

Article

Juridical Analysis of Criminal Law Enforcement in Economic Crime in the Bjorka Hacker Case in Indonesia

Petrus Bernadus Hanafi

¹Master of Law, Faculty of Law, Universitas Pancasila, Jakarta, Indonesia

Article information	Abstract
DOI : xxx Correspondence : qpk.han307@gmail.com	The rapid expansion of Indonesia's digital economy has been accompanied by increasingly sophisticated cybercrime, including the illegal acquisition and sale of personal data. The case of the hacker known as Bjorka, involving the theft and sale of personal data, exposed both the vulnerability of national data systems and the difficulty of holding offenders accountable under existing law. This study aims to analyse the legal construction of the illegal theft and sale of personal data attributed to Bjorka under Indonesian positive law, and to assess the adequacy of the legal protection available to victims of such data breaches. The study employs a normative juridical approach, grounded in statutory and conceptual analysis. Its primary legal materials are Law No. 11 of 2008 concerning Electronic Information and Transactions, as amended by Law No. 19 of 2016, and Law No. 27 of 2022 concerning Personal Data Protection, examined alongside secondary materials drawn from legal scholarship and relevant case documentation. The findings indicate that Bjorka's conduct satisfies the elements of cybercrime and may be subject to criminal penalties under the relevant provisions of both statutes. The analysis further identifies the statutory basis on which the theft and sale of personal data may be characterised as an offence and examines the remedies, compensation mechanisms, and supervisory oversight through which the framework addresses harm to affected data subjects. The study contributes to Indonesian digital-economic criminal law by clarifying how the Electronic Information and Transactions Law and the Personal Data Protection Law apply to large-scale personal-data offences, and by highlighting the need for stronger enforcement and more effective protection for data-breach victims as digital activity continues to expand.
Submission Track	
Submission : April 25, 2026 Final Review : June 10, 2026 Accepted : June 14, 2026	
Keywords	
Bjorka hacker, digital economic crime, data protection, law enforcement, cybercrime	



This is an open access article under the CC BY <https://creativecommons.org/licenses/by/4.0/>

INTRODUCTION

Criminal law enforcement in an era of rapid digitalization is a crucial issue requiring serious attention from all parties. Cybercrime, particularly the theft and misuse of personal data, has become a tangible threat that harms individuals and institutions and may undermine a country's social and economic stability (Noor, 2025; Suryandari, 2024). One prominent example that has drawn the attention of the public and law-enforcement agencies is the case of the hacker known as Bjorka, which attracted widespread attention in Indonesia between 2022 and 2025. Bjorka became known for allegedly breaching and exposing millions of personal records belonging to Indonesian citizens and strategic institutions, including confidential government documents and bank-customer data.

Such conduct not only compromises data security but also generates public anxiety and raises serious legal, technological, and human-rights concerns. The unauthorized acquisition and dissemination of personal data can expose individuals to identity theft, fraud, discrimination, and other forms of harm, while simultaneously weakening the integrity of institutions responsible for protecting information (Gulyamov & Raimberdiyev, 2023; Schubert & Barrett, 2024). From a philosophical perspective, personal-data protection is a fundamental expression of respect for privacy, autonomy, and human dignity. Personal data forms part of an individual's identity and must therefore be protected against exploitation and misuse by irresponsible parties (McCoy et al., 2023; Omotubora & Basu, 2020). The conduct attributed to Bjorka allegedly violates these fundamental values by treating personal information as a commodity rather than as a legally protected aspect of individual personhood. It also undermines public confidence in digital-security systems and government institutions, demonstrating that cybercrime produces consequences extending beyond individual victims to the legitimacy and reliability of digital governance as a whole (Mphatheni & Maluleke, 2022; Shandler & Gomez, 2022).

