Ilomata International Journal of Social Science
P-ISSN: 2714-898X; E-ISSN: 2714-8998
Volume 5, Issue 3, July 2024
Page No. 818-830

Data Security and Individual Privacy from the Perspective of Public Administration

Jayanti Armida Sari[1], Isnaeni Yuliani[2], Tora Akadira[3], Amud Sunarya[4], Rashid Ating[5]
[1234]Universitas Terbuka, Indonesia
[5]Universiti Malaya (UM), Malaysia
Correspondent: jayanti@ecampus.ut.ac.id[1]

Received : May 28, 2024
Accepted : July 18, 2024
Published : July 31, 2024

Citation: Sari, J, A., Yuliani, I., Akadira, T., Sunarya, A., Ating, R. (2024). Data Security and Individual Privacy from the Perspective of Public Administration. Ilomata International Journal of Social Science, 5(3), 818-830.
https://doi.org/10.61194/ijss.v5i3.1297

ABSTRACT: The widespread use of Information and Communication Technology (ICT) has transformed social, economic, and everyday interactions, creating challenges in data security and individual privacy. This study explores aspects of data security and privacy within public administration in Indonesia, highlighting existing challenges, policies, and initiatives. The research methodology is a qualitative literature review encompassing journal articles, books, and research reports on data security and privacy. The findings indicate that cyber threats such as hacking, phishing, ransomware, and data breaches have led to financial losses, reputational damage, and privacy violations in Indonesia. The discussion of this research suggests that data security strategies, including security policies, encryption technology, firewalls, access controls, and risk management, are crucial for protecting sensitive information. Legislative measures, public awareness, and technological protection are necessary to balance technological benefits and the safety of individual rights, ensuring compliance with regulatory standards and enhancing public trust in government and organizations.

Keywords: Data Security, Hacking, Individual Privacy, Ransomware, Technological Protection.

INTRODUCTION

The extensive use of Information and Communication Technology (ICT) platforms has significantly shaped and regulated cyberspace, which has become an integral part of human existence. This phenomenon is evident in how social interactions, economic activities, and daily life are increasingly connected with digital technology. Although this cyberspace does not replace the reality of daily routines, it complements and becomes an inseparable part of that reality. This means humans live in two complementary dimensions: the natural and virtual worlds (Levin & Mamlok, 2021).

The information revolution has had a profound impact by enabling accessible communication with others and access to various forms of information and knowledge without geographical or time constraints. This digital transformation is further realized in the context of smart homes, which help create innovative life services and add user value (Mao & Chang, 2023). Every individual can now interact and access information from around the world in previously unimaginable ways. This capacity enhances efficiency and productivity and transforms how people understand and interact with the world around them.

These changes have wide-ranging and profound implications for society's social aspects. Human interactions have experienced significant transformations in this social domain, becoming more dynamic and complex. Online social networks have become the primary platforms for communication and social relationships, replacing or complementing traditional forms of interaction (Alalawneh et al., 2022). Platforms such as Facebook, Twitter, Instagram, LinkedIn, TikTok, and WhatsApp provide means for sharing information and communication and reshape the structure and dynamics of social relationships.

In the economic sphere, the development of digital technology has enabled transactions and business operations to be conducted online with high efficiency (Bangsawan, 2023). It reduces the need for physical presence and significantly expands the global market. With the advent of e-commerce platforms (Sudaryono et al., 2020), digital financial services (Sastiono & Nuryakin, 2019), and internet-based business applications (Indrajaya et al., 2022) companies can operate at lower costs and with broader reach. Consumers can easily purchase products and services worldwide, while companies can access international markets that were previously difficult to reach.

Furthermore, the information revolution has enabled broader and more inclusive access to educational resources in the context of education and knowledge. Information and communication technology has opened up opportunities for distance learning and lifelong education, which are crucial in an era of rapidly evolving skills and knowledge (Putra & Pratama, 2023). E-learning platforms, massive open online courses (MOOCs), and digital education applications facilitate individuals from diverse backgrounds to access quality educational materials without geographical limitations (Oh et al., 2020). Thus, the information revolution not only enhances accessibility and flexibility in education but also ensures that learning can continue throughout life, enabling individuals to update and develop their skills according to contemporary needs continuously.

