Cyber law analysis of E-KTP data leakage: A case approach of 102 million KTP data allegedly leaked from the Ministry of Social Affairs to a hacker forum

Richart Sahatatua[1], Yenrizka Gusmaria[2], I Ketut Astawa[3], Ade Maman Suherman[4], Try Setiady[5], Wahyu Donri Tinambunan[6]
Universitas Singaperbangsa Karawang, Indonesia[1-6]
manurungrichart@gmail.com[1], ygusmaria@gmail.com[2], ketut.astawa@fh.unsika.ac.id[3], Ade.maman@fh.unsika.ac.id[4], tri.setiady@fh.unsika.ac.id[5], wahyu.donri@fh.unsika.ac.id[6]

Article History
Received on 20 July 2024
1st revision on 25 July 2024
Accepted on 30 July 2024

Abstract:

Purpose: This study investigates the legal implications and cybersecurity vulnerabilities surrounding the leak of 102 million electronic identity (E-KTP) records allegedly originating from the Indonesian Ministry of Social Affairs. It highlights the urgency of improving data protection mechanisms in the era of digital governance.

Research methodology: The research adopts a qualitative document analysis method, collecting and examining data from laws, government regulations, academic literature, credible news sources, and case studies related to cybercrime and information security. An interdisciplinary approach is applied, integrating perspectives from law, information technology, and cybersecurity.

Results: The study reveals that the current regulatory framework is insufficient to fully address the growing risks of data breaches in public digital infrastructures. It identifies critical gaps in cybersecurity readiness, institutional accountability, and legal enforcement related to personal data protection.

Conclusions: Strengthening personal data protection in Indonesia requires a combination of stricter regulatory enforcement, increased public awareness, technological investment, and cross-sector collaboration. The legal system must adapt more proactively to emerging digital threats.

Limitations: This research is limited to secondary data sources and does not include interviews or empirical fieldwork, which may restrict the depth of analysis on institutional practices.

Contribution: This paper contributes to the development of cyber law discourse in Indonesia by offering legal and policy recommendations aimed at enhancing data privacy, institutional responsibility, and public trust in digital identity systems.

Keywords: *Data Protection, Cybersecurity, E-KTP, Legal Analysis, Information Security*

How to Cite: Sahatatua, R., Gusmaria, Y., Astawa, I. K., Suherman, A. M., Setiady, T., & Tinambunan, W. D. (2024). Cyber law analysis of E-KTP data leakage: A case approach of 102 million KTP data allegedly leaked from the Ministry of Social Affairs to a hacker forum. *Journal of Multidisciplinary Academic and Practice Studies,* 2(3), 151-161.

1. Introduction

The Identity Card (KTP) is a fundamental document that serves as legal proof of identity for every Indonesian citizen. It contains essential personal data, such as name, date of birth, address, and citizenship status. In Indonesia, the possession of a KTP is not only a civil obligation but also a legal requirement for accessing various public and private services, including voting, banking, education, health care, and employment. To regulate the management of population data, the government enacted Law No. 24 of 2013 on Population Administration, supported by its implementing regulation Permendagri No. 73 of 2022, which elaborates on the procedures for accurately recording and protecting identity in official documents. This regulation aims to ensure that every citizen is officially registered and their identity is well protected (Ukwuoma, Cirman, & Oye, 2022). These regulations aim to ensure that every individual is properly registered in the national database, thereby securing their legal status and access to civil rights.

Despite the existence of such regulations, the rise of digital technology has introduced significant challenges in protecting personal data. As government services increasingly transition to digital platforms, the risk of unauthorized access, manipulation, or theft of sensitive data becomes more prominent (Ahmad & Dyah Febria, 2025; Simanjuntak, 2024; Solikhah, 2025). The issue of data leakage is particularly alarming because it opens the door to various forms of cybercrime, including identity theft, online fraud, impersonation, and unauthorized surveillance. Once personal information is compromised, the consequences for the affected individuals can be long-term and difficult to remedy. The case of ID card data leaks, especially those involving large scales, such as the leak of 102 million ID card data from the Ministry of Social Affairs (Kemensos) of the Republic of Indonesia, raises serious concerns about the privacy and security of individual data (Oranefo & Egbunike, 2021). This incident drew widespread attention after reports emerged that the leaked data were being offered on an online hacker forum, indicating a major breach of the country’s cybersecurity defenses. The data allegedly include sensitive personal identifiers, such as full names, addresses, national identification numbers (NIK), and other demographic details. The scale of the breach not only threatens the privacy and security of affected citizens but also severely damages the public’s trust in the government's ability to manage and protect sensitive information (Preecha, 2025). Moreover, it raises questions regarding institutional accountability, the enforcement of data protection laws, and the adequacy of preventive measures within the state agencies.