Since 2022, Bjorka has allegedly disclosed millions of personal records belonging to Indonesian citizens, including sensitive information such as national identity-card numbers, SIM-card registration data, and government data. If substantiated, the conduct indicates not merely unauthorized possession of information but a sequence of legally relevant acts: intrusion into protected electronic systems, acquisition of data without lawful authority, and subsequent transfer or public dissemination of that data. The alleged access would fall within Article 30 of Law No. 11 of 2008 concerning Electronic Information and Transactions, which prohibits intentional and unauthorized access to another person's computer or electronic system. The subsequent copying, transfer, or dissemination of personal data may also satisfy the material elements of Article 32, provided that the prosecution can establish that the information belonged to another person or to the public and that the acts were committed without right or lawful authorization. Accordingly, the legal assessment should distinguish between the initial unauthorized access and the later handling of the data, because each act may constitute a separate violation requiring proof of its own elements (Curley, 2022; Zhang & Bellovin, 2023). The strength of the case would ultimately depend on evidence establishing the source of the data, the method of intrusion, Bjorka's control over the relevant accounts or systems, the absence of authorization, and the connection between the accused conduct and the public disclosure.

The conduct is also legally relevant under Law No. 27 of 2022 concerning Personal Data Protection, which establishes rights for data subjects and imposes duties on data controllers to maintain the confidentiality, security, and lawful use of personal data. Articles 12 and 16 provide an important basis for protecting data-subject rights and seeking remedies where personal data is unlawfully processed, disclosed, or misused. The alleged conduct may therefore constitute not only an unauthorized interference with electronic information under the Electronic Information and Transactions Law but also a violation of the more specific personal-data protection framework. Depending on the evidence established, Articles 362 and 378 of the Indonesian Criminal Code concerning theft and fraud may also be considered, particularly where deception was used to obtain access, personal data was appropriated for unlawful gain, or the disclosure caused demonstrable financial or other legally recognizable losses to victims. These provisions should, however, be applied only where the prosecution can prove each offense's distinct elements, including unlawful intent, the method of acquisition, the existence of loss, and the causal connection between the alleged conduct and the resulting harm.

From a juridical perspective, the alleged offences must be assessed primarily under the Electronic Information and Transactions Law and the Personal Data Protection Law, which together establish the principal legal framework for addressing unauthorized access, unlawful acquisition, disclosure, and misuse of personal data. Their concurrent application is important because the alleged conduct may comprise several legally distinct stages: intrusion into an electronic system, obtaining or controlling personal data without authorization, and subsequently transmitting, selling, or publicly disseminating

that data. Treating these stages separately enables law enforcement to identify the specific elements of each offence and prevents the legal analysis from collapsing different forms of wrongdoing into a single general allegation.

Nevertheless, the existence of statutory provisions does not by itself ensure effective prosecution. Law enforcement must still prove the source and authenticity of the data, the method of access, the absence of authorization, the accused's control over the relevant accounts or systems, and the causal connection between the alleged conduct and the resulting harm. These evidentiary difficulties are intensified because digital crime may be transnational, difficult to trace, and continuously transformed by technological development (Suryandari, 2024; Zhou et al., 2024). Accordingly, the Indonesian legal framework must be supported by specialized digital-forensic capacity, interagency coordination, and mechanisms for obtaining and preserving electronic evidence. Without such measures, the gap between formal legal protection and practical enforcement may allow serious violations of personal-data rights to remain inadequately addressed. Furthermore, addressing these institutional challenges requires overcoming persistent obstacles related to agency coordination and the standardization of digital evidence protocols (Badzlin et al., 2026).

An adaptive and coordinated enforcement strategy is therefore required among law-enforcement agencies, information-technology specialists, public institutions, and the private sector. Sociologically, the alleged data breaches have had wide negative effects. Vulnerabilities in data security foster fear and reduce public confidence in the ability of government bodies and private organizations to manage personal information. Data breaches may also cause economic disruption and reputational damage that is difficult to remedy.

The present study examines the enforcement of criminal law in the context of economic crime through an analysis of the Bjorka hacker case. It pursues two principal objectives. First, it seeks to develop a legal characterisation of the alleged unlawful acquisition and sale of personal data by determining whether the conduct attributed to Bjorka fulfills the statutory elements of offences under the Electronic Information and Transactions Law and the Personal Data Protection Law, as well as how these provisions relate to the general provisions of the Indonesian Criminal Code. Second, the study evaluates the adequacy of legal protection afforded to victims of data breaches under Indonesian law, with particular attention to available remedies, compensation mechanisms, and supervisory arrangements. In doing so, the study contributes to the development of Indonesian digital-economic criminal law by clarifying the application of existing legal provisions to large-scale personal-data offences and identifying reforms needed to address the gap between formal legal protection and its effective implementation.