The advancement of digital technology has brought significant benefits, such as increased operational efficiency, more accessible access to public information, and more responsive services, as previously explained. However, these advancements also elevate the risks to data security and privacy. Cyberattacks, data breaches, and misuse of personal information are real threats that can erode public trust in government institutions. Misusing personal data constitutes criminal acts, such as theft, fraud, and other crimes, both from objective and subjective perspectives (Situmeang, 2021). Such incidents can result in substantial financial and reputational losses and disrupt effective government functioning.

Cyberattacks on government data continue to occur frequently. In 2004, a ransomware attack crippled the Temporary National Data Center, causing disruptions to the Public DNS (PDNS) managed by the Ministry of Communication and Information Technology (Kominfo). As a result, the digital services of the Directorate General of Immigration at the Ministry of Law and Human

Rights were rendered inoperative. Additionally, the New Student Admissions Services (PPDB) in various regions experienced disruptions, forcing local governments to extend registration periods. Other impacts included the paralysis of immigration services, including passport and visa applications. Overall, 282 government agency services were affected by this incident (BBC News Indonesia, 2024).

Furthermore, data from the Ministry of Communication and Information Technology (Kominfo) revealed 1,730 detected online fraud content from August 2018 to February 16, 2023. Financial losses from online fraud in Indonesia reached an astounding Rp 18.7 trillion from 2017 to 2021 (Katadata, 2023). Additionally, approximately 1.3 billion prepaid SIM card registration data were allegedly leaked and traded on the online forum. A data seller with the username Bjorka claimed that the leaked data originated from a server owned by the Ministry of Communication and Information Technology (Kompas, 2022). Furthermore, Kominfo is investigating the alleged leak of 34 million Indonesian passports, adding to concerns about data security and privacy in Indonesia (Menpan-RB, 2023). These findings highlight significant challenges in managing and protecting personal data in the digital era and the need for immediate action to strengthen national data security systems.

In Indonesia, efforts to address data security challenges have begun by introducing various regulations and initiatives, such as the Information and Electronic Transactions Law (UU ITE) and Law Number 27 of 2022 on Personal Data Protection. These regulations aim to provide a clear legal framework for protecting personal data and ensuring information security in public administration. However, the implementation and effectiveness of these regulations still need to overcome several obstacles, including a lack of understanding and awareness among civil servants regarding data security and technical challenges in implementing effective data security systems. Additionally, significant law enforcement measures to address vulnerabilities in government data systems still need to be evident.

The reviewed papers highlight various aspects of data security challenges in e-government initiatives. Djuric (2024) emphasizes the need for robust security protocols and secure communication channels to address public trust issues, underscoring the multifaceted obstacles in developing countries. Raza (2024) highlights the importance of national and international frameworks for cybersecurity and data privacy in e-governance, calling for the implementation of best practices. Lastly, Peeran, M., & Shanavas (2022) analyze the critical need for information security technology to ensure the smooth operation of e-governance projects.

This study aims to explore aspects of data security and individual privacy from the public administration perspective in Indonesia. By highlighting the challenges faced, existing policies, and ongoing initiatives, this research provides comprehensive insights into how public administration can enhance the protection of citizens' data. The implications of this paper are to provide a strong foundation for policymakers and practitioners in public administration to understand and address challenges related to data security and individual privacy. Consequently, a secure and trustworthy digital ecosystem can be created, supporting efficient and transparent public services while protecting citizens' privacy rights.

Data Security

Data protection and cybersecurity are crucial components of the modern digital landscape. As organizations increasingly rely on digital platforms, safeguarding sensitive information from cyber threats becomes paramount. Data protection, data privacy, and information privacy are defined as protecting essential data or information from damage, fraud, and loss. Schaar (2017) explains that data protection is not just about safeguarding the data but also about protecting personal data to uphold the right to self-determination and preserve personal privacy. Data protection guards individuals' privacy and personal data from misuse or unauthorized access. The fundamental principles of data protection laws include the legality of processing, access to justice, transparency, and accountability (de Hert et al., 2013)

Cybersecurity encompasses a set of tools, policies, security concepts, safeguards, risk management approaches, actions, training, best practices, assurances, and technologies that can be used to protect the cyber environment, organizational assets, and users (Yadav, 2022). Challenges in cybersecurity include phishing, social engineering, and email fraud, underscoring the need for increased awareness and training to protect the digital environment from electronic threats (Mijwil et al., 2023). Therefore, data security policies are necessary, serving as formal statements that outline an organization's approach to managing information security, detailing essential requirements to protect data assets, and setting management expectations regarding data confidentiality, integrity, and availability (C. Photopoulos, 2008).

