

Criminal Liability of Cybercrime Perpetrators from the Perspective of Personal Data Protection

Rahmawati¹, Syaiful Bahri², Muhammad Abdillah³, Benny Karya Limantara⁴

¹ Institut Rahmadiyah Sekayu, Indonesia; rahma.stihrahmaniyah@gmail.com

² Institut Rahmadiyah Sekayu, Indonesia; syaifulmusahatif@gmail.com

³ UIN Raden Fatah Palembang, Indonesia; muhammadabdillah@radenfatah.ac.id

⁴ Universitas Bandar Lampung, Indonesia; Email: beni.karya@ubl.ac.id

* Correspondence e-mail; rahma.stihrahmaniyah@gmail.com

Article history

Submitted: 2026/08/15; Revised: 2026/09/12; Accepted: 2026/10/13

Abstract

The expansion of digital technologies has increased the collection, processing, and circulation of personal data while creating new forms of cybercrime and challenges to privacy. This study aims to analyze criminal liability for cybercrime perpetrators from the perspective of personal data protection in Indonesia, particularly involving unlawful acquisition, disclosure, and use of personal data. The research employs normative juridical legal research using statutory, conceptual, and case approaches. Primary legal materials include Law No. 27 of 2022 concerning Personal Data Protection, Law No. 1 of 2024 concerning amendments to the Electronic Information and Transactions Law, relevant criminal-law provisions, and judicial decisions. The findings demonstrate that Indonesian law provides a stronger basis for criminal accountability, but liability cannot be established solely from the occurrence of a data breach. It requires precise attribution of unlawful conduct, legally relevant culpability, reliable electronic evidence, and differentiation between individual perpetrators, corporations, and electronic-system providers. The study concludes that personal data protection requires integration of criminal law, cybercrime regulation, corporate liability, and digital evidence. Its contribution lies in proposing an analytical framework for strengthening criminal accountability while maintaining legality, culpability, procedural fairness, and protection of data-subject rights.

Keywords

Corporate Criminal Liability; Criminal Liability; Cybercrime; Electronic Evidence; Personal Data Protection.



© 2026 by the authors. This is an open access publication under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY SA) license, <https://creativecommons.org/licenses/by-sa/4.0/>.

INTRODUCTION

The rapid expansion of digital technologies has fundamentally transformed the way personal information is collected, processed, exchanged, and utilized in contemporary society. In an ideal legal order, the increasing dependence on digital platforms should be accompanied by an equally strong system of personal data

protection, effective cybersecurity governance, and clear criminal accountability for unlawful conduct in cyberspace. Personal data should not merely be treated as an economic resource but as an extension of individual privacy and a component of constitutional protection of personal dignity. In Indonesia, this normative commitment has been strengthened through Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which recognizes personal data protection as part of the protection of individual rights and establishes obligations concerning data processing, the rights of data subjects, and criminal provisions for unlawful acquisition, disclosure, use, and falsification of personal data (Republic of Indonesia, 2022). The PDP Law therefore represents a significant shift from a fragmented regulatory approach toward a more integrated framework of data governance. Its criminal provisions specifically prohibit the unlawful acquisition or collection, disclosure, and use of another person's personal data, while Article 67 establishes imprisonment and fines for specified violations (Republic of Indonesia, 2022). This becomes particularly important because the PDP Law entered its full implementation phase in October 2024, creating a contemporary legal context in which the effectiveness and doctrinal coherence of criminal accountability mechanisms require closer examination (Ministry of Communication and Digital Affairs, 2024).

Empirically, however, Indonesia continues to face substantial cybersecurity and personal-data risks despite the strengthening of its legal framework. The 2024 Indonesian cybersecurity landscape recorded 1,367 cyber-incident notifications identified by the National Cyber and Crypto Agency's cyber contact center, with data breaches accounting for 535 incidents, or approximately 39.1% of the reported classifications, making data breach the largest identified category in that dataset (BSSN, 2024). Major incidents involving public and private digital infrastructure have further demonstrated that personal-data protection is not merely a theoretical legal concern but a practical problem involving potentially extensive social, economic, and privacy-related consequences. Research published during 2023–2025 has identified continuing difficulties in applying criminal responsibility to personal-data misuse, particularly regarding unauthorized acquisition, disclosure, and use of personal information, as well as uncertainty concerning liability when data protection failures occur within organizations (Nababan et al., 2023; Kurniawan et al., 2024). More recent studies likewise identify technological complexity, difficulties in proving fault and causation, limitations in digital forensics, cross-border jurisdiction, and weaknesses in cybersecurity compliance as significant obstacles to effective criminal enforcement (Husri & Samsul, 2026; Simanjuntak & Waluyo, 2025). The empirical reality therefore