METHOD

This research applies a normative juridical method to examine the legal construction of the alleged unauthorized acquisition and disclosure of personal data in the Bjorka case. This method is appropriate because the study is primarily concerned with interpreting legal norms, determining the relationship between overlapping statutory provisions, and assessing the adequacy of existing legal protection rather than measuring the frequency or prevalence of cybercrime empirically. The analysis focuses on the application of the Electronic Information and Transactions Law, the Personal Data Protection Law, and relevant provisions of the Indonesian Criminal Code to the alleged conduct.

The study relies on literature-based legal materials comprising primary, secondary, and tertiary sources. Primary legal materials include Indonesian statutes and regulations, particularly the Electronic Information and Transactions Law, the Personal Data Protection Law, and relevant provisions of the Indonesian Criminal Code. Secondary legal materials include legal scholarship, academic articles, legal commentaries, and other studies addressing cybercrime, personal-data protection, electronic evidence, and criminal-law enforcement. Tertiary materials, such as legal dictionaries and reference works, are

used to clarify relevant legal concepts and terminology.

These materials are analyzed qualitatively through a statutory, conceptual, and case-oriented approach. The statutory approach is used to identify and interpret the elements of offences and the remedies available to victims. The conceptual approach clarifies the legal meaning of unauthorized access, unlawful acquisition, disclosure, personal-data misuse, and legal protection. The case-oriented approach connects those legal norms to the alleged facts of the Bjorka case without treating unproven allegations as established facts. The analysis compares the relevant provisions, examines their possible concurrent application, and evaluates whether the existing framework provides effective protection and enforceable remedies. This approach enables the study to identify both the strengths and limitations of Indonesian law, including potential overlaps between general criminal provisions and more specific rules governing electronic systems and personal data. The conclusions are therefore based on legal interpretation and systematic analysis of the relevant materials rather than on unsupported assumptions about the accused's guilt or the precise extent of the alleged harm.

RESULT AND DISCUSSION

Legal Construction of the Illegal Theft and Sale of Personal Data in the Bjorka Case

The alleged unlawful acquisition and sale of personal data attributed to Bjorka represents a serious form of cybercrime with significant implications for Indonesian digital-economic criminal law. Its potential harm extends beyond the immediate violation of individual privacy: large-scale data breaches may expose victims to identity theft, financial fraud, reputational damage, and psychological distress, while also undermining public confidence in institutions responsible for protecting personal information. The conduct may further threaten the integrity of digital infrastructure and, depending on the nature and source of the compromised data, raise broader concerns relating to national security and economic stability. Accordingly, its legal assessment must proceed through an integrated philosophical, juridical, and sociological analysis. This approach is necessary to determine not only whether the alleged conduct satisfies the statutory elements of offences under Indonesian law, but also whether the existing legal framework provides an effective and proportionate response to large-scale personal-data violations. Because the allegations must not be treated as established facts, the analysis should distinguish carefully between the reported conduct, the available evidence, and the legal consequences that would follow if the relevant elements of the offences were proven.

Philosophically, personal-data protection is grounded in respect for human rights, human dignity, autonomy, and the right to privacy. Personal data is not merely an economic asset or a technical resource; it is an extension of an individual's identity and personal sphere. Its collection, use, and disclosure must therefore be subject to legality, necessity, transparency, and accountability. Unauthorized acquisition and sale of personal data violate these principles by depriving individuals of meaningful control over information concerning themselves and by treating their identities as commodities without consent. If proven, the conduct attributed to Bjorka would represent not only an infringement of the privacy of millions of individuals but also a serious violation of their dignity and autonomy. The alleged mass dissemination of personal data further weakens public confidence in institutions entrusted with data governance, demonstrates the potential human consequences of inadequate information-security practices, and reinforces the state's obligation to establish effective preventive, remedial, and enforcement mechanisms (Gulyamov & Raimberdiyev, 2023; Rahmadani & Prastyanti, 2025; Schubert & Barrett, 2024). These philosophical considerations support a legal response that protects both individual rights and the public trust on which Indonesia's digital economy depends.

