based criminal policy framework that balances crime control, technological innovation, and community resilience. The findings contribute theoretically to the development of criminal law policy in the digital era and practically to policy formulation aimed at strengthening public trust and sustainability within digitally driven communities.

Policy Implications. The findings of this study underscore that criminal policy on digital crime must be systematically aligned with the overarching goals of smart and sustainable community development. Policymakers are encouraged to adopt adaptive and forward looking legal frameworks that are responsive to rapid technological change while remaining grounded in fundamental rights protection.(Hagemann et al., 2018) Criminal law should be harmonized with data protection regimes, digital governance policies, and human rights standards to ensure proportional, transparent, and accountable enforcement. Furthemore, effective policy implementation requires strengthened interagency and international coordination, continuous capacity building for law enforcement in digital investigation and evidence handling, and the integration of preventive strategies such as public digital literacy programs and technological safeguards. By embedding criminal policy within a broader smart community governance framework, states can enhance public trust, reduce digital vulnerability, and ensure that criminal law contributes meaningfully to community resilience and long term sustainability in the age of disruption.

Research Method

This research employs a normative juridical method with a criminal law policy approach. The study is conducted through library-based legal research by analyzing primary legal materials in the form of statutory regulations on digital crime, supported by secondary materials such as legal doctrines, scholarly articles, and international conference proceedings, as well as tertiary legal references. Data are analyzed qualitatively using descriptive-analytical and prescriptive techniques to assess existing criminal policies and to formulate recommendations for adaptive criminal policy in building smart and sustainable communities in the digital era.

Discussion

Criminal Policy on Digital Crime in the Context of Smart Community Development

This section addresses Research Problem 1 by examining the distinctive characteristics of digital crime and critically evaluating existing criminal policy frameworks within the evolving context of smart community development, drawing upon contemporary theories of criminal policy, risk regulation, and digital governance.

Digital crime represents a significant challenge to modern criminal law systems. Unlike conventional crimes, digital crimes are frequently transboundary, technologically sophisticated, and highly dependent on digital evidence that is vulnerable to manipulation, loss, and jurisdictional complexity.(Valeriano & Maness, 2015) These characteristics complicate investigation, prosecution, and adjudication processes, particularly within legal systems historically designed for

territorially bounded, physically observable, and individualized criminal conduct. As a result, traditional criminal law frameworks often struggle to respond effectively to digital offenses that operate within decentralized and data-driven environments.(Smith et al., 2017)

From a theoretical perspective, digital crime reflects the transformation described in Ulrich Beck's risk society theory, in which contemporary harms increasingly arise from manufactured and systemic risks generated by technological advancement rather than direct physical wrongdoing.(Beck, 2006) Digital crime exemplifies this shift, as its impacts are often diffuse, networked, and mediated through complex technological infrastructures. Consequently, criminal policy must adapt from a reactive, offense-centered model toward a risk-oriented governance framework capable of addressing future-oriented digital threats.

Existing criminal policies generally respond to digital crime through the criminalization of specific cyber offenses, the expansion of investigative and surveillance powers, and the development of international cooperation mechanisms. These approaches reflect the influence of transnational criminal law theory, particularly through cybercrime conventions and mutual legal assistance regimes aimed at overcoming jurisdictional fragmentation.(Amoo et al., 2024) While such measures demonstrate state commitment to protecting public interests, their implementation often reveals structural weaknesses, including fragmented regulations, limited technical capacity among law enforcement agencies, and inconsistencies between substantive criminal law and procedural rules. These deficiencies reduce the overall effectiveness and legitimacy of criminal policy in addressing digital threats.

In this context, David Garland's concept of the "culture of control" provides a useful analytical lens.(De Giorgi, 2017) Late-modern criminal policy often oscillates between punitive expansion and managerial risk control, a tendency clearly visible in digital crime regulation. Although expanded criminalization and surveillance powers may signal state responsiveness, excessive reliance on punitive measures risks undermining public trust if not supported by institutional capacity, procedural safeguards, and accountability mechanisms.