demonstrates a critical tension: Indonesia has moved toward a stronger statutory framework, yet the increasing frequency and complexity of cyber incidents indicate that formal criminalization alone may not adequately secure personal data. The central problem consequently concerns how criminal responsibility should be constructed and applied when cybercriminal conduct causes, facilitates, or exploits violations of personal data protection.

A review of previous scholarship reveals an important research gap. Existing studies have generally examined personal-data misuse through a normative analysis of Law No. 27 of 2022, focusing separately on prohibited conduct, criminal sanctions, data-controller obligations, or particular forms of cybercrime such as doxing and hacking (Nababan et al., 2023; Alam, 2026). Other research has concentrated on the effectiveness of the PDP Law or on institutional and regulatory weaknesses, while studies of data breaches by electronic system providers have emphasized corporate responsibility, negligence, cybersecurity standards, and enforcement limitations (Sihotang & Ginting, 2026; Husri & Samsul, 2026). Although these contributions are valuable, they tend to analyze criminal liability within particular factual categories rather than developing an integrated framework connecting the elements of cybercrime, the principle of criminal fault, individual and corporate liability, unlawful processing of personal data, electronic evidence, and the protection of data subjects. A further deficiency lies in the limited examination of how the PDP Law interacts systematically with the amended Electronic Information and Transactions Law and the evolving Indonesian criminal-law framework. Recent scholarship has also identified the absence of cybercrime-specific procedural mechanisms and difficulties in identifying perpetrators and validating digital evidence in cases such as doxing (Fikriansyah & Harris, 2026). Thus, what remains insufficiently developed is not merely an identification of applicable sanctions, but a coherent doctrinal explanation of when, why, and on what basis a cyber offender can be held criminally responsible while simultaneously ensuring effective protection of the victim's personal data rights. This research addresses that gap by positioning criminal responsibility as the analytical bridge between cybercrime regulation and substantive personal-data protection.

The urgency of this research is strengthened by the fact that the Indonesian personal-data protection regime has entered a decisive implementation period. Since the PDP Law became fully applicable on 17 October 2024, public and private organizations have been expected to comply with its data-processing obligations, while the legal system must increasingly respond to actual violations rather than

merely establish abstract regulatory standards (Ministry of Communication and Digital Affairs, 2024). At the same time, cybercrime is becoming increasingly complex through ransomware, unauthorized access, identity theft, doxing, data exploitation, and transnational attacks, creating situations in which a single incident may involve several overlapping criminal acts and multiple potentially responsible actors. The 2024 National Data Centre ransomware incident, for example, demonstrated how cyberattacks can simultaneously disrupt public services and raise questions concerning the protection and governance of personal information (Yusliwidaka et al., 2024). From a legal-policy perspective, the current moment therefore requires more than additional criminal sanctions: it requires conceptual clarity regarding attribution, fault, participation, corporate responsibility, evidentiary standards, and the relationship between punishment and the restoration of victims' rights. Scientifically, examining these issues is important because criminal law must remain sufficiently precise to impose responsibility on genuinely culpable actors while avoiding an overly broad attribution of criminal liability for technological failures that may arise from complex organizational or systemic causes. A rigorous analysis can consequently contribute to a more balanced model in which deterrence, accountability, due process, cybersecurity governance, and effective protection of personal data operate within a coherent legal framework.