From a juridical perspective, the conduct implicates several provisions of Law No. 11 of 2008 concerning Electronic Information and Transactions, as amended by Law No. 19 of 2016. Article 30 prohibits intentional and unauthorized access to another person's computer or electronic system. Article

32 prohibits, without right, altering, adding, reducing, transmitting, damaging, removing, transferring, or concealing electronic information or electronic documents belonging to another person or to the public. Unauthorized access to confidential information and the subsequent dissemination of personal data may therefore attract imprisonment, fines, or both under the corresponding penalty provisions (Bagheri & Hassan, 2016; Pratama, 2023).

Law No. 27 of 2022 concerning Personal Data Protection provides a more specific legal framework for protecting data subjects and imposing duties on data controllers and processors to maintain the confidentiality, integrity, and security of personal data. Articles 12 and 16 recognize important data-subject rights, including the right to bring legal claims and seek compensation when personal data is unlawfully processed or misused. The law's criminal provisions also establish liability for persons who intentionally and unlawfully obtain, disclose, use, or falsify personal data. Accordingly, if the alleged conduct attributed to Bjorka is proven, it may constitute not merely unauthorized access to electronic systems but also an independent violation of personal-data protection obligations. The PDP Law therefore strengthens the legal basis for holding perpetrators accountable, protecting victims, and requiring responsible institutions to adopt effective safeguards against large-scale data breaches. Its application should, however, be assessed together with the Electronic Information and Transactions Law to avoid overlap and to determine whether the evidence satisfies the distinct elements of each offence (Aliyah & Putra, 2025; Tritto et al., 2020).

Article 32 paragraphs, and of the Electronic Information and Transactions Law provide a significant juridical basis for examining the alleged unauthorized acquisition, alteration, transfer, and dissemination of electronic information or documents, including victims' personal information. These provisions are particularly relevant where the conduct involved access to, transmission of, or disclosure of data without legal authority. Their application must, however, be assessed against the specific evidence and statutory elements of each paragraph rather than assumed solely from the existence of a data breach. In parallel, violations of Law No. 27 of 2022 concerning Personal Data Protection may trigger criminal and administrative sanctions, especially where personal data was unlawfully obtained, disclosed, used, or otherwise misused. The combined application of these laws strengthens the legal framework for addressing data theft by protecting both the integrity of electronic information and the rights of the individuals to whom the data relates, while ensuring that liability is imposed only when the relevant unlawful conduct is established.

From the perspective of the Indonesian Criminal Code, Article 362 on theft and Article 378 on fraud may also be relevant, but only if their specific statutory elements are established. Article 362 could be considered where personal data is treated as an object capable of possession and is unlawfully taken with the intention of exercising control over it or benefiting from it. Article 378 may apply where deception or a series of misleading acts was deliberately used to obtain personal data, access credentials, or a financial advantage, thereby causing loss to the victim. Nevertheless, the mere unauthorized access, copying, or disclosure of personal data does not automatically satisfy the elements of theft or fraud. Their application must therefore be assessed cautiously in relation to the evidence of unlawful taking, intent, deception, possession, causation, and actual material or non-material loss, while giving priority to the more specific provisions of the Electronic Information and Transactions Law and the Personal Data Protection Law (Badzlin et al., 2026; Priyati et al., 2024). This approach prevents overextension of general criminal offences and ensures that liability is based on the distinct legal character of the alleged conduct.

Sociologically, this form of crime has consequences that extend beyond the immediate harm suffered by individual victims. The disclosure of personal information reduces public trust in the ability of government agencies, private organizations, and digital-service providers to safeguard personal data. It also increases the risk of identity theft, financial fraud, reputational injury, psychological distress, targeted exploitation, and other forms of misuse. At a broader level, large-scale data breaches may discourage

public participation in digital services, weaken confidence in digital economic activities, and expose institutional weaknesses in data governance and cybersecurity. Accordingly, the social impact of the alleged conduct supports the need for an integrated response combining victim protection, institutional accountability, public education, stronger preventive safeguards, and effective law enforcement.

The legal response should therefore be preventive as well as repressive. Prevention requires public education, stronger organizational safeguards, and improved information-security systems. In the Bjorka case, law-enforcement authorities, particularly the Cybercrime Directorate of the Criminal Investigation Department of the Indonesian National Police, conducted investigations intended to identify and apprehend the perpetrator. This demonstrates institutional seriousness in addressing cybercrime. Technical and legal obstacles remain, however, including digital tracing, attribution of online conduct, collection and authentication of electronic evidence, and effective delivery of justice across jurisdictions (Amoo et al., 2024; Kumar, 2024; Manikandan, 2025).

