Interdisciplinary Journal
Fakultas Ekonomi Universitas Kristen Tentena
Vol. 2, No. 2, (Oktober, 2024) (Hal, 83 - 94)
E-ISSN : 3021-7822
https://jurnal.unkrit.ac.id/index.php/Ide

Analysis of Cybersecurity Implementation in Indonesia Based on the Framework of Administrative Law

Yuyun Alfasius Tobondo[1], Sanny Feria Juliana[2*], Henry Anderson Ruagadi[3], Sulvia Fery Hanry Tondowala[4], Yakin Ngguna[5]
[1,4]Fakultas Keguruan dan Ilmu Pendidikana, Universitas Kristen Tentena
[2]Fakultas Ekonomi, Universitas Kristen Tentena*
[3,5]Fakutlas Ilmu Sosial dan Ilmu Politik, Universitas Kristen Tentena
**email: Shany.sfj@gmail.com*

ABSTRAK

Penelitian ini menganalisis penerapan hukum administrasi dalam meningkatkan keamanan siber di Indonesia, mengevaluasi kebijakan perlindungan data dalam konteks ini, serta mengidentifikasi tantangan dan peluang dalam menerapkan cy-bersecurity di era Society 5.0. Memanfaatkan metode Tinjauan Literatur, penelitian ini mengintegrasikan hasil dari berbagai penelitian untuk memberikan perkiraan kuantitatif yang kuat tentang efek peraturan yang ada. Data berasal dari literatur primer dan sekunder, termasuk buku, jurnal, dan penelitian ilmiah. Temuan menunjukkan bahwa meskipun ada peraturan, implementasi dan penegakan tetap tidak memadai, sebagaimana dibuktikan dengan seringnya pelanggaran data di berbagai bagian. Penelitian ini secara signifikan berkontribusi pada literatur tentang hubungan antara hukum administrasi dan keamanan siber, serta perlindungan data per-sonal di era digital. Namun, keterbatasan penelitian ini termasuk ketergantungannya pada literatur yang ada, dengan perhatian terbatas pada aspek teknis keamanan siber. Penelitian di masa depan harus menggabungkan pendekatan teknis dan kebijakan untuk mengembangkan solusi keamanan siber yang lebih komprehensif.

Kata Kunci : Hukum administrasi, Keamanan siber, Perlindungan data pribadi, Tata kelola yang baik, Masyarakat 5.0

ABSTRACT

This study analyzes the application of administrative law in enhancing cybersecurity in Indonesia, evaluates data protection policies within this context, and identifies challenges and opportunities in implementing cy-bersecurity in the Society 5.0 era. Utilizing the Literature Review method, this research integrates results from various studies to provide a robust quantitative estimate of the effects of exist-ing regulations. The data derives from primary and secondary literature, including books, journals, and scientific research. Findings indicate that despite existing regulations, the implementation and enforcement remain inadequate, as evidenced by frequent data breaches across various sec-tors. This research significantly contributes to the literature on the rela-tionship between administrative law and cybersecurity, as well as per-sonal data protection in the digital era. However, this study's limitations include its reliance on existing literature, with limited attention to the technical aspects of cybersecurity. Future research should combine technical and policy approaches to develop more comprehensive cyber-security solutions.

Keywords **:** *Administrative Law, Cybersecurity, Personal Data Protection, Good Governance, Society 5.0*

INTRODUCTION

Administrative law regulates government activities and interactions between the government, citizens, and third parties. It encompasses the execution of public administration duties, including policy formulation, implementation, and oversight. Its primary aim is to

ensure that government actions comply with legal and justice principles, protecting citizens' rights and establishing legal certainty (Paramitha et al., 2024). Key manifestations include legislation, public policies, administrative decisions (beschikking), audits, inspections, and public complaints, ensuring compliance and accountability. Important principles in administrative law are legality, transparency, accountability, and public participation (Susanto, 2019).

Cybersecurity involves protecting systems, networks, and programs from digital attacks aimed at accessing, altering, or destroying sensitive information, extorting money, or disrupting processes (Budi et al., 2021). Strategies include firewalls, data encryption, intrusion detection systems, and security policies. Education and training raise awareness of cyber threats, while legal frameworks ensure compliance with security standards.