Accordingly, this research aims to analyze the criminal responsibility of perpetrators of cybercrime from the perspective of personal data protection, with particular attention to the legal elements of cyber offenses, forms of unlawful personal-data processing, the basis of individual and corporate criminal liability, and the evidentiary and enforcement challenges arising from cybercrime. It also seeks to examine the extent to which Law No. 27 of 2022 provides a sufficiently coherent legal foundation for attributing criminal responsibility to perpetrators whose conduct unlawfully obtains, discloses, uses, or falsifies personal data, while considering its interaction with the broader Indonesian cybercrime framework. The study is expected to contribute theoretically by strengthening the conceptual relationship between cybercrime, criminal responsibility, fault, and personal-data protection within Indonesian criminal law scholarship. Practically, the findings may provide a legal analytical framework for law-enforcement authorities, judges, prosecutors, investigators, data controllers, electronic-system providers, and policymakers in interpreting and applying criminal provisions concerning personal-data violations. More broadly, the research is expected to contribute to the development of a more coherent enforcement model that protects data subjects without sacrificing the

fundamental principles of legality, culpability, proportionality, and due process. In this respect, the study does not merely evaluate whether criminal sanctions exist, but investigates whether the existing framework can translate statutory protection into meaningful accountability in an increasingly complex digital environment.

METHODS

This study employs a normative juridical (doctrinal legal research) method with a statutory, conceptual, and case-oriented approach to examine criminal liability for perpetrators of cybercrime from the perspective of personal data protection. The normative juridical approach is appropriate because the research questions concern the interpretation, coherence, and application of legal norms governing unlawful acquisition, disclosure, use, and processing of personal data rather than the measurement of behavioral variables. The primary legal materials comprise Law No. 27 of 2022 on Personal Data Protection, Law No. 1 of 2024 amending Law No. 11 of 2008 on Electronic Information and Transactions, the Indonesian Criminal Code and relevant implementing regulations, while secondary legal materials consist of scholarly articles, legal books, research reports, and authoritative academic commentaries published primarily during 2020–2025. Relevant judicial decisions and documented cybercrime cases are treated as tertiary/case materials where they provide evidence of how criminal responsibility and personal-data violations are interpreted in practice. Data are collected through documentary and library research, using systematic identification, classification, and examination of relevant legislation, jurisprudence, academic literature, and official documents. The research instrument is a structured legal-document review matrix used to identify provisions concerning the elements of offenses, forms of culpability, perpetrators, sanctions, evidentiary requirements, and protection of data-subject rights (Marzuki, 2021; Soekanto & Mamudji, 2020).

The collected materials are analyzed qualitatively through juridical-normative analysis, beginning with legal interpretation and classification of the relevant statutory provisions, followed by conceptual analysis of criminal responsibility, culpability, cybercrime, and personal-data protection. The analysis subsequently compares the normative framework under the PDP Law with related cybercrime legislation and relevant judicial decisions to identify consistency, regulatory overlap, normative gaps, and difficulties in attributing criminal responsibility. A prescriptive analytical stage is then employed to formulate a legally reasoned interpretation concerning the appropriate construction of criminal liability for cybercrime involving personal data. This method is scientifically justified because the central issue is not how frequently

cybercrime occurs, but whether the existing legal norms provide a coherent and sufficiently precise basis for attributing criminal responsibility while protecting the rights of personal-data subjects. Accordingly, normative juridical research ensures direct alignment between the research objective, legal materials, analytical procedure, and expected contribution, while the statutory, conceptual, and case approaches enable the study to move beyond merely describing legislation toward critically evaluating its normative adequacy (Marzuki, 2021; Ali, 2021).

FINDINGS AND DISCUSSION

The normative analysis demonstrates that the Indonesian legal framework has established a relatively explicit basis for imposing criminal liability on perpetrators who unlawfully obtain, disclose, or use personal data in cyberspace. Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) constitutes the principal legal instrument because it directly criminalizes several forms of personal-data misuse and provides imprisonment and monetary penalties for violations of its substantive prohibitions. The analysis further indicates that the criminal provisions cannot be interpreted independently from the broader cybercrime framework, particularly Law No. 1 of 2024 amending the Electronic Information and Transactions Law. The two regulatory regimes address different but interconnected dimensions of cybercrime: the PDP Law emphasizes the unlawful treatment of personal data, whereas the electronic-transactions framework regulates broader unlawful conduct involving electronic systems and information. Consequently, criminal responsibility must be determined by identifying the precise unlawful act and matching its factual elements with the applicable statutory provision rather than automatically treating every data breach as a criminal offense. This finding is consistent with recent normative research demonstrating that Indonesia's PDP Law has strengthened the legal basis for criminal sanctions while leaving important questions concerning its practical application and enforcement unresolved (Kurniawan et al., 2024; Nababan et al., 2023).