Given the potential impact of such a breach, it is crucial to examine the legal implications and responsibilities of the government in safeguarding citizens' digital identities. Indonesia has enacted Law No. 27 of 2022 on Personal Data Protection (UU PDP), which establishes rights for individuals and obligations for data controllers and processors (Muryani and Wiraguna, 2025). However, challenges remain in its implementation, including unclear enforcement mechanisms, low public awareness, and weak inter-agency coordination (Darnela & Rusdiana; Hamonangan & Silalahi, 2025; Lihawa, 2025). A comprehensive cyber law analysis is needed to evaluate how existing legal frameworks apply in practice and whether they provide sufficient deterrence and remedies in the event of a data breach (Prasetyo, Handayani, & Sulistiyono, 2025).

Therefore, this study seeks to analyze the legal dimensions of the E-KTP data leak case by applying a multidisciplinary approach, integrating perspectives from law, information technology, and cybersecurity governance (Sitaresmi, Rahmah, Wijoyo, Anom, & Prayogo, 2025; Wicaksono, Widodo, & Adi, 2023). Through document analysis of laws, regulations, and related case studies, this research aims to identify legal gaps and institutional weaknesses and propose actionable recommendations for improving data protection policies in Indonesia. Ultimately, the goal is to contribute to strengthening the security of citizens' digital identities and enhancing public trust in government-managed information systems in the digital era. The leak was allegedly spread on a hacker forum, which shows that the information technology infrastructure used by government agencies is still vulnerable to cyberattacks. This case not only harms individuals whose personal data were leaked but also tarnishes the government's credibility in managing sensitive data (Ahmad & Dyah Febria, 2025).

In this context, it is important to understand the legal implications of the E-KTP data leak and the government's responsibility to protect citizens' data. A cyber law analysis of this data leak case is highly relevant for exploring how existing regulations are applied and what can be done to improve the data security system. This study aims to provide better insight into personal data protection and information security in Indonesia and provide recommendations to improve the protection of citizens' data in the future.

2. Literature review

The literature used in this research covers a wide range of sources relevant to understanding the context of cyber law, personal data protection, and public policy related to information security. This study combines national laws, international regulations, case studies, and a review of the development of cyber law and public policy in the government sector. The following are some of the key literatures that form the basis of this research:

2.1 Law No. 11/2008 on Electronic Information and Transactions (UU ITE)

The ITE Law provides a strong legal basis for the protection of electronic data in Indonesia. Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), as amended by Law No. 19 of 2016 provides an important legal foundation for the protection of electronic data in Indonesia. Article 26(1) of the ITE Law explicitly states that "the use of any information through electronic media that involves a person's personal data must be done with the consent of the data subject." This provision is particularly relevant in the context of electronic identity data such as the E-KTP, which contains sensitive information, including full name, national identification number (NIK), address, and other personal identifiers. In addition, the ITE Law outlines the obligations of electronic system providers, both public and private, to ensure that their systems are secure, reliable, and accountable (Afriyani, Indrayani, Indrawan, Wibisono, & Ngaliman, 2023). It regulates various aspects of the use of information technology and electronic transactions, including provisions for the protection of personal data. Personal data in this context include information contained in the E-KTP. Government Regulation No. 71/2019 on the Implementation of the EIT Law further stipulates the obligation of data owners and electronic system providers to protect the confidentiality, integrity, and availability of personal data (Djafar, 2019).

Furthermore, Government Regulation No. 71 of 2019 (GR 71/2019) on the Implementation of Electronic Systems and Transactions, which serves as the implementing regulation of the ITE Law, strengthens the obligation to protect the confidentiality, integrity, and availability of personal information. GR 71/2019 introduces principles similar to those found in the GDPR, such as the requirement for explicit consent from the data subject, limitations on data use for stated purposes only, and the obligation to apply technical and organizational measures to prevent unauthorized access, leakage, or data manipulation (Majumdar, Sarma, & Majumdar, 2020; Zairina, Wibisono, Ngaliman, Indrayani, & Satriawan, 2023). However, implementation remains challenging due to the lack of clear operational definitions for key terms such as "personal data controller," as well as the limited supervisory capacity to enforce administrative sanctions against negligent electronic system providers (Makarim, 2020; Yusliwidaka, Abqa, & Wardana, 2024).