Personal data protection aims to safeguard individuals' information from unauthorized access, use, or dissemination. In the digital era, personal data includes identifying information like names, addresses, and financial details (Iswandari, 2021). The goal is to maintain privacy and prevent data misuse. Laws and regulations, such as the Personal Data Protection Act, govern data collection, storage, and use. Control mechanisms include consent, data access and correction rights, and sanctions for violations. Technologies like encryption and access controls are essential(Arham & Risal, 2023).

In Indonesia, low awareness about digital data security is a major concern. The 2017 Wannacry ransomware incident showed only 33% of institutions complied with system update recommendations from the Ministry of Communication and Informatics (Aji, 2023). Data breaches in 2021 involving ministries, agencies, and private sectors, such as BPJS Health and BRI Life, highlighted national cybersecurity weaknesses (Firdaus, 2024). Indonesia’s 0% ranking in the 2020 Global Cybersecurity Index (GCI) report further illustrated these challenges (Annur, 2022).

Cybersecurity in Indonesia remains inadequate. Existing theories often fail to address specific problems faced by Indonesia, such as the lack of resources and infrastructure. The theory of Good Governance, emphasizing transparency and accountability, has not been fully implemented, causing uncertainty in handling data breaches (Adellya Salsabilla Hermawan, 2022).

This paper aims to analyze the application of administrative law in enhancing cybersecurity in Indonesia, evaluate personal data protection policies within this context, and identify challenges and opportunities in implementing cybersecurity in the Society 5.0 era (Siburian, 2024). By understanding how administrative law can strengthen cybersecurity and personal data protection, effective solutions to current problems may be found. The hypothesis is that effective application of administrative law can enhance cybersecurity and personal data protection in Indonesia and address the challenges of cybersecurity in the Society 5.0 era (DSG, 2023).

METHOD

The object of this research is the low awareness among public and private institutions in Indonesia regarding digital data security. This is evidenced by the Wannacry ransomware inci-dent in 2017, where only 33% of institutions complied with the Ministry of Communication and Information's advice to update their systems (Adellya Salsabilla Hermawan, 2022). Additionally, several data breaches in 2021 in-volving ministries, agencies, and the private sector highlighted weaknesses in national cybersecu-rity. The challenges in developing cybersecurity policies in Indonesia are further illustrated by Indonesia's 0% ranking in the 2020 Global Cybersecurity Index (GCI) report.

This research employs a library research approach with a Systematic Literature Review (SLR) methodology. Primary data comes from relevant literature discussing low awareness among public and private institutions regarding digital data security, as demonstrated by the Wannacry ransomware incident in 2017 and the 2021 data breaches (Adellya Salsabilla Hermawan, 2022). Secondary data includes literature on related research keywords sourced from books, journals, and other scientific studies.

The foundational theories in this research include the Theory of Good Governance and the Theory of Cyber Attack. The Theory of Good Governance, as defined by Sadjijono (2007), de-scribes effective government actions to achieve state goals based on norms and public interests (Adellya Salsabilla Hermawan, 2022). The Theory of Cyber Attack refers to various types of malware attacks, including spyware, ad-ware, bots, and ransomware, which can cause significant damage to information systems. These theories provide a framework for analyzing the existing problems.

The research process involves several stages and data collection techniques utilizing the Literature Review technique. The process begins with determining spe-cific research topics and questions. Researchers then collect secondary data from published stud-ies using strict inclusion-exclusion criteria. The data collection technique involves searching litera-ture through electronic databases and extracting relevant data from selected studies. Researchers calculate the effect size for each study and conduct statistical analyses to combine the results, providing more precise and robust effect estimates.

Data analysis in this research uses content analysis methods. This involves studying and processing data to identify patterns, relationships, and important information. Content analysis enables researchers to deeply analyze the data collected from various studies, identify key find-ings, and evaluate the strengths and weaknesses of each analyzed study. This technique helps generate more valid and reliable conclusions based on the available data.

RESULTS AND DISCUSSION

Administrative Law

The literature review on Administrative Law underscores its crucial role in regulating government activities and interactions with citizens and third parties. Administrative law is identified as essential in ensuring that every administrative action aligns with principles of justice, transparency, and accountability, which are fundamental for building public trust and achieving good governance (Paramitha et al., 2024).

The data from the literature highlights that administrative law principles extend beyond legality to include public participation and oversight. This framework encourages active citizen involvement in monitoring and controlling government actions, thereby promoting greater accountability and transparency in governance (Paramitha et al., 2024).

The analysis reveals that effective implementation of administrative law can significantly address governance issues in Indonesia. Weaknesses in applying these principles often lead to public distrust and ineffective policies. Therefore, enhancing administrative law is critical for improving governance in Indonesia (Paramitha et al., 2024).