The second finding concerns the elements required for criminal responsibility. The analysis shows that the existence of unauthorized access to or dissemination of personal data is insufficient by itself to establish criminal liability; investigators and prosecutors must establish the prohibited conduct, unlawfulness, the relevant form of culpability, the identity of the responsible actor, and a legally valid evidentiary connection between the actor and the cyber activity. This distinction is particularly significant in cases involving hacking, phishing, account takeover, doxing, unauthorized disclosure, or the exploitation of databases, because the person who obtains data, the person who distributes it, and the person who benefits from it may

be different actors. The research therefore identifies criminal responsibility as an attribution process rather than merely a consequence of the occurrence of a data breach. Previous research similarly indicates that difficulties arise when the legal framework is required to determine responsibility for personal-data misuse or failures in data protection, particularly where the relationship between the data controller, processor, and actual perpetrator is not clearly established (Nababan et al., 2023).

A third finding concerns the position of corporations and electronic-system providers in criminal responsibility. The analysis indicates that personal-data violations may involve not only individual cybercriminals but also organizational actors responsible for collecting, processing, storing, and securing personal data. The PDP framework provides a basis for addressing corporate responsibility, but attribution cannot be constructed solely from the fact that a security failure occurred within an organization. Criminal liability requires a connection between the prohibited conduct and the responsible individual or corporate entity, including evidence concerning authorization, organizational decision-making, negligence or intentional conduct where legally relevant, and failure to fulfil legally required duties. This distinction is important because a data breach resulting from an external cyberattack does not necessarily establish criminal culpability of the organization that controlled the data. Recent scholarship identifies the same problem, emphasizing that proving fault and causation remains a significant challenge, particularly where data breaches result from complex technological systems, inadequate internal security, or external attacks (Husri & Samsul, 2026). The results therefore support a differentiated model of liability in which direct perpetrators and organizational actors are assessed according to their respective conduct and legally established forms of responsibility.

The fourth finding concerns electronic evidence and enforcement limitations. The analysis reveals that the substantive criminalization of personal-data misuse is more developed than the procedural capacity required to establish responsibility in technologically complex cases. Cybercrime frequently involves anonymous accounts, encrypted communications, distributed infrastructure, foreign servers, rapidly changing digital traces, and multiple intermediaries. Consequently, proving who actually performed an unlawful acquisition, disclosure, or use of personal data requires reliable digital forensic evidence and an adequate chain of evidentiary attribution. Recent research on doxing reaches a similar conclusion, identifying difficulties in perpetrator identification and digital-evidence validation as significant enforcement obstacles and noting that general procedural mechanisms may not fully accommodate the distinctive characteristics of cybercrime (Fikriansyah & Harris,

2026). The research therefore finds a structural distinction between normative availability of criminal sanctions and practical enforceability of those sanctions. This distinction is critical because an expansive statutory prohibition does not automatically produce effective accountability when investigators cannot sufficiently establish the digital origin, identity, intent, participation, and causal relationship of the alleged perpetrator.

Finally, the overall findings indicate that criminal responsibility for cybercrime involving personal data in Indonesia should be constructed through an integrated interpretation of substantive criminal law, personal-data protection law, cybercrime regulation, and electronic evidence. The PDP Law provides a specific legal foundation for addressing unlawful acquisition, disclosure, and use of personal data, but its effectiveness depends upon accurate classification of the prohibited conduct and the ability of law enforcement to establish the relevant elements of criminal responsibility. The analysis also confirms a continuing normative and enforcement gap concerning attribution in complex data-breach cases, particularly where several actors, technological systems, or organizational responsibilities intersect. This finding corresponds with earlier research identifying ambiguity concerning responsibility for failures to protect personal data and the need for greater legal clarity concerning the responsibilities of data managers (Nababan et al., 2023). Thus, the results indicate that effective personal-data protection through criminal law requires more than the availability of sanctions: it requires precise attribution of culpability, technologically competent evidence-gathering, coherent application of overlapping legislation, and differentiation between intentional cybercrime and security failures that do not automatically constitute criminal conduct.