Individual Privacy

Individual privacy is a critical element of public administration, contributing to public trust, legal compliance, information misuse prevention, human rights respect, and administrative efficiency. Protecting citizens' privacy should be a top priority for every government agency to ensure fair, transparent, and accountable services. In the context of public administration, protecting personal data becomes increasingly important with implementing e-government services to enhance efficiency and transparency. Strong policies for protecting personal data can encourage broader and more effective e-government adoption (Scope et al., 2022).

The importance of privacy in public administration is closely tied to compliance with various data protection regulations (Caimi et al., 2015). Protecting individual privacy plays a significant role in enhancing public trust in government institutions. When citizens feel that their information is well protected, they are more likely to trust and participate in government programs (Photopoulos, 2008). Furthermore, safeguarding privacy is crucial to prevent the misuse of personal information, leading to identity theft, fraud, or unauthorized use of data. Clear policies and procedures regarding privacy protection can improve administrative efficiency, including better data management and reduced risk of data breaches (Safaat et al., 2022)

METHOD

This study employs a qualitative approach through a literature review to explore data security and individual privacy from the public administration perspective. The research stages include collecting relevant primary and secondary literature sources, such as journal articles, books, and research reports, which discuss aspects of data security and privacy in public administration. Once the data is collected, it organizes and categorizes information based on emerging key themes. References are systematically recorded to present the research findings and abstract information comprehensively. Subsequently, the data is interpreted to generate knowledge that supports the conclusions, focusing on how public administration can balance data protection and individual privacy in the digital era. Adlini et al. (2022) state that the qualitative approach is well-suited for holistically and contextually exploring this phenomenon's complexity without being constrained by formal procedures or calculations. In this context, the qualitative approach allows a deep understanding of the challenges and strategies in securing data and protecting individual privacy, providing valuable insights for more effective public policy (Darmalaksana, 2020).

RESULT AND DISCUSSION

The current era of digitalization presents new challenges in balancing the government's responsibility to safeguard public interests with the individual right to privacy. Public administrators must navigate the complexities of collecting, storing, and utilizing vast amounts of data to inform policy decisions, provide essential services, and ensure national security while adhering to transparency, accountability, and respect for civil liberties (Kim et al., 2014). In the context of cybersecurity and data sovereignty, developing the capacity and capabilities of Indonesian citizens is crucial, particularly concerning the protection of personal data (Aji, 2023). Therefore, a concerted effort from various stakeholders is necessary to strengthen data protection regulations.

Individual Privacy in the Digital Era

Uncontrolled access to information and personal data on global networks allows digital technology to violate fundamental information security and privacy principles. Technological advances drive private and government organizations to collect personal data without explicit consent as users browse the internet. This data influences citizen behavior and decisions through persuasive technology (Palvia, 2024). Furthermore, Akhlaq et al. (2022) highlight that a significant challenge to privacy in the digital age is companies and governments' extensive collection and utilization of personal data. Numerous websites and applications gather information such as browsing history, location, and online purchases to tailor advertisements and enhance services. However, the data can also be leveraged to construct detailed individual profiles, which may be sold to third parties or employed for targeted advertising.

Therefore, it is essential to steer the development of surveillance technology responsibly, considering ethical standards and the impact on individual privacy and social frameworks. Javvaji (2023) asserts that a combination of legislative measures, public awareness, technological safeguards, and collaborative efforts is crucial to balance the advantages of surveillance technology with the protection of individual rights. It also involves considering global differences in surveillance practices, cultural and social implications, and the challenges of cross-border data sharing.