Within the framework of smart community development, ineffective criminal policy poses broader governance risks. Smart communities depend on public trust in digital systems, data security, and fair, transparent governance. When digital crime is inadequately addressed, citizens may become reluctant to engage with digital public services, thereby weakening the inclusiveness, sustainability, and resilience of smart community initiatives. From the perspective of procedural justice theory (Tyler), the legitimacy of criminal policy depends not only on enforcement outcomes but also on public perceptions of fairness, transparency, and accountability. Digital crime enforcement that relies heavily on opaque technologies or intrusive data practices risks eroding this legitimacy, particularly in participatory and data-driven governance environments.(Nwaimo et al., 2023)

Moreover, regulatory criminology and risk-based governance theories, as articulated by scholars such as Jonathan Simon and Julia Black, highlight that contemporary criminal policy increasingly functions as a mechanism of risk management rather than moral condemnation alone. In smart communities where governance relies on predictive analytics, algorithmic systems, and interconnected digital infrastructures criminal policy must address both existing offenses and emerging systemic risks. When criminal policy remains siloed or reactive, regulatory gaps may be exploited by digital offenders, undermining the reliability of smart systems and eroding citizens' confidence in digital public services.

According to smart governance theory, effective smart communities require integrated legal frameworks that align criminal law, administrative regulation, data protection, and cybersecurity governance. Criminal policy on digital crime should therefore be understood as part of a broader governance ecosystem rather than a standalone punitive instrument. Synchronization with smart city regulations, digital governance standards, and data protection mechanisms is essential to ensure coherent and comprehensive protection.

Furthermore, insights from preventive justice and situational crime prevention theories support the argument that criminal policy should not focus solely on post-offense punishment. Preventive and anticipatory approaches such as early detection mechanisms, regulatory support for secure digital design (security by design), data protection by default, and collaboration among law enforcement agencies, technology providers, and community stakeholders are increasingly recognized as essential complements to penal enforcement. In smart communities, these strategies enhance institutional resilience and reduce digital vulnerability without inhibiting innovation or participation.

Drawing on responsive regulation theory (Ayres and Braithwaite), an effective criminal policy framework should combine enforcement, prevention, and cooperation in a graduated and adaptive manner. Such an approach enables criminal law to function proactively, preserves fundamental rights, and supports the long-term sustainability of smart communities.

In sum, theoretical insights from risk society theory, regulatory criminology, procedural justice, and smart governance reveal that existing criminal policies remain insufficiently aligned with the structural realities of digitalized communities. These limitations underscore the need for a more adaptive, rights-based, and integrated criminal policy framework an issue that will be further elaborated in the subsequent section on adaptive criminal policy for smart and sustainable communities.

Toward an Adaptive Criminal Policy for Smart and Sustainable Communities

This section addresses Research Problem 2 by formulating the ideal direction of criminal policy that is adaptive, rights based, and supportive of smart, sustainable, and just communities in the digital era.

The development of smart and sustainable communities requires an adaptive criminal policy that balances effective crime control with the protection of fundamental rights, including privacy, data protection, and freedom of expression. Excessive penalization and overly expansive surveillance powers risk stifling innovation and digital participation, while weak or fragmented enforcement exposes communities to persistent digital threats. Accordingly, criminal policy must be carefully designed to uphold the principles of proportionality, accountability, and transparency.

An adaptive criminal policy should emphasize flexibility and future-oriented regulation. This entails updating substantive legal definitions to accommodate emerging forms of digital crime such as algorithmic fraud, large-scale data exploitation, and technology-facilitated harassment through technology-neutral and principle-based criminalization. Such an approach ensures legal certainty while maintaining the capacity to respond to future technological risks.

Procedural adaptation is equally essential to address the evidentiary and jurisdictional challenges posed by digital crime. (Smith et al., 2017)As smart communities rely heavily on data-driven systems, digital evidence becomes central to criminal proceedings. Criminal policy must therefore strengthen procedural safeguards governing the collection, preservation, and admissibility of digital evidence, while simultaneously ensuring due process and robust protection of privacy rights. Maintaining this balance is crucial for sustaining public trust in digital governance and law enforcement institutions.

Furthermore, adaptive criminal policy requires institutional capacity building and effective inter-agency coordination. Responses to digital crime depend on cooperation among law enforcement agencies, prosecutors, courts, regulatory authorities, and private digital service providers. In the absence of integrated governance, fragmented institutional responses may weaken enforcement and create regulatory gaps. Criminal policy should thus promote coordinated enforcement models, information sharing, and continuous development of technical expertise.