Table 1. Analytical Framework of Criminal Liability for Cybercrime Involving Personal Data

No	Legal Dimension	Main Issue	Analytical Focus
1	Unlawful Conduct	Unauthorized acquisition, disclosure, or use of personal data	Identification of prohibited acts and their statutory elements
2	Criminal Culpability	Intent, negligence, and attribution of responsibility	Determination of individual or corporate criminal liability

3	Electronic Evidence	Identification, authentication, and preservation of digital evidence	Establishing the connection between the perpetrator and the cybercrime
---	---------------------	--	--

The table 1. demonstrates that the transformation of urban open spaces into resilience infrastructure requires changes across several interconnected dimensions rather than a single physical intervention. Ecological capacity represents the foundational layer because vegetation, permeable surfaces, and retention areas enable open spaces to contribute to stormwater management and environmental regulation.

The findings demonstrate that criminal accountability for cybercrime involving personal data in Indonesia cannot be adequately understood through the PDP Law alone. The results indicate that Law No. 27 of 2022 provides a more specific criminal-law basis for unlawful acquisition, disclosure, and use of personal data, while the amended Electronic Information and Transactions Law addresses broader forms of cyber conduct such as unauthorized access and interference with electronic systems. This finding is consistent with Asmadi et al. (2023), who identified the PDP Law as introducing a more explicit criminal basis for unlawful dissemination of personal data compared with the earlier ITE framework. However, the present analysis extends that finding by demonstrating that the central legal problem is not simply the existence of overlapping statutes, but the qualification and attribution of the criminal act when one cyber incident simultaneously contains several legally distinct forms of conduct. Simanjuntak and Waluyo (2025), for example, similarly found that ransomware attacks involving personal data may constitute multiple offenses under the ITE Law and PDP Law. The theoretical implication is that the principle of legality requires each form of liability to be linked to clearly defined statutory elements, while the principle of culpability requires the prosecution to establish the offender's legally relevant mental relationship with the prohibited conduct.

This finding can be further explained through the actus reus–mens rea framework in criminal law. The occurrence of unauthorized access, disclosure, or use constitutes the factual dimension of the offense, but criminal responsibility requires more than proof that an unlawful event occurred. The distinction is theoretically important because criminal law generally rejects liability based exclusively on the occurrence of harmful consequences without an adequate basis for attribution and culpability. Nababan et al. (2023) similarly found that the regulation of personal-data misuse still presents difficulties in determining responsibility when the data are managed by another party. More recent scholarship reaches a comparable conclusion, emphasizing that personal-data misuse can involve unauthorized acquisition,

disclosure, account takeover, identity manipulation, and other subsequent offenses, each requiring an appropriate legal qualification (Septiani et al., 2026). Scientifically, this distinction prevents the expansion of criminal law into a form of strict liability unless such liability is specifically and legitimately established by legislation.

The findings concerning corporate and electronic-system-provider responsibility reveal another important theoretical dimension. A personal-data breach frequently occurs within organizational systems, meaning that the person who directly commits the cyberattack may be different from the entity responsible for processing or safeguarding the data. This corresponds with Ismaidar and Ula (2025), whose study concludes that corporations may incur criminal liability in personal-data breaches when negligence or failure to fulfil legally required data-protection obligations can be established. It is also compatible with Saipudin et al. (2025), who explain that Indonesian criminal law increasingly recognizes the corporation as an independent subject of criminal law and develops criteria for determining when corporate conduct can generate criminal responsibility. From the perspective of corporate criminal liability theory, this finding is significant because contemporary cybercrime challenges the traditional model that associates criminal responsibility primarily with an identifiable natural person.

The role of vicarious and organizational liability theories becomes particularly relevant when cybercrime is committed by employees, agents, or contractors who operate within an organizational structure. Mandala and Firmansyah (2025), using vicarious-liability theory to examine misuse of personal data by online-loan debt collectors, demonstrate that corporate responsibility can become legally relevant where individual misconduct is connected to the corporation's business activity and organizational control. This interpretation also corresponds with the 2025 literature on corporate criminal liability, which emphasizes the need to formulate clearer attribution criteria for corporations under Indonesia's evolving criminal-law framework (Ahmad, 2025). The theoretical implication is therefore that corporate criminal responsibility in cybercrime should be constructed through organizational attribution rather than simple substitution of corporate liability for individual liability.