Organizations must adopt comprehensive privacy policies and robust security measures to safeguard personal data. It includes ensuring transparency about data collection practices, obtaining explicit consent from users, and providing options for users to control their data. Public awareness campaigns and educational initiatives are essential to inform individuals about the importance of privacy and how to protect their data online. Governments and regulatory bodies should also proactively enforce data protection laws and hold organizations accountable for data breaches and privacy violations.

Data Security Strategies and Implementation

Data security has become increasingly important in the current digital era. Data security and privacy risks have also escalated with the growing volume and complexity of data organizations' management. Various strategies have been developed to protect data from evolving threats, including data security policies, security technologies and tools, risk management, and security audits.

A study by Cai & Dumlao (2024) discusses strategies for data security. Theoretically, it is necessary to clarify the main concepts of data management, data security, and data analysis and establish an integrated management system and standard specifications. Data collection, storage, processing, analysis, and application stages must be considered to ensure the interconnectedness between data security and data analysis. Empirical research and case analysis should learn from successful and failed experiences and formulate integration strategies suited to the company's conditions. Additionally, it is crucial to strengthen talent development and organizational innovation to support sustainable integration strategies. Companies must continuously innovate in organizational mechanisms and management models and promote cross-departmental and domain collaboration.

Encryption and firewalls can enhance security posture and protect against evolving cyber threats (Hoshmand & Ratnawati, 2023). Firewalls regulate incoming and outgoing traffic from computer networks, allowing control over system access and enhancing protection against external attacks. Using firewalls as part of an organization's security strategy, combined with strict security policies and adequate employee training, is essential to ensure network infrastructure security and prevent unauthorized access. Encryption transforms data into an unreadable form for unauthorized parties, protecting the confidentiality and integrity of sensitive data such as citizens' personal information and public financial transactions. The combination of these technologies, strict security policies, and staff training is integral to data protection strategies in public administration, aiming to maintain public trust, protect individual privacy, and ensure the security of information used in public services.

An analysis by Swanzy et al. (2024) highlights that implementing access control and usage strategies that incorporate user identification and authentication safeguards data confidentiality, integrity, and non-repudiation, ensuring its security at rest and during transmission. Audit trails generate electronic records that validate security documentation and operational actions, which is crucial for addressing non-compliance. Furthermore, the study emphasizes the importance of staff training and industry collaboration to enhance awareness of security threats and establish best practices. Organizations, including financial institutions, should integrate technical and social elements into their data protection strategies, such as adopting homomorphic encryption and developing robust cybersecurity training programs.

Security audits are essential legal and economic mandates for organizations' sustainability, reputation, and influence. It is imperative for organizations operating large or medium-sized computer systems to establish and publish comprehensive security policies. Given the specialized nature of security, it cannot be effectively managed solely by internal personnel. Audits should concentrate on security issues, raising awareness among management, agents, and clients by identifying detrimental practices. Critical audit areas include network topology, system resilience, servers, connectivity equipment, network applications, database management systems (DBMS) and databases, messaging systems, and specialized applications. Intrusive tests must be meticulously planned to prevent any disruption of normal operations. (Zaidoun, 2022).

Challenges in Data Security and Individual Privacy in Public Administration

Cybersecurity has become increasingly crucial in Indonesia with the rapid development of technology and the internet. Cyber threats such as hacking, phishing, ransomware, and data breaches have significantly impacted organizations and individuals in the country, including financial losses, reputational damage, and privacy violations. Unauthorized access, data breaches, and the misuse of personal or confidential data can have serious consequences that require careful attention. Robust security measures are essential to protect data in digitalization and address these challenges (Hyka et al., 2023).

A study by Teoh et al. (2018) outlines that cybersecurity challenges in organizations include a lack of skilled human resources, process issues, and the rapid pace of technological advancements, all of which affect the implementation and effectiveness of cybersecurity measures. At the organizational level, key process-related challenges include the lack of detailed, executable implementation plans, which can hinder the execution of effective security strategies. The second challenge related to human resources is the need for more alignment in the placement and transfer of personnel trained in cybersecurity, which can reduce the effectiveness of risk management. Additionally, more budgets allocated for cybersecurity are a critical issue, as adequate funding can limit an organization's ability to protect its systems and data. On the technological front, the rapid development and updates in cybersecurity technologies present a challenge. The fast pace of technological advancements often makes it difficult for organizations to stay up-to-date with the latest tools and techniques needed to protect data effectively. The lack of quick adaptation to technological innovations can increase the risk to data protection, ultimately threatening the integrity and confidentiality of sensitive information.