2.2 International Regulations

This study also covers relevant international regulations, such as the General Data Protection Regulation (GDPR), which is the most comprehensive personal data protection framework established by the European Union. One of the core elements of the GDPR lies in the Principles of Data Processing outlined in Article 5. These principles state that personal data must be processed lawfully, fairly, and transparently in relation to the data subject; collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes (purpose limitation); the data collected must be adequate, relevant, and limited to what is necessary (data minimization); it must be accurate and, where necessary, kept up to date; storage must be limited to the period necessary for processing (storage limitation); and it must be processed securely to ensure its integrity and confidentiality (Adil, Sapar, & Jasman, 2023). The regulation also requires data controllers to demonstrate compliance with these principles (accountability) (Adelika & Nurbaiti, 2023; De Terwangne, 2020; Regulation, 2018).

In addition, the GDPR provides significant rights to individuals, including the right to access their personal data, the right to erasure (the "right to be forgotten"), and the right to restrict the processing of their data. The successful implementation of the GDPR in various jurisdictions demonstrates the crucial role of strict legal regulations and effective law enforcement in protecting personal data. For example, comparative studies between Indonesia's Personal Data Protection Law (Law No. 27 of 2022) and the GDPR have highlighted areas where Indonesian regulations still need improvement, such as the need for an independent supervisory authority, increased public awareness regarding individual data rights, and detailed technical guidelines for implementing regulations to match international standards (Achmad Fitrian et al., 2025; Firaldi, Wibisono, Ngaliman, Indrayani, & Satriawan, 2023; Simanjuntak, 2024).

2.3 Case Studies and Overview of Cyber Law Developments

This study examines various data breach case studies from several countries to understand the implementation of cyber law and the challenges faced in enforcing laws against cybercrime. It provides a comprehensive overview of how different jurisdictions handle data breach incidents and the extent to which existing legal systems can respond to rapidly evolving digital crimes (Khudori & Lala, 2024; Lallie, Thompson, Titis, & Stephens, 2025; Nahai, 2019). By analyzing real-world cases, this study identifies legal loopholes, best practices, and obstacles to the effective enforcement of cyber laws. Data breach cases in the United States, the European Union, and several Asian countries offer diverse perspectives on the legal approaches used to address data breaches and efforts to protect personal data. Each region has its own policies, regulations, and enforcement mechanisms that reflect differences in legal culture and the level of institutional preparedness to face cyber threats. By comparing these approaches, this study aims to identify patterns that can serve as references for formulating more effective global data protection policies.

One notable case study is the data breach experienced by Target Corporation in the United States, which highlighted the importance of implementing proactive cybersecurity measures and responding quickly to data breach incidents (Yudistira & Ramadani, 2023; Zairina et al., 2023). In the European Union, the British Airways data leak case underlined the severe legal consequences and significant fines for companies that fail to protect their personal data. Both cases emphasize that, beyond technical aspects, legal and regulatory frameworks play a critical role in shaping a resilient cybersecurity ecosystem.

2.4 Public Policy on Cyber Security in the Public Sector

This research includes an extensive review of the literature concerning public policy on cyber security within the public sector, focusing particularly on how government agencies manage, secure, and protect the vast and sensitive data they are entrusted with. The study emphasizes that effective cybersecurity governance in the public sector is not limited to technological solutions alone, but requires a comprehensive and strategic policy framework (Magnusson, Iqbal, Elm, & Dalipi, 2025; Mishra, Alzoubi, Anwar, & Gill, 2022). Various national and international policies were analyzed to understand the approaches taken by governments to mitigate cyber risks, particularly those affecting critical public infrastructure and citizen data. For instance, the cybersecurity policies implemented by the Singaporean government serve as a benchmark for the best practices in the region (Latunusa, Timuneno, & Fanggidae, 2023). Their approach, which combines robust regulatory mechanisms, regular employee training programs, public sector awareness campaigns, and consistent investment in advanced information security technologies, has proven effective in reducing vulnerabilities and enhancing institutional readiness (Mokhtar, 2024; Riyadi Suriaatmadja, 2023). This study also highlights the importance of co-operation between the public and private sectors in creating a strong cyber security environment (Putra, Ahadiyat, & Keumalahayati, 2023).

Furthermore, this study highlights that the protection of government-held data requires not only internal capacity but also an integrated governance model that aligns policy, organizational behavior, and technological infrastructure. A critical aspect of this is the development of cyber security policies that are not static but responsive to evolving threats, requiring regular policy reviews and updates (Bada, Sasse, & Nurse, 2019). For example, in the United Kingdom, the National Cyber Security Strategy mandates continuous risk assessment and the establishment of baseline security standards across government departments (UK 2022). In many jurisdictions, cyber security is now embedded within broader national security strategies, recognizing the increasing interdependence between digital infrastructure and public trust in government services (Rahu, Neolaka, & Djaha, 2023).