The consequences of the alleged breach extend far beyond the immediate harm suffered by individual victims. By exposing weaknesses in the protection and governance of personal data, the incident intensified public distrust of government institutions, private organizations, and digital-service providers. The disclosure also increased victims' vulnerability to identity theft, financial fraud, targeted exploitation, psychological distress, and lasting reputational harm. At the institutional level, the case demonstrates that inadequate cybersecurity can undermine confidence in essential digital services and impose broader social and economic costs. It therefore illustrates not merely the vulnerability of Indonesian data systems to cyberattacks, but also the urgent need for stronger preventive safeguards, institutional accountability, and effective mechanisms to protect public trust and national digital stability.

Enforcement should therefore not rely exclusively on criminal penalties. Preventive measures must include improved data security and stronger public awareness of the need to maintain the confidentiality of personal information. Effective enforcement also requires coordination among relevant institutions. The Financial Transaction Reports and Analysis Center may assist in tracing financial activity associated with cybercrime, while the competent personal-data supervisory authority should monitor compliance and support victim protection. Such coordination is important for closing regulatory and institutional gaps as technology and offenders' methods continue to evolve.

Legal Protection for Victims of Data Breaches under Indonesian Law

Legal protection for victims of personal-data breaches, including those attributed to Bjorka, is essential to safeguarding citizens' constitutional rights, privacy, dignity, and security in the digital era. As information technology develops, the collection, storage, and processing of personal data have expanded across government, business, and public-service systems, increasing both the potential benefits and the risks of misuse. A data breach can expose individuals to identity theft, financial fraud, reputational damage, psychological distress, and continued exploitation beyond the initial disclosure. The state therefore has a responsibility to establish clear, effective, and enforceable legal mechanisms that prevent violations, hold responsible parties accountable, provide accessible remedies and compensation to victims, and restore public confidence in the protection of personal data.

The principal legal basis for protecting victims is Law No. 27 of 2022 concerning Personal Data Protection, read together with the Civil Code, the Electronic Information and Transactions Law, and their implementing regulations. This legal framework is significant because it does not treat a data breach solely as a violation of institutional security; it recognizes the individual data subject as the holder of legally protected rights. Accordingly, victim protection should encompass the right to receive clear information about the breach, obtain appropriate assistance, seek the cessation or limitation of unlawful processing, and pursue remedies for material and non-material harm where the legal requirements are satisfied.

The framework also distributes responsibility among data controllers, processors, and other relevant actors, thereby making accountability possible beyond the immediate perpetrator of the cyberattack. Controllers and processors are expected to adopt safeguards, maintain the confidentiality and security of personal data, and respond appropriately when a breach occurs. Where negligence, unlawful processing, or failure to comply with statutory duties contributes to the harm, victims should be able to pursue administrative, civil, and, where the elements of an offence are established, criminal remedies. This layered approach is essential because criminal prosecution alone may punish an offender without adequately restoring the victim's position or addressing institutional failures that enabled the breach.

Nevertheless, the existence of these legal instruments does not automatically guarantee effective protection. Victims may face difficulties identifying the responsible party, proving the causal connection between the breach and the harm suffered, preserving electronic evidence, quantifying non-material loss, and obtaining timely compensation. The effectiveness of the framework therefore depends on practical enforcement, accessible complaint and litigation mechanisms, institutional supervision, and coordination among law-enforcement authorities, regulatory bodies, and organizations responsible for processing personal data. A victim-centered interpretation of the law should ensure that procedural and evidentiary difficulties do not deprive victims of meaningful remedies, while still requiring proof of the relevant legal elements and preventing liability from being imposed without a sufficient legal and factual basis.