Cybersecurity

The literature review on cybersecurity highlights that it encompasses practices designed to protect systems, networks, and programs from digital attacks. Various strategies are identified to safeguard digital assets, including firewalls, data encryption, and intrusion detection systems (Budi et al., 2021).

The data from the literature indicates that cybersecurity extends beyond technological solutions to include policies and procedures. Essential components are education and training to raise awareness about cyber threats and the development of legal frameworks and regulations to ensure compliance with security standards (Budi et al., 2021).

The real-world context in Indonesia shows significant cybersecurity challenges, including low awareness and compliance with cybersecurity policies. The Wannacry ransomware incident in 2017 and multiple data breaches in 2021, such as those involving BPJS Kesehatan, exemplify these issues. Consequently, enhancing awareness and compliance with cybersecurity policies is crucial for improving Indonesia's cybersecurity landscape (Budi et al., 2021).

Personal Data Protection

The literature review on personal data protection highlights efforts to safeguard individuals' personal information from unauthorized access, use, or dissemination. Various laws and regulations govern the collection, storage, and use of personal data, aiming to ensure privacy and prevent misuse that could harm individuals (Yovita, 2016).

The data from the literature underscores the importance of personal data protection, emphasizing mechanisms such as obtaining individual consent before data usage, providing the right to access and correct data, and enforcing sanctions for data protection violations (Yovita, 2016).

In reality, personal data protection in Indonesia faces significant challenges. Despite existing laws, the implementation and enforcement remain weak, evidenced by numerous data breaches. Therefore, strengthening law enforcement and raising awareness about the importance of personal data protection are crucial steps to enhance the current situation (Yovita, 2016).

Good Governance

The literature review on good governance highlights principles such as transparency, accountability, public participation, and effectiveness. These principles form a framework essential for ensuring that governance meets public needs (Susanto, 2019).

The data indicate that good governance is not only about formulating sound policies but also about their effective implementation and oversight. This includes mechanisms to ensure policies are properly enacted and adequate oversight is in place to prevent abuse of power (Susanto, 2019).

In practice, the implementation of good governance principles in Indonesia requires significant strengthening. Despite efforts to improve transparency and accountability, many challenges persist. Enhancing oversight mechanisms and increasing public participation are crucial steps for achieving effective good governance in Indonesia (Susanto, 2019).

Society 5.0

The literature review on Society 5.0 highlights the integration of technology and society to create a smarter and more connected community. Society 5.0 utilizes advanced technologies such as the Internet of Things (IoT) and artificial intelligence (AI) to enhance the quality of life (Setiawan et al., 2019).

The data indicates that Society 5.0 aims to leverage technology to address social and economic issues. This includes improving healthcare, education, and transportation services, as well as creating safer and more comfortable environments (Setiawan et al., 2019).

In reality, the implementation of Society 5.0 in Indonesia faces significant challenges. Despite the availability of technology, effective implementation requires robust infrastructure and supportive policies. Therefore, investing in technology infrastructure and developing supportive policies are essential steps for realizing Society 5.0 in Indonesia (Setiawan et al., 2019).

Discussion

The findings of this study reveal several important insights related to the application of administrative law in the context of cybersecurity in Indonesia, as illustrated in the table below:

Table 1. Research Findings

No	Research Objective	Research Findings
1	To analyze the application of state administrative law in enhancing cybersecurity in Indonesia.	The application of state administrative law is not yet optimal in improving cybersecurity. Regulations exist, but enforcement and implementation are weak.
2	To evaluate personal data protection policies in Indonesia within the context of state administrative law.	Personal data protection policies are still ineffective, with many data breach incidents indicating weaknesses in the legal and protection systems.
3	To identify challenges and opportunities in the implementation of cybersecurity in the era of Society 5.0.	The main challenges include a lack of awareness and trained human resources. However, there are opportunities in leveraging new technologies such as IoT and AI to strengthen cybersecurity.

Source: *Analysed from the primary source.*

Suboptimal Implementation

The application of administrative law in enhancing cybersecurity in Indonesia has been suboptimal. Despite existing regulations aimed at protecting digital infrastructure and data, implementation and enforcement remain weak and inconsistent, resulting in numerous data breaches across both public and private sectors. These breaches reveal significant vulnerabilities within the cybersecurity framework, underscoring the need for more robust enforcement