In addition, criminal policy must be integrated with preventive and non-penal strategies. Overreliance on punitive measures risks unnecessary criminalization that may hinder technological innovation and community participation. Preventive approaches such as digital literacy programs, public awareness initiatives, technological safeguards, and collaborative governance involving public and private stakeholders should be embedded within the criminal policy framework to enhance resilience and reduce digital vulnerability.

An adaptive criminal policy should also be grounded in a risk-based and evidence-informed approach. Criminal law responses ought to be calibrated according to the level and scale of digital risk, prioritizing serious and systemic threats such as organized cybercrime, large-scale data breaches, and attacks on critical digital infrastructure.(Lehto, 2022) This approach enables more effective allocation of enforcement resources while avoiding disproportionate penalization.

Moreover, the adaptive orientation of criminal policy necessitates continuous legal evaluation and policy learning. Given the rapid evolution of digital technologies, criminal law cannot remain static. Periodic regulatory review, context-sensitive judicial interpretation, and policy feedback mechanisms are essential to ensure that criminal norms remain relevant, enforceable, and responsive to technological change.

Finally, the legitimacy of criminal policy in the digital era depends on transparency and meaningful public engagement. In smart communities, citizens are active participants in digital governance rather than mere objects of regulation. Therefore, the formulation and implementation of criminal policy should involve public consultation, clear accountability mechanisms, and

accessible legal remedies. Such participatory governance strengthens social trust, reinforces democratic values, and ensures that crime control measures contribute positively to inclusive and sustainable community development.

From the perspective of the United Nations Sustainable Development Goals (SDGs), an adaptive criminal policy on digital crime directly advances several interconnected goals. It supports SDG 16 (Peace, Justice, and Strong Institutions) by strengthening the rule of law, access to justice, and institutional accountability in the digital environment; SDG 11 (Sustainable Cities and Communities) by ensuring that smart community ecosystems are safe, inclusive, and resilient; and SDG 9 (Industry, Innovation, and Infrastructure) by protecting digital infrastructure while enabling innovation within a secure legal framework.

By explicitly aligning criminal policy with these SDGs, the regulation of digital crime can be understood not merely as a security agenda, but as an integral component of sustainable development policy. This alignment reinforces the argument that adaptive criminal policy is essential to ensuring that digital transformation advances social welfare, institutional trust, and long-term community sustainability in the age of disruption.

Conclusion

This study demonstrates that digital crime poses a serious and evolving challenge to the development of smart and sustainable communities in the age of disruption. While existing criminal policies play an essential role in safeguarding public interests, they often remain constrained by structural and normative limitations in addressing the complex, transnational, and technology-driven nature of digital crime. Such limitations risk eroding public trust in digital systems and weakening the resilience of communities that increasingly rely on technology-based governance and services.

In line with the policy implications identified in this study, the conclusion emphasizes that criminal policy must be reconceptualized as a strategic component of smart community governance rather than a purely repressive legal instrument. An adaptive and rights-based criminal policy one that is aligned with data protection, digital governance, and human rights frameworks can simultaneously enhance legal certainty, protect fundamental rights, and foster public confidence in digital transformation initiatives.

Accordingly, the effectiveness of criminal policy in the digital era depends on its ability to integrate enforcement, prevention, and governance objectives. By adopting a balanced and future-oriented criminal policy approach, states can ensure that technological advancement functions as a driver of innovation, inclusiveness, and community resilience. Ultimately, a coherent and adaptive criminal policy framework is a key prerequisite for building smart, sustainable, and trustworthy communities in the age of digital disruption.

Acknowledgements

The author gratefully acknowledges the academic support and intellectual contributions received during the preparation of this paper. Sincere appreciation is extended to fellow scholars and peer reviewers for their valuable insights, critical comments, and constructive suggestions that significantly improved the quality of this study. The author also thanks the academic institution for providing a supportive research environment and access to relevant legal and scholarly resources. All views expressed and any remaining limitations of this paper are solely the responsibility of the author.

Recommendations

Based on the findings and conclusions of this study, several recommendations can be proposed as follows:

For Policymakers

The government should undertake a reformulation of criminal law policy that is adaptive to the rapid development of digital technology. Regulatory updates should adopt a technology-neutral and principle-based approach to ensure that evolving forms of digital crime can be effectively addressed without inhibiting innovation. Furthermore, criminal policy must be harmonized with personal data protection regimes, digital governance frameworks, and human rights standards to ensure proportional, transparent, and accountable law enforcement.