This finding is strongly supported by Manurung and Harefa (2024), who identify continuing difficulties in the practical use of electronic evidence within Indonesian criminal proceedings and emphasize the need to reconcile evidentiary requirements with privacy protection under the PDP Law. Even more recent research by Samudra et al. (2026) argues that Indonesia's electronic-evidence framework remains fragmented and insufficiently adapted to the characteristics of digital investigations.

This explains why the research findings identify a gap between substantive criminalization and practical enforceability. The theoretical implication is that criminal responsibility in cyberspace requires an evidentiary model capable of establishing authenticity, integrity, attribution, and causal relevance without weakening procedural safeguards or the privacy rights of persons whose data become part of the investigation.

The findings concerning doxing and unlawful disclosure further demonstrate why the PDP Law should be interpreted within a broader conceptual framework of privacy, autonomy, and harm prevention. Doxing illustrates a situation in which personal information may initially have been lawfully accessible but becomes unlawful when collected, combined, disclosed, or used in a context that violates the rights of the data subject. Recent studies consistently identify this regulatory difficulty. Fikriansyah and Harris (2026) argue that although the PDP Law can provide a basis for prosecuting doxing, enforcement is constrained by difficulties in perpetrator identification, digital evidence, and the absence of cybercrime-specific procedural mechanisms. Similarly, Salsabila et al. (2025) conclude that the PDP Law can be applied to doxing even though Indonesian legislation does not expressly formulate doxing as a distinct offense. Ahmad et al. (2026), meanwhile, identify the fragmented nature of the applicable provisions as a continuing source of uncertainty concerning the elements of the offense, proof, and sanctions. The theoretical consequence is that technology-neutral criminal-law interpretation becomes essential: the legal focus should remain on unauthorized acquisition, disclosure, use, or other prohibited conduct and the legally relevant harm, rather than treating every new technological practice as requiring a completely separate offense.

Finally, the combined findings indicate that the principal challenge in Indonesian personal-data criminal law lies in the translation of normative protection into legally attributable and procedurally enforceable responsibility. This explains why the existence of the PDP Law has not eliminated uncertainty concerning cybercrime enforcement. Sihotang and Ginting (2026) similarly identify a continuing effectiveness problem despite the existence of Law No. 27 of 2022, while Risal et al. (2026) emphasize the continuing tension between Indonesia's regulatory framework and the realities of cybercrime, including major data-breach incidents and weaknesses in cybersecurity governance. The scientific implication is a shift from a purely sanction-oriented understanding of personal-data protection toward an integrated criminal-law model combining substantive offense construction, culpability, corporate attribution, digital evidence, and victim protection. Such an approach also explains why strengthening criminal sanctions alone is insufficient: without precise attribution mechanisms and technologically appropriate evidentiary procedures, expanded criminalization may

increase the formal scope of liability without producing equivalent improvements in enforceability or legal certainty.

CONCLUSION

The study concludes that criminal liability for cybercrime involving personal data in Indonesia has acquired a stronger normative foundation through Law No. 27 of 2022 on Personal Data Protection and its interaction with the broader cybercrime framework. Nevertheless, criminal responsibility cannot be established solely from the occurrence of a data breach; it requires precise attribution of the prohibited act, legally relevant culpability, reliable electronic evidence, and differentiation between individual perpetrators and corporate or electronic-system-provider responsibility. The principal scientific contribution of this study is therefore the formulation of an integrated perspective that connects criminal liability, cybercrime, electronic evidence, and personal-data protection, demonstrating that effective legal protection depends not only on substantive criminalization but also on coherent attribution and enforceable procedural mechanisms. The main limitation is that the study relies predominantly on normative legal analysis and documented cases, without empirical investigation involving investigators, prosecutors, judges, data controllers, or victims, thereby limiting its ability to assess the practical effectiveness of enforcement in different institutional contexts.

Future research should complement normative analysis with empirical socio-legal research, particularly through interviews and analysis of court decisions involving personal-data-related cybercrime, to examine how culpability, corporate responsibility, and electronic evidence are actually interpreted and applied in practice. Comparative research involving other jurisdictions could subsequently be conducted to identify procedural and institutional mechanisms that may strengthen Indonesia's criminal enforcement framework while maintaining legality, proportionality, and protection of data-subject rights.