Another key theme identified in the literature is the need for collaborative frameworks between the public and private sectors to build a secure cyber environment (Tiimub et al., 2023). Governments increasingly rely on private vendors for digital service provision and infrastructure development, which introduces additional layers of risk if they are not governed appropriately. Therefore, public-private partnerships are essential for establishing shared standards, improving incident response coordination, and fostering innovation in cyber-resilience strategies (Carr, 2016; Laidlaw, 2021). The study underscores that without strong cooperation across sectors and continuous policy innovation, government agencies remain vulnerable to large-scale data breaches that can compromise national security, economic stability and citizen privacy.

2.5 Additional Regulations and Related Literature

In addition to the primary sources mentioned above, this study also reviewed additional relevant regulations and literature, such as:

1. Law No. 27 of 2022 on Personal Data Protection. This law provides more specific protection for personal data in Indonesia, establishing the rights and obligations of data owners and electronic system providers, as well as sanctions for data protection violations (Djafar, 2019). Cyber Law Books and Journals: Works such as "Criminal Offences of Information & Electronic Transactions" by Chazawi and Ferdian provide in-depth insights into the legal aspects of cybercrime in Indonesia (Ferdian & Chazawi, 2015).
2. Journal Articles and Case Study Reports Articles such as "Twitter Sentiment Analysis of Personal Data Protection with Machine Learning Approach" by Nursiyono and Huda, and "Legal Protection of PT PLN's Consumer Personal Data Leak" by Riyadi and Suriaatmadja add depth to analyses on personal data protection and information security (Nursiyono & Huda, 2023).

In addition to the primary sources previously discussed, this study incorporates a comprehensive review of supplementary regulations and scholarly literature directly relevant to personal data protection and cyber law enforcement in Indonesia. Among the key regulatory frameworks examined is Law No. 27 of 2022 on Personal Data Protection, which represents a significant advancement in the country's legal infrastructure regarding data privacy. This law clearly outlines the rights of personal data owners, including the right to access, correct, and delete personal information, and sets forth strict obligations for electronic system providers to ensure the confidentiality, integrity, and availability of the data they manage. Moreover, it includes administrative and criminal sanctions for violations, emphasizing accountability and regulatory compliance (Djafar, 2019; Endi, Fanggidae, & Ndoen, 2023). This legal foundation plays a critical role in shaping data governance standards in both the public and private sectors.

In addition to statutory regulations, this study engages with foundational legal literature in the field of cyber law, such as the widely cited book "Criminal Offences of Information & Electronic Transactions" by Chazawi and Ferdian. This study offers a deep and nuanced interpretation of Indonesia's Law on Information and Electronic Transactions (UU ITE), particularly in relation to cybercrime, digital evidence, and procedural law in the context of cyber offenses (Ferdian & Chazawi, 2015). These texts are essential for understanding the doctrinal framework underpinning the country's approach to prosecuting cyber-related offenses, and they help contextualize the practical challenges in enforcing digital laws amid rapid technological change.

Furthermore, this study draws on recent academic journal articles and case-based reports to enrich the analysis with empirical and technical perspectives. For example, the article "Twitter Sentiment Analysis of Personal Data Protection with Machine Learning Approach" by Nursiyono and Huda employs artificial intelligence methods to explore public opinion and sentiment surrounding data protection, revealing patterns in societal awareness and trust levels regarding data security (Nursiyono & Huda, 2023). Another relevant study, "Legal Protection of PT PLN's Consumer Personal Data Leak" by Riyadi and Suriaatmadja (2023), provides a case-specific exploration of how corporate-level data breaches are handled under Indonesian law and the implications for consumer protection and regulatory reform.

By integrating sources from the legal, technical, and socio-political disciplines, this research aims to develop a holistic understanding of the multifaceted legal challenges involved in managing the E-KTP data leak incident. Additionally, it seeks to generate practical insights and recommendations for the development of more robust public policies and law enforcement strategies aimed at securing personal data from ongoing and emerging cyber threats (Ibrahim, Hasan, & Ishak, 2025). By combining various literature sources from various disciplines, this research aims to provide a holistic understanding of the cyberlegal challenges faced in handling the E-KTP data leak. In addition, this study seeks to provide useful insights for the development of policies and law enforcement strategies that are more effective in protecting people's personal data from cyber threats.

3. Research Methodology

This research employs a qualitative document analysis method as the main approach to systematically gather, review, and interpret relevant data from a wide range of primary and secondary sources. The primary sources consist of authoritative documents, such as official laws and regulations specifically related to data security, government-issued policies on cybersecurity, and legal rulings or court decisions that address various cybercrime cases. These primary materials serve as the foundational legal framework that guides the understanding of how data protection is enforced and regulated in the EU. Meanwhile, the secondary sources include comprehensive news reports that cover recent and past incidents, scholarly academic articles that provide theoretical and empirical insights, and detailed case studies that offer in-depth examinations of particular data breach events.