For Law Enforcement Agencies and Related Institutions

Strengthening institutional capacity is an urgent necessity, particularly in enhancing the technical competencies of investigators, prosecutors, and judges in handling digital crimes and electronic evidence. Improved coordination among law enforcement agencies, digital sector regulators, and international cooperation mechanisms is also essential to address the transnational nature of digital crime, which cannot be effectively managed through fragmented or isolated responses.

For the Development of Smart Community Governance

Criminal policy on digital crime should not be oriented solely toward repressive measures but must be integrated with preventive strategies and smart community governance frameworks. Preventive approaches such as improving public digital literacy, implementing security by design and privacy by design, and fostering collaboration among government authorities, technology providers, and civil society should be incorporated into the criminal policy framework. In this way, criminal law functions as a supporting instrument for community resilience and public trust within the digital ecosystem.

For Academics and Future Researchers

Future research is encouraged to examine criminal policy on digital crime through empirical or comparative cross-national approaches in order to assess the effectiveness of existing policies within the context of smart community development. In addition, interdisciplinary studies linking criminal law, technology, and digital governance are necessary to further enrich the theoretical and practical development of criminal law policy in the digital era.

Overall, the implementation of these recommendations is expected to promote the establishment of an adaptive, just, and sustainability-oriented criminal policy framework, thereby supporting the development of smart and sustainable communities amid the dynamics of digital disruption.

References

Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). 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.

Andriani, A. D., Yuniawati, R. I., Hamidin, D., Priambodo, A., Sulaeman, M., Susanti, L., Darmawan, A., & Martono, S. (2022). Transformasi Indonesia Menuju Cashless Society. Tohar Media.

Ariyanti, V. (2019). Kebijakan penegakan hukum dalam sistem peradilan pidana Indonesia. Jurnal Yuridis, 6(2), 33–54.

Beck, U. (2006). Risk Society Revisited: eory, Politics and Research Programmes. In The sociology of risk and gambling reader (pp. 68–90). Routledge.

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55.

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). RIKONSTRUKSI HUKUM PIDANA TERHADAP KEJAHATAN SIBER (CYBER CRIME) DALAM SISTEM PERADILAN PIDANA INDONESIA: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. Dame Journal of Law, 1(1), 1–23.

Criado, J. I., & Gil-Garcia, J. R. (2019). Creating public value through smart technologies and strategies: From digital services to artificial intelligence and beyond. International Journal of Public Sector Management, 32(5), 438–450.

De Giorgi, A. (2017). Punishment and political economy. In Alternative criminologies (pp. 51–72). Routledge.

Godase, V. (2025). Navigating the digital battlefield: An in-depth analysis of cyber-attacks and cybercrime. International Journal of Data Science, Bioinformatics and Cyber Security, 1(1), 16–27.

Hagemann, R., Huddleston Skees, J., & Thierer, A. (2018). Soft law for hard problems: The governance of emerging technologies in an uncertain future. Colo. Tech. LJ, 17, 37.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3–42). Springer.

Lestari, R., Windarwati, H. D., & Hidayah, R. (2023). The power of digital resilience: Transformasi berpikir kritis dan penguatan kesehatan mental emosional di era disrupsi. Universitas Brawijaya Press.

Losavio, M. M., Chow, K.-P., Koltay, A., & James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. Security and Privacy, 1(3), e23.

McCusker, R. (2017). Transnational organised cyber crime: distinguishing threat from reality. In Transnational financial crime (pp. 415–432). Routledge.

Milakovich, M. E. (2012). Digital governance: New technologies for improving public service and participation. Routledge.

Nwaimo, C. S., Oluoha, O. M., & Oyedokun, O. (2023). Ethics and governance in data analytics: balancing innovation with responsibility. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(3), 823–856.

Powell, A., Stratton, G., & Cameron, R. (2018). Digital criminology: Crime and justice in digital society. Routledge.

Simmler, M., Canova, G., & Schedler, K. (2023). Smart criminal justice: Phenomena and normative requirements. International Review of Administrative Sciences, 89(2), 415–432.

Smith, G. J. D., Bennett Moses, L., & Chan, J. (2017). The challenges of doing criminology in the big data era: Towards a digital and data-driven approach. British Journal of Criminology, 57(2), 259–274.

Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.