Philosophically, the legal protection of personal data is grounded in fundamental human-rights principles, particularly respect for human dignity, autonomy, privacy, and personal security. Personal information is not merely an economic asset or an administrative resource; it is closely connected to an individual's identity and capacity to control how information about them is collected, used, and disclosed. A data breach therefore constitutes more than a technical failure: it may interfere with the individual's autonomy, expose them to continuing harm, and weaken their ability to participate safely in social and economic life. The state must uphold these principles by recognizing personal-data protection as a legal right and by ensuring effective enforcement against both unlawful data processing and institutional negligence. Justice for victims should consequently extend beyond punishing perpetrators to include timely notification, accessible complaint mechanisms, effective remedies, and, where legally established, compensation for material losses, psychological harm, and other forms of legally recognized damage. Such protection is necessary to restore victims' dignity, reinforce institutional accountability, and maintain public trust in the digital systems on which contemporary society increasingly depends (Li & Heine, 2026; Murphy, 2021; Robalo & Rahim, 2023).

From a sociological perspective, a breach on the scale attributed to Bjorka produces harm that extends beyond the immediate exposure of personal information. It can undermine public confidence in government institutions, private data controllers, and digital services, while increasing feelings of vulnerability, anxiety, and distrust among affected individuals. When citizens believe that their personal data cannot be adequately protected, they may become less willing to use online public services, participate in digital transactions, or share information with institutions, thereby weakening the effectiveness of digital governance and social cooperation. The consequences may also be unevenly distributed, with individuals who lack financial resources, digital literacy, or access to legal assistance facing greater difficulty in preventing further misuse and obtaining redress. Law-enforcement and regulatory responses should therefore extend beyond the prosecution of individual perpetrators to include stronger preventive safeguards, mandatory institutional accountability, timely public notification, victim-support mechanisms, and sustained public education on personal-data security. These measures are necessary not only to reduce the likelihood of similar incidents but also to restore public trust and ensure that digital development does not deepen existing social inequalities (Apeh et al., 2024; Bua & Idris, 2025).

CONCLUSION

The cybercrime attributed to Bjorka presents a major challenge to the Indonesian legal system. The Electronic Information and Transactions Law and the Personal Data Protection Law provide a substantial legal framework for prosecuting perpetrators and protecting personal data. Nevertheless, public distrust and the social and economic consequences of data breaches demonstrate that enforcement and data-protection systems must continue to be strengthened. Legal protection for victims should be reinforced through accessible civil claims, effective compensation mechanisms, and supervision by the competent personal-data protection authority. Future priorities should include closer coordination among law-enforcement agencies, continuous improvement of information-technology security, and public education concerning personal-data protection. These measures are necessary to create effective data security and uphold human rights in Indonesia's digital environment.

REFERENCES

- Aliyah, I. F., & Putra, N. D. (2025). Analysis of criminal liability for personal data violations: Case studies of the General Elections Commission and e-commerce from the perspective of the ITE Law and the PDP Law 2023–2024. *West Science Law and Human Rights*, 3(4), 459–469. <https://doi.org/10.58812/wslhr.v3i04.2470>
- 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. <https://doi.org/10.30574/wjarr.2024.21.2.0438>
- Apeh, C. E., Odionu, C. S., Bristol-Alagbariya, B., Okon, R., & Austin-Gabriel, B. (2024). Enhancing data management and security protocols in financial sector projects. *World Journal of Advanced Research and Reviews*, 21(3), 2655–2666. <https://doi.org/10.30574/wjarr.2024.21.3.0735>
- Badzlin, M. Z., Adnin, K. P., Sembiring, J. M., Siahaan, J. C., & Ramadani, S. (2026). Application of legal sanctions against perpetrators of social media account theft based on the Law on Information and Electronic Transactions. *Discourse Journal on Law and Society*, 2(1), 46–51. <https://doi.org/10.70062/djls.v2i1.137>
- Bagheri, P., & Hassan, K. H. (2016). Data privacy in electronic commerce: Analysing legal provisions in Iran. *Journal of Politics and Law*, 9(7), 133–140. <https://doi.org/10.5539/jpl.v9n7p133>
- Bua, I. T., & Idris, N. I. (2025). Analisis kebijakan keamanan siber di Indonesia: Studi kasus kebocoran data nasional pada tahun 2024. *Desentralisasi*, 2(2), 100–114. <https://doi.org/10.62383/desentralisasi.v2i2.653>
- Curley, N. (2022). Death of the limited license to data: *United States v. Van Buren*. *SMU Science and Technology Law Review*, 25(1), 47–72. <https://doi.org/10.25172/smustr.25.1.4>
- Gulyamov, S., & Raimberdiyev, S. (2023). Personal data protection as a tool to fight cyber corruption. *International Journal of Law and Policy*, 1(7). <https://doi.org/10.59022/ijlp.119>
- Kumar, C. R. (2024). Cybercrime and the law: Challenges in prosecuting digital offenses. *Indian Journal of Law*, 2(5), 20–25. <https://doi.org/10.36676/ijl.v2.i5.53>
- Li, S., & Heine, K. (2026). Developing a harm-based approach to understand digital vulnerability in the era of AI: A perspective of the European Union. *Computer Law & Security Review*, 60, Article 106266. <https://doi.org/10.1016/j.clsr.2026.106266>
- Manikandan, K. P. (2025). Cross-border cybercrime litigation: Challenges in jurisdiction, evidence, and international cooperation. *Journal of Advanced Legal Studies*, 1(1), 22–32. <https://doi.org/10.63665/jals.v1.i1.03>
- McCoy, M. S., Allen, A. L., Kopp, K., Mello, M. M., Patil, D. J., Ossorio, P. N., Joffe, S., & Emanuel, E. (2023). Ethical responsibilities for companies that process personal data. *The American Journal of Bioethics*, 23(11), 11–23. <https://doi.org/10.1080/15265161.2023.2209535>
- Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime.