REFERENCES

- Antunes, P., & Guimarães, N. (2024). Guiding the implementation of data privacy with microservices. *International Journal of Information Security*, 23, 3591–3608. DOI: <https://doi.org/10.1007/s10207-024-00907-y>
- Arbelaez, A., & Climent, L. (2025). Iterative local search for preserving data privacy. *Applied Intelligence*, 55, 189. DOI: <https://doi.org/10.1007/s10489-024-05909-w>
- Bäumer, F. S., Schultenkämper, S., Geierhos, M., et al. (2024). Mirroring privacy risks with digital twins: When pieces of personal data suddenly fit together. *SN*

- Computer Science*, 5, 1109. DOI: <https://doi.org/10.1007/s42979-024-03413-z>
- Beebejaun, A., & Mandarun, R. (2024). Corporate criminal liability and the identification principle: A critical and comparative analysis across Mauritius, US, UK and Canada. *Journal of Financial Crime*, 32(3), 572–583. DOI: <https://doi.org/10.1108/JFC-02-2024-0071>
- Bekkers, L., Leukfeldt, R., & Kleemans, E. (2026). Police investigations into financial-economic cybercriminal networks: The experiences and perceptions of Dutch law enforcement. *European Journal on Criminal Policy and Research*, 32, 305–324. DOI: <https://doi.org/10.1007/s10610-025-09615-2>
- Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, 10(1), tyae017. DOI: <https://doi.org/10.1093/cybsec/tyae017>
- Casino, F., Pina, C., & López-Aguilar, P. (2022). SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, 8(1), tyac014. DOI: <https://doi.org/10.1093/cybsec/tyac014>
- Chomanski, B., & Lauwaert, L. (2025). Digital privacy and the law: The challenge of regulatory capture. *AI & Society*, 40, 2777–2787. DOI: <https://doi.org/10.1007/s00146-024-02041-8>
- Cram, W. A., & D'Arcy, J. (2023). “What a waste of time”: An examination of cybersecurity legitimacy. *Information Systems Journal*, 33(6), 1396–1422. DOI: <https://doi.org/10.1111/isj.12460>
- Dizon, M. A. C. (2024). Socio-legal study of technology: A norms and values approach to hacking and encryption law and policy. *Computer Law & Security Review*, 52, 105958. DOI: <https://doi.org/10.1016/j.clsr.2024.105958>
- Dong, B., Chernov, S., & Akpınar, K. O. (2024). Legal aspects of corporate systems for preventing cybercrime among personnel. *Crime, Law and Social Change*, 81(1), 75–96. DOI: <https://doi.org/10.1007/s10611-023-10108-8>
- Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology*, 35, 3. DOI: <https://doi.org/10.1007/s13347-022-00497-4>
- Guo, Z. (2023). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Security Review*, 48, 105774. DOI: <https://doi.org/10.1016/j.clsr.2022.105774>
- Hellmann, F., André, E., Benouis, M., Buchner, B., et al. (2024). Anonymization of faces: Technical and legal perspectives. *Datenschutz und Datensicherheit – DuD*, 48, 364–367. DOI: <https://doi.org/10.1007/s11623-024-1938-6>