The focus is placed on the E-KTP data leak case, which is used as a central example to explore the practical implications of these legal and regulatory measures. By collecting and analyzing this diverse array of documents, this study aims to build a thorough and multidimensional understanding of the complexities involved in data breaches, encompassing legal, technical, and societal perspectives.

Additionally, this study adopts an interdisciplinary approach by integrating literature from various fields, such as law, information technology, and cybersecurity. This integration enables a holistic exploration of the legal challenges and technical complexities involved in addressing data breaches. The combination of legal frameworks and technological insights helps identify gaps in existing laws and evaluate their effectiveness in mitigating cybercrime risks. This approach also supports a nuanced analysis of how regulatory, technical, and operational factors interact in real-world cyber incidents. Throughout the research process, the data were coded and categorized to identify recurring themes and patterns related to the enforcement of cyber laws, the effectiveness of data protection mechanisms, and institutional responses to data leakage. This methodological framework not only strengthens the validity of the findings but also provides a robust basis for recommending policy improvements in cyber security governance (Yudistira & Ramadani, 2023).

4. Results and discussions

4.1 Legal Protection of Personal Data in the Context of E-KTP Data Leakage

Legal protection of personal data is crucial in this digital era, especially in the case of the leak of 102 million ID card data from the Ministry of Social Affairs in Indonesia. Law No. 11/2008 on Electronic Information and Transactions (ITE Law) provides a strong legal basis for protecting electronic data in Indonesia. However, its implementation still faces challenges, such as a lack of awareness and understanding among the public and government institutions. The leakage of E-KTP data can result in various negative consequences, including identity abuse, fraud, and other crimes that can harm individuals and society at large (Djafar, 2019).

To overcome this challenge, concrete steps are needed, such as raising awareness of the importance of data privacy, strengthening regulations, and strict law enforcement. Raising public awareness of the importance of personal data protection can be achieved through educational campaigns and training for the public and government employees. Strengthening regulations is also important to ensure that existing laws are comprehensive enough to address the various forms of cybercrime. Strict law enforcement against personal data protection violations will deter criminals and strengthen public confidence in the existing legal system (Putri, Syamsu, & Triono, 2024).

4.2 Cyber Law Implications for Government Agencies

The Ministry of Social Affairs and other government agencies have a legal obligation to protect sensitive data, such as the E-KTP. Data leaks can lead to serious legal consequences, including civil and criminal liability and public prosecution, which can undermine public trust in the credibility and integrity of government agencies. In this context, it is important for government agencies to update their information security policies and systems to deal with increasingly complex cyber security threats (Riyadi & Suriaatmadja, 2023).

Government agencies can take include the use data encryption to protect sensitive information, restrict access to personal data to authorized parties, and implement up-to-date security systems to prevent unauthorized access. In addition, government agencies must adopt a comprehensive information security policy and ensure that all employees understand and comply with it. Training and awareness-raising among government employees are also important to ensure that they can identify and effectively deal with cyber security threats (Fakir & Miah, 2021).

4.3 Law Enforcement Mechanism against Cyber Criminals

Law enforcement against cybercriminals involved in the E-KTP data leak requires a thorough investigation, evidence collection, and a fair trial. Challenges in law enforcement include the limitations of existing laws, the complexity of digital footprints, and cross-border cooperation. Cybercriminals often use techniques and tools to hide their digital footprints, complicating the investigation and prosecution processes (Yudistira & Ramadani, 2023).

To improve the effectiveness of law enforcement against cybercrime, a stronger legal framework and better capacity of law enforcement agencies are required. Updating regulations to accommodate technological developments and emerging cybercrime tactics is essential. In addition, increased international cooperation between law enforcement agencies from different countries is needed to tackle cross-border cybercrimes. Investments in digital forensic technology and training for law enforcement officers can help improve their ability to identify, track, and prosecute cyber criminals.

5. Conclusion

5.1 Conclusion

The leak of 102 million ID card data from the Ministry of Social Affairs highlights the significant complexity and multifaceted challenges involved in managing data security threats in today’s increasingly digital world. This massive breach not only exposes vulnerabilities in the protection of sensitive personal information but also reflects the evolving tactics used by cybercriminals to exploit system weaknesses. This incident serves as a stark reminder that data security cannot be treated lightly, especially when it involves the personal information of millions of citizens, underscoring the critical need for robust protective measures and continuous vigilance.