- International Journal of Research in Business and Social Science*, 11(4), 384–396. <https://doi.org/10.20525/ijrbs.v11i4.1714>
- Murphy, C. (2021). Technology and transitional justice. *Social Philosophy and Policy*, 38(2), 170–190. <https://doi.org/10.1017/s0265052522000103>
- Noor, M. A. F. (2025). Cybercrime and data protection emerging legal challenges. *International Journal of Law and Policy*, 3(9), 66–79. <https://doi.org/10.59022/ijlp.369>
- Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, 29(2), 151–173. <https://doi.org/10.1080/13600834.2020.1732055>
- Pratama, Y. A. (2023). Legal framework publication of state secrets via cyberspace in Indonesia. *Constitutionale*, 4(2), 99–110. <https://doi.org/10.25041/constitutionale.v4i2.3196>
- Priyati, S., Sudarsono, G. P., Sumartini, S., Permana, D. B., & Swastika, P. A. E. (2024). Legal liability for the crime of data theft in fake job postings. *Journal of Multidisciplinary Research*, 3(2), 57–70. <https://doi.org/10.56943/jmr.v3i2.643>
- Rahmadani, S., & Prastyanti, R. A. (2025). Human rights and cybersecurity: Reinforcing legal protections for personal data. *International Journal of Law Dynamics Review*, 3(1), 20–29. <https://doi.org/10.62039/ijldr.v3i1.80>
- Robalo, T. L. A. S., & Rahim, R. B. A. (2023). Cyber victimisation, restorative justice and victim-offender panels. *Asian Journal of Criminology*, 18(1), 61–74. <https://doi.org/10.1007/s11417-023-09396-9>
- Schubert, K. D., & Barrett, D. (2024). Data governance, privacy, and ethics. In *Technology, work and globalization* (pp. 87–110). Springer International Publishing. https://doi.org/10.1007/978-3-031-51063-2_5
- Shandler, R., & Gomez, M. A. (2022). The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology & Politics*, 20(4), 359–374. <https://doi.org/10.1080/19331681.2022.2112796>
- Suryandari, W. D. (2024). Efforts to reform law enforcement in tackling cybercrime. *International Journal of Law, Social Sciences and Management*, 1(2). <https://doi.org/10.69726/ijlssm.v1i2.27>
- Tritto, A., He, Y., & Junaedi, V. A. (2020). Governing the gold rush into emerging markets: A case study of Indonesia's regulatory responses to the expansion of Chinese-backed online P2P lending. *Financial Innovation*, 6(1), Article 20. <https://doi.org/10.1186/s40854-020-00202-4>
- Zhang, J., & Bellovin, S. M. (2023). Preventing intimate image abuse via privacy-preserving credentials. *SMU Science and Technology Law Review*, 26(2), 149–180. <https://doi.org/10.25172/smustr.26.2.2>
- Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and cybercrime: Exploring the convergence and divergence in digital criminality. *Asian Journal of Criminology*, 19(3), 419–439. <https://doi.org/10.1007/s11417-024-09436-y>