- Holzenberger, N., & Maxwell, W. (2025). A quantitative approach to the GDPR's anonymisation and “appropriate technical and organisational measures” tests. *Computer Law & Security Review*, 59, 106173. DOI: <https://doi.org/10.1016/j.clsr.2025.106173>
- Juliussen, B. A., Kozyri, E., Johansen, D., & Rui, J. P. (2023). The third country problem under the GDPR: Enhancing protection of data transfers with technology. *International Data Privacy Law*, 13(3), 225–243. DOI: <https://doi.org/10.1093/idpl/ipad013>
- Jurcys, P., Corrales Compagnucci, M., & Fenwick, M. (2022). The future of international data transfers: Managing legal risk with a “user-held” data model. *Computer Law & Security Review*, 46, 105691. DOI: <https://doi.org/10.1016/j.clsr.2022.105691>
- Kinikoglu, B. (2023). Implementing a new data protection law: Lessons from the Turkish experience. *International Data Privacy Law*, 13(1), 25–46. DOI: <https://doi.org/10.1093/idpl/ipad001>
- Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*, 362, 112133. DOI: <https://doi.org/10.1016/j.forsciint.2024.112133>
- Lam, W. M. W., & Seifert, J. (2023). Regulating data privacy and cybersecurity. *The Journal of Industrial Economics*, 71(1), 143–175. DOI: <https://doi.org/10.1111/joie.12316>
- Lazarus, S., Tickner, P., & McGuire, M. R. (2025). Cybercrime against senior citizens: Exploring ageism, ideal victimhood, and the pivotal role of socioeconomics. *Security Journal*, 38, 42. DOI: <https://doi.org/10.1057/s41284-025-00482-4>
- Leijten, E., & van der Hof, S. (2025). Dissecting the commercial profiling of children: A proposed taxonomy and assessment of the GDPR, UCPD, DSA and AI Act in light of the precautionary principle. *Computer Law & Security Review*, 57, 106143. DOI: <https://doi.org/10.1016/j.clsr.2025.106143>
- Li, W., Li, Z., Li, W., Zhang, Y., & Li, A. (2025). Mapping the empirical literature of the GDPR's (in-)effectiveness: A systematic review. *Computer Law & Security Review*, 57, 106129. DOI: <https://doi.org/10.1016/j.clsr.2025.106129>
- Luhina, N., & Paliukh, O. (2025). Peculiarities of proof in criminal proceedings related to cybercrime. *Social Development: Economic and Legal Issues*, 4. DOI: <https://doi.org/10.70651/3083-6018/2025.4.27>
- Luo, Q., & Zhao, Y. (2025). Butcher or be butchered: Understanding the unwitting recruitment by cybercrime groups in China. *Trends in Organized Crime*. DOI:

- <https://doi.org/10.1007/s12117-025-09568-2>
- Mahadew, B. (2024). The need for a robust legal framework on corporate criminal liability in Mauritius: Lessons from the French model. *Journal of Financial Crime*, 31(1), 88–100. DOI: <https://doi.org/10.1108/JFC-02-2023-0030>
- Markos, E., Peña, P., Labrecque, L. I., & Swani, K. (2023). Are data breaches the new norm? Exploring data breach trends, consumer sentiment, and responses to security invasions. *Journal of Consumer Affairs*, 57(3), 1089–1119. DOI: <https://doi.org/10.1111/joca.12554>
- Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of personal data in the context of e-commerce. *Journal of Cybersecurity and Privacy*, 4(3), 731–761. DOI: <https://doi.org/10.3390/jcp4030034>
- Pichlak, M., & Gaczol, K. (2023). Simple and advanced reflexivity in GDPR enforcement: Empirical evidence from DPA activity. *International Data Privacy Law*, 13(4), 267–283. DOI: <https://doi.org/10.1093/idpl/ipad018>
- Purtova, N., & Leenes, R. (2023). Code as personal data: Implications for data protection law and regulation of algorithms. *International Data Privacy Law*, 13(4), 245–266. DOI: <https://doi.org/10.1093/idpl/ipad019>
- Rughiniş, R., Rughiniş, C., Vulpe, S. N., & Rosner, D. (2021). From social netizens to data citizens: Variations of GDPR awareness in 28 European countries. *Computer Law & Security Review*, 42, 105585. DOI: <https://doi.org/10.1016/j.clsr.2021.105585>
- Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, 49, 105801. DOI: <https://doi.org/10.1016/j.clsr.2023.105801>
- Surakanti, S., Goundar, S., & Dwight, J. (2025). Countering anti-forensic tactics in cybercrime investigations: A systematic literature review. *International Journal of Information Security*, 24, 210. DOI: <https://doi.org/10.1007/s10207-025-01131-y>
- Teichmann, F. M. J., & Wittmann, C. (2023). When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. *Journal of Financial Crime*, 30(6), 1491–1498. DOI: <https://doi.org/10.1108/JFC-04-2022-0093>
- Velasco, C. (2022). Cybercrime and artificial intelligence: An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, 23, 109–126. DOI: <https://doi.org/10.1007/s12027-022-00702-z>