One significant data breach in the Indonesian government was the voter data leak managed by the General Elections Commission (KPU) in 2020. The personal data of more than 2.3 million Indonesian voters was allegedly leaked and spread on online forums (Antara, 2020). This breach occurred when sensitive information from the KPU database was found to be publicly accessible through an online forum. The leaked data included full names, places and dates of birth, addresses, and National Identification Numbers (NIK). The impact of this data breach was substantial, as the leaked personal data could be used for criminal activities such as fraud and identity theft. This breach undermined public trust in the government's ability to protect their data, prompting tighter regulations and security measures to safeguard public data.

Another data breach case in Indonesia involved Tokopedia in 2020. Tokopedia, one of the largest e-commerce platforms in Indonesia, experienced a data breach that exposed the personal information of 91 million users. This breach occurred due to unauthorized access to Tokopedia's database, allowing attackers to obtain information such as usernames, emails, and encrypted passwords (Perkasa & Saly, 2022). The impact of this data breach was significant, with Tokopedia incurring substantial costs to enhance security measures and compensate affected users. The breach damaged Tokopedia's reputation and reduced user trust in the platform. Additionally, users experienced adverse effects such as increased spam messages from unknown accounts, misuse of personal data, and suspicious transactions on their Tokopedia accounts (Sihombing et al., 2023). Therefore, assessing information security management in public administration units is crucial to establishing recommended solutions and improving security practices (Szczepaniuk et al., 2020).

Policy Recommendations

Several key elements must be considered in developing effective data security policies for public institutions to ensure comprehensive protection of sensitive information and compliance with regulatory standards. A literature review from leading academic journals highlights these essential elements: data classification and ownership, access control and authentication, data encryption, data backup and recovery, incident response and reporting, employee training and awareness, mobile device security, and third-party risk management.

Data classification and ownership are fundamental components of data security policies, ensuring that data is identified and classified based on its sensitivity and importance and that data ownership is established to ensure accountability (Chaturvedi et al., 2014; Szczepaniuk et al., 2020). Access control and authentication, including strong passwords, multi-factor authentication, and role-based access, are crucial to prevent unauthorized access to sensitive data. Data encryption is necessary to protect data at rest, in transit, and in use by employing robust encryption algorithms and secure critical management practices (Joshi & Singh, 2017). Data backup and recovery are essential for mitigating the impact of data loss through regular backup schedules, periodic data integrity testing, and secure off-site backup storage (Rezgui & Marks, 2008).

Incident response and reporting involve clear incident response plans to detect, control, and recover from security breaches and effective reporting channels for timely incident management. the necessity of regular training and effective policies to enhance cybersecurity awareness and promote cyber hygiene (Concepcion & Palaoag, 2024). Mobile device security must be addressed with secure mobile device usage guidelines, including password protection, encryption, remote wipe capabilities, and regular updates (Venter et al., 2019). Third-party risk management involves evaluating and managing risks associated with vendors or third-party partners, establishing contractual obligations related to data security, and conducting regular security audits (Nie & Dai, 2016).

Conducting research on data security and individual privacy in Indonesia's public administration is fraught with several obstacles. Gaining access to comprehensive and reliable data from public administration sources can be challenging due to bureaucratic restrictions and confidentiality concerns. The cybersecurity threat landscape evolves rapidly, with new vulnerabilities and attack methods emerging continuously. Keeping research findings up-to-date with these changes is a significant challenge. There is a shortage of trained cybersecurity professionals within public administration. This lack of expertise makes it difficult to obtain insightful data and implement advanced security measures effectively.

CONCLUSION

In the current era of digitalization, governments face the challenge of balancing the responsibility of safeguarding public interests with the individual right to privacy. Public administrators must manage large datasets to support policymaking, provide essential services, and ensure national security while adhering to transparency, accountability, and respect for civil liberties. Cybersecurity challenges, including threats such as hacking, phishing, ransomware, and data breaches, have resulted in financial losses, reputational damage, and privacy violations in Indonesia. High-profile data breach incidents, such as the General Elections Commission (KPU) voter data leak and the user data breach at Tokopedia, underscore the need for stricter regulations and enhanced security measures to protect public data.