To address these challenges, the legal protection of personal data requires more effective implementation and greater awareness, both within government agencies and among the general public. Although laws and regulations may exist to safeguard data, their success heavily relies on how well they are enforced and understood by stakeholders. Government institutions, in particular, must prioritize developing and maintaining strong policies that align with rapid technological advancements and invest in up-to-date information security systems to effectively manage and protect sensitive data. Without such proactive efforts, the risk of future breaches remains high, with potentially severe consequences for individuals and for national security.

Furthermore, law enforcement mechanisms must be substantially strengthened to act as effective deterrents against cybercrime and prevent the recurrence of similar data leaks. This requires not only enhanced technical capabilities but also improved coordination among various agencies and the establishment of clear protocols for responding to cyber incidents. Importantly, addressing data security issues in the digital era requires the joint efforts of multiple stakeholders, including government bodies, private sector organizations, and civil society. By working collaboratively, these parties can ensure that personal data protection and information security remain central priorities, thereby building resilience against dynamic and persistent threats in the evolving digital landscape.

5.2. suggestion

Based on the findings of this study regarding the data breach of 102 million ID card records originating from the Ministry of Social Affairs, several strategic recommendations are proposed. These may serve as references for the government and other relevant stakeholders to strengthen personal data protection and information security systems in the digital era.

First, the government, particularly institutions that manage population data, must improve the effectiveness of implementing personal data-protection regulations. Existing legal frameworks should be translated into operational policies that can be implemented at the institutional level. Furthermore, the capacity of human resources should be enhanced through regular training programs on data protection and cybersecurity, ensuring that all parties involved understand their responsibilities in safeguarding confidential information.

Second, the information technology infrastructure within public institutions must be strengthened by adopting appropriate information security standards such as ISO/IEC 27001. Security audits should be conducted regularly, accompanied by the implementation of early detection technologies for cyberattacks. The procurement and maintenance of information security systems must also be prioritized in the budgeting plans of public institutions that process large-scale personal data.

Third, law enforcement mechanisms related to cybercrime must be reinforced in terms of regulations, institutional capacity, and inter-agency coordination. The government should establish clear incident response protocols and promote integrated cooperation among law enforcement, data protection authorities, and private sector entities. In addition, national digital literacy campaigns are needed to raise public awareness of the importance of personal data protection and individual preventive measures. This cross-sectoral collaboration is essential for building a resilient, adaptive, and responsive digital security ecosystem against evolving cyber threats.

References

Achmad Fitrian, S., Akhyar, C. F., SH, M., Mardia Ibrahim, S., Tora Yuliana, S., Resti Riancana, S., . . . MM, M. (2025). *Hukum Perdata Dan Hak Asasi Manusia: Menjamin Keadilan Individu*: PT. Nawala Gama Education.

Adelika, A., & Nurbaiti, N. (2023). Upaya Pencegahan Terjadinya Pencurian Data Pada E-Ktp Bagi Penduduk Pada Dinas Kependudukan Dan Pencatatan Sipil Kota Medan. *Jurnal Pengabdian Masyarakat Khatulistiwa, 6*(2), 124-133.

Adil, A., Sapar, S., & Jasman, J. (2023). The effect of job appraisal and job training on employee performance at PT. Bank Sulselbar Luwu. *Journal of Multidisciplinary Academic Business Studies, 1*(1), 71-82. doi:https://doi.org/10.35912/jomabs.v1i1.1816

Afriyani, N., Indrayani, I., Indrawan, M. G., Wibisono, C., & Ngaliman, N. (2023). The influence of training, discipline, and innovation on the performance of members of the Regional National Crafts Council (Dekranasda) in Tanjungpinang City: A quantitative study. *Journal of Multidisciplinary Academic Business Studies, 1*(1), 53-69. doi:https://doi.org/10.35912/jomabs.v1i1.1780

Ahmad, F., & Dyah Febria, W. (2025). PROTECTING PRIVACY IN THE DIGITAL ERA: PERSONAL DATA SECURITY IN INDONESIA. *Inovasi Pembangunan : Jurnal Kelitbangan, 13*(1). doi:https://doi.org/10.35450/jip.v13i1.915

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43-62. doi:https://doi.org/10.1111/1468-2346.12504

Darnela, L., & Rusdiana, E. Public Legal Awareness and the Effectiveness of Indonesia's Personal Data Protection Law: Bridging Normative Framework and Privacy Paradox. *Supremasi Hukum: Jurnal Kajian Ilmu Hukum, 14*(1). doi:https://doi.org/10.14421/2gg2rp29

De Terwangne, C. (2020). Principles relating to processing of personal data *The EU general data protection (GDPR): a commentary* (pp. 309-320): Oxford University Press.