A comprehensive data security strategy is required, encompassing security policies, security technologies, tools, risk management, and security audits. Encryption and firewalls are crucial for protecting data from cyber threats, while effective access control strategies can safeguard data confidentiality and integrity. Additionally, legislative measures, public awareness, and technological protections are necessary to balance the benefits of technology and the protection of individual rights. Implementing these elements within data security policies will help protect sensitive information, ensure compliance with regulatory standards, and enhance public trust in the government's and organization's ability to safeguard personal data.

REFERENCE

Adlini, M. N., Dinda, A. H., Yulinda, S., & Chotimah, O. (2022). Metode Penelitian Kualitatif Studi Pustaka. *Jurnal Edumaspul*, *6*(1), 974–980. https://doi.org/10.33487/edumaspul.v6i1.3394

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Akhlaq, M., Mustafa, M. T., & Jahangir, H. A. (2022). Defending the Right to Privacy in the Digital Age. *Journal of Policy Research*, *8*(4), 534–538. https://doi.org/10.61506/02.00006

Alalawneh, A. A., Al-Omar, S. Y. S., & Alkhatib, S. (2022). The Complexity of Interaction between Social Media Platforms and Organizational Performance. *Journal of Open Innovation: Technology,* *Market, and Complexity*, *8*(4), 169. https://doi.org/10.3390/joitmc8040169

Antara. (2020). *KPU checks data server security after personal data breach claim*. https://en.antaranews.com/news/149115/kpu-checks-data-server-security-after-personal-data-breach-claim

Bangsawan, G. (2023). Kebijakan Akselerasi Transformasi Digital di Indonesia: Peluang dan Tantangan untuk Pengembangan Ekonomi Kreatif. *Jurnal Studi Kebijakan Publik*, *2*(1), 27–40. https://doi.org/10.21787/jskp.2.2023.27-40

BBC News Indonesia. (2024). *Pusat Data Nasional Sementara lumpuh akibat ransomware, mengapa instansi pemerintah masih rentan terhadap serangan siber?* https://www.bbc.com/indonesia/articles/cxee2985jrvo

Cai, J., & Dumlao, M. F. (2024). Research on the Integration Strategy of Enterprise Data Security Governance and Data Analysis Applications. *Academic Journal of Business & Management*, *6*(5). https://doi.org/10.25236/AJBM.2024.060532

Caimi, C., D'Errico, M., Gambardella, C., Manea, M., & Wainwright, N. (2015). *Implementing Privacy Policies in the Cloud BT - Cyber Security and Privacy* (F. Cleary & M. Felici (eds.); pp. 3–13). Springer International Publishing. https://doi.org/10.1007/978-3-319-25360-2_1

Chaturvedi, M., Narain Singh, A., Prasad Gupta, M., & Bhattacharya, J. (2014). Analyses of issues of information security in Indian context. *Transforming Government: People, Process and Policy*, *8*(3), 374–397. https://doi.org/10.1108/TG-07-2013-0019

Concepcion, J. D., & Palaoag, T. D. (2024). An Assessment of Cybersecurity Awareness among Academic Employees at Quirino State University: Promoting Cyber Hygiene. *Journal of Electrical Systems*, *20*(7), 769–775. https://doi.org/10.52783/jes.3445

Darmalaksana, W. (2020). *Metode penelitian kualitatif studi pustaka dan studi lapangan*.

de Hert, P., Papakonstantinou, V., Wright, D., & Gutwirth, S. (2013). The proposed Regulation and the construction of a principles-driven system for individual data protection. *Innovation: The European Journal of Social Science Research*, *26*(1–2), 133–144. https://doi.org/10.1080/13511610.2013.734047

Djuric, A. (2024). Challenges, Citizens' Trust and Privacy Protection Models in e-Government Systems: Security and Privacy Perspective: Student paper. *2024 23rd International Symposium INFOTEH-JAHORINA (INFOTEH)*, 1–6. https://doi.org/10.1109/INFOTEH60418.2024.10495931

Hoshmand, M. O., & Ratnawati, S. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. *Jurnal Sains Dan Teknologi*, *5*(2 SE-), 679–686. https://ejournal.sisfokomtek.org/index.php/saintek/article/view/2347

Hyka, D., Hyra, A., Basholli, F., Mema, B., & Basholli, A. (2023). *Data security in public and private administration: Challenges, trends, and effective protection in the era of digitalization*.

Indrajaya, T., Primasyah, D., Yulianti, S., Rosmiati, E., & Sova, M. (2022). Peran E-Bisnis Dalam Pengembangan UMKM. *Jurnal Economina*, *1*(2), 239–247. https://doi.org/10.55681/economina.v1i2.73

Javvaji, S. (2023). Surveillance technology: balancing security and privacy in the digital age. *EPRA International Journal of Multidisciplinary Research (IJMR)*, *9*(7), 178–185. https://doi.org/10.36713/epra13852

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, *35*, 128–137. https://doi.org/https://doi.org/10.1016/j.jisa.2017.06.006

Katadata. (2023). *No TitleKominfo Catatkan 1.730 Kasus Penipuan Online, Kerugian Ratusan Triliun*. https://katadata.co.id/digital/teknologi/63f8a599de801/kominfo-catatkan-1730-kasus-penipuan-online-kerugian-ratusan-triliun

Kim, G.-H., Trimi, S., & Chung, J.-H. (2014). Big-data applications in the government sector. *Commun. ACM*, *57*(3), 78–85. https://doi.org/10.1145/2500873

Kompas. (2022). *1,3 Miliar Data Registrasi Kartu SIM Diduga Bocor, Pengamat Sebut Datanya Valid*. https://tekno.kompas.com/read/2022/09/01/13450037/13-miliar-data-registrasi-kartu-sim-diduga-bocor-pengamat-sebut-datanya-valid?page=all

Levin, I., & Mamlok, D. (2021). Culture and Society in the Digital Age. *Information*, *12*(2), 1–13. https://doi.org/10.3390/info12020068

Mao, C., & Chang, D. (2023). Review of cross-device interaction for facilitating digital transformation in smart home context: A user-centric perspective. *Advanced Engineering Informatics*, *57*, 102087. https://doi.org/10.1016/j.aei.2023.102087

Menpan-RB. (2023). *Kominfo Telusuri Dugaan Kebocoran Data Paspor 34 Juta WNI*. https://www.menpan.go.id/site/berita-terkini/berita-daerah/kominfo-telusuri-dugaan-kebocoran-data-paspor-34-juta-wni

Mijwil, M., Omega John Unogwu, Youssef Filali, Indu Bala, & Humam Al-Shahwani. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian Journal of CyberSecurity*, *2023*(SE-Articles), 57–63. https://doi.org/10.58496/MJCS/2023/010

Nie, J., & Dai, X. (2016). On the Information Security Issue in the Information Construction process of colleges and universities. *2016 12th International Conference on Computational Intelligence and Security (CIS)*, 582–585. https://doi.org/10.1109/CIS.2016.0141

Oh, E. G., Chang, Y., & Park, S. W. (2020). Design review of MOOCs: application of e-learning design principles. *Journal of Computing in Higher Education*, *32*(3), 455–475. https://doi.org/10.1007/s12528-019-09243-w

Palvia, R. (2024). Right to Privacy in The Digital Age: Addressing Challenges in The Era of Technology Advancement. *Journal of Unique Laws and Students (JULS)*, *3*(1), 77–85. https://doi.org/10.59126/v3i1a7

Peeran, M., & Shanavas, D. A. M. (2022). Information Security Issues with E-Governance. *International Journal of Next-Generation Computing*, *13*(3). https://doi.org/10.47164/ijngc.v13i3.649

Perkasa, J., & Saly, J. N. (2022). *Legal Liability of Marketplace Companies Against Leaking of User Data Due to Third Party Breaking According to Law Number 8 of 1999 Concerning Consumer Protection (Case Example: Tokopedia User Data Leaking in 2020) BT - Proceedings of the 3rd Tarumanagara International Conference on the Applications of Social Sciences and Humanities (TICASH 2021)*. 606–614. https://doi.org/10.2991/assehr.k.220404.096

Photopoulos, C. (2008). *Chapter 4 - Data Security Policy* (C. B. T.-M. C. L. of S. D. Photopoulos (ed.); pp. 93–124). Syngress. https://doi.org/10.1016/B978-1-59749-239-3.00004-3

Putra, L. D., & Pratama, S. Z. A. (2023). Pemanfatan media dan teknologi digital dalam mengatasi masalah pembelajaran. *Journal Transformation of Mandalika*, *4*(8), 323–329.