Djafar, W. (2019). *Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan.* Paper presented at the Seminar Hukum dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM.

Endi, A. C., Fanggidae, R. E., & Ndoen, W. M. (2023). The effect of religiosity and spirituality on financial behavior district. *Journal of Multidisciplinary Academic and Practice Studies, 1*(1), 45-53. doi:https://doi.org/10.35912/jomaps.v1i1.1455

Fakir, M. K. J., & Miah, M. R. (2021). Factors Influencing E-WOMs in Restaurant Business: Evidence from Bangladesh. *Journal of Sustainable Tourism and Entrepreneurship, 3*(1), 17-36.

Ferdian, A., & Chazawi, A. (2015). Tindak Pidana Informasi & Transaksi Elektronik. *Malang: Media Nusa Creative*.

Firaldi, Y., Wibisono, C., Ngaliman, N., Indrayani, I., & Satriawan, B. (2023). The influence of leadership, discipline, and workload on employee performance through job satisfaction as an intervening variable in Regional Revenue Agency Riau Islands Province. *Journal of Multidisciplinary Academic Business Studies, 1*(1), 27-52. doi:https://doi.org/10.35912/jomabs.v1i1.1779

Hamonangan, M. K., & Silalahi, W. (2025). Igniting the Spirit of the Personal Data Protection Law: Advancing Justice, Ethics, and Institutional Reform in Indonesia's Digital Legal Politics. *Journal of Business, Management, and Social Studies, 5*(3), 107-115. doi:https://doi.org/10.53748/jbms.v5i3.130

Ibrahim, V., Hasan, Y., & Ishak, P. (2025). Personal Data Protection Policies and Their Impact on Victims of Cybercrime. *Jurnal Ilmu Hukum Kyadiren, 6*(2), 13-25. doi:https://doi.org/10.46924/jihk.v6i2.225

Khudori, A., & Lala, A. (2024). Legal Implications of Data Breach Cases in Indonesia: Challenges and Solutions in the Era of Personal Data Protection. *Indonesian Cyber Law Review, 1*(1), 13-20. doi:https://doi.org/10.59261/iclr.v1i2.1

Laidlaw, E. (2021). Privacy and cybersecurity in digital trade: The challenge of cross border data flows. *Available at SSRN 3790936*. doi:https://dx.doi.org/10.2139/ssrn.3790936

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers, 14*(2), 49. doi:https://doi.org/10.3390/computers14020049

Latunusa, P. M., Timuneno, T., & Fanggidae, R. E. (2023). The effect of multiple role conflict and work stress on the performance of women nurses during the covid-19 with coping stress as intervening variables (Study at SoE Regional General Hospital). *Journal of Multidisciplinary Academic and Practice Studies, 1*(1), 29-43. doi:https://doi.org/10.35912/jomaps.v1i1.1462

Lihawa, R. (2025). Digital Privacy Crisis: Legal Protection of Social Media Users' Data in Indonesia's 2022 Law. *Estudiante Law Journal, 7*(1), 280-296. doi:https://doi.org/10.33756/eslaj.v7i1.30980

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends. *International Journal of Information Security, 24*(4), 177. doi:https://doi.org/10.1007/s10207-025-01097-x

Majumdar, S. K., Sarma, A. P., & Majumdar, S. (2020). E-commerce and digital connectivity: unleashing the potential for greater India–ASEAN integration. *Journal of Asian Economic Integration, 2*(1), 62-81. doi:https://doi.org/10.1177/2631684620910524

Makarim, E. (2020). Privacy and personal data protection in indonesia: the hybrid paradigm of the subjective and objective approach *Data Protection Around the World: Privacy Laws in Action* (pp. 127-164): Springer.

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security, 120*, 102820. doi:https://doi.org/10.1016/j.cose.2022.102820

Muryani, V. D., & Wiraguna, S. A. (2025). Efektivitas Undang-Undang Perlindungan Data Pribadi Dalam Menjawab Tantangan Keamanan Siber Di Indonesia. *Causa: Jurnal Hukum dan Kewarganegaraan*, 81-90. doi:https://doi.org/10.3783/causa.v12i3.12780

Nahai, F. (2019). General Data Protection Regulation (GDPR) and data breaches: What you should know (Vol. 39, pp. 238-240): Oxford University Press US.

Nursiyono, J. A., & Huda, Q. (2023). Analisis Sentimen Twitter Terhadap Perlindungan Data Pribadi Dengan Pendekatan Machine Learning. *Jurnal Pertahanan dan Bela Negara, 13*(1), 1-16.