Raza, M. A. (2024). Cyber Security and Data Privacy in the Era of E-Governance. *Social Science Journal for Advanced Research*, *4*(1 SE-Articles), 5–9. https://doi.org/10.54741/ssjar.4.1.2

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7), 241–253. https://doi.org/https://doi.org/10.1016/j.cose.2008.07.008

Safaat, P. A., Suparman, N., & Maolani, D. Y. (2022). Inovasi pelayanan publik melalui Program One Hour Service pada Pengadilan Negeri Kelas IB Indramayu. *Jurnal Dialektika: Jurnal Ilmu Sosial*, *20*(2), 83–92. https://doi.org/10.54783/dialektika.v20i2.67

Sastiono, P., & Nuryakin, C. (2019). Inklusi keuangan melalui program layanan keuangan digital dan laku pandai. *Jurnal Ekonomi Dan Pembangunan Indonesia*, *19*(2), 7. https://doi.org/10.21002/jepi.2019.15

Schaar, P. (2017). *Data Protection Empowerment BT - Cyber Security. Simply. Make it Happen.: Leveraging Digitization Through IT Security* (F. Abolhassan (ed.); pp. 21–26). Springer International Publishing. https://doi.org/10.1007/978-3-319-46529-6_3

Scope, N., Rasin, A., Lenard, B., Heart, K., & Wagner, J. (2022). Harmonizing privacy regarding data retention and purging. *Proceedings of the 34th International Conference on Scientific and Statistical Database Management*, 1–12. https://doi.org/10.1145/3538712.3538718.

Sihombing, G. P., Hamzah, H. A., Tian, C., Lianda, T. A. C., Daniswara, M. D., & Saputra, M. N. (2023). Analisis dampak kejahatan siber terhadap kepercayaan konsumen dalam berbelanja di Tokopedia. *Jurnal Ekonomika Dan Manajemen*, *12*(2), 110–120. https://doi.org/10.36080/jem.v12i2.2362

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI*, *27*(1), 38–52. https://doi.org/10.47268/sasi.v27i1.394

Sudaryono, S., Rahwanto, E., & Komala, R. (2020). E-Commerce Dorong Perekonomian Indonesia, Selama Pandemi Covid 19 sebagai Entrepreneur Modern dan Pengaruhnya Terhadap Bisnis Offline. *Jurnal Manajemen Dan Bisnis*, *2*(02), 110–124. https://doi.org/10.47080/10.47080/vol1no02/jumanis

Swanzy, P. N., Abukari, A. M., & Ansong, E. D. (2024). Data Security Framework for Protecting Data in Transit and Data at Rest in the Cloud. *Current Journal of Applied Science and Technology*, *43*(6), 61–77. https://doi.org/10.9734/cjast/2024/v43i64387

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security*, *90*, 101709. https://doi.org/10.1016/j.cose.2019.101709

Teoh, C. S., Mahmood, A. K., & Dzazali, S. (2018). Cyber Security Challenges in Organisations: A Case Study in Malaysia. *2018 4th International Conference on Computer and Information Sciences (ICCOINS)*, 1–6. https://doi.org/10.1109/ICCOINS.2018.8510569

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as &#x201c;the three R's&#x201d; *Heliyon*, *5*(12). https://doi.org/10.1016/j.heliyon.2019.e02855

Yadav, B. (2022). Overview of Cyber Security. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, *2*(4), 489–492. https://doi.org/10.48175/IJARSCT-3959

Zaidoun, A. S. (2022). Security Management. In *Computer Science Security* (pp. 147–164). https://doi.org/10.1002/9781394163847.ch8