Oranefo, P. C., & Egbunike, C. F. (2021). An exploration of the viability of forensic accounting techniques in combating financial statement fraud in Nigerian organizations. *Annals of Management and Organization Research, 3*(1), 69-81.

Perdana, A., & Mokhtar, I. A. (2024). Digital transformation in government: Lessons from GovTech Singapore. *Journal of Information Technology Teaching Cases*, 20438869251362871. doi:https://doi.org/10.1177/20438869251362871

Prasetyo, B., Handayani, I. G. A. K. R., & Sulistiyono, A. (2025). Data Protection Laws in Indonesia: Navigating Privacy in the Digital Age. *Side: Scientific Development Journal, 2*(1), 9-16. doi:https://doi.org/10.59613/petfxv64

Preecha, J. (2025). *Cybersecurity and Public Trust in Digital Governance: Focusing on Citizen Trust.* Paper presented at the Proceeding of International Conference on Social Science and Humanity.

Putra, M. F., Ahadiyat, A., & Keumalahayati, K. (2023). The influence of leadership style on performance with motivation as mediation (study on employees of Metro City Trade Services during pandemi). *Journal of Multidisciplinary Academic and Practice Studies, 1*(1), 15-27. doi:https://doi.org/10.35912/jomaps.v1i1.1536

Putri, A. M., Syamsu, S., & Triono, A. (2024). Policy to replace electronic card into population digital in South Lampung Regency. *Journal of Governance and Accountability Studies, 4*(1), 19-29.

Rahu, K. Y. d., Neolaka, M. N. B. C., & Djaha, A. S. A. (2023). Personnel management information system in order to create up-to-date and integrated personel data and information in the personnel and human resources agency in malaka regency. *Journal of Multidisciplinary Academic and Practice Studies, 1*(1), 55-70. doi:https://doi.org/10.35912/jomaps.v1i1.1449

Regulation, G. D. P. (2018). Principles relating to processing of personal data.

Riyadi, G. A., & Suriaatmadja, T. T. (2023). *Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.* Paper presented at the Bandung Conference Series: Law Studies.

Simanjuntak, P. H. (2024). Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR). *Jurnal Esensi Hukum, 6*(2), 105-124. doi:https://doi.org/10.35586/jsh.v6i2.412

Sitaresmi, A., Rahmah, M., Wijoyo, S., Anom, A. P., & Prayogo, F. M. (2025). Legal Frameworks for Cybersecurity and Data Protection in Cloud-Based Notarial Systems in Indonesia: An Intersectional Analysis of Positive Law and Islamic Legal Principles. *Al-'Adalah, 22*(1). doi:https://doi.org/10.24042/adalah.v22i1.26813

Solikhah, M. a. (2025). Personal Data Protection in the Era of Digital Transformation: Challenges and Solutions in the Indonesian Cyber Law Framework. *Indonesian Cyber Law Review, 2*(1), 39-50. doi:https://doi.org/10.59261/iclr.v2i1.15

Tiimub, B. M., Christophé, N., Atepre, B. A., Tiimob, R. W., Tiimob, G. L., Tiimob, E. N., . . . Agyenta, J. J. (2023). Crop production potential of reclaimed mine sites for sustainable livelihoods. *Journal of Multidisciplinary Academic and Practice Studies, 1*(1), 1-13. doi:https://doi.org/10.35912/jomaps.v1i1.1785

UK, G. (2022). National cyber strategy 2022.

Ukwuoma, H. C., Cirman, N. E., & Oye, P. O. (2022). The role of e-Government in overcoming the consequences of the COVID-19 pandemic in Nigeria. *Journal of Governance and Accountability Studies, 2*(1), 79-92.

Wicaksono, J. A., Widodo, A. P., & Adi, K. (2023). Systematic Literature Review on Information Technology Governance in Government. *Telematika: Jurnal Informatika dan Teknologi Informasi, 20*(2), 226-237. doi:https://doi.org/10.31315/telematika.v20i2.9642

Yudistira, M., & Ramadani, R. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO. *UNES Law Review, 5*(4), 3917-3929.

Yusliwidaka, A., Abqa, M. A. R., & Wardana, K. A. (2024). A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law? *Pandecta Research Law Journal, 19*(2), 173-202.

Zairina, S., Wibisono, C., Ngaliman, N., Indrayani, I., & Satriawan, B. (2023). The influence of product quality, prices, and promotions on buyer decisions in the small and medium industry handicrafts of Tanjungpinang City. *Journal of Multidisciplinary Academic Business Studies, 1*(1), 13-25. doi:https://doi.org/10.35912/jomabs.v1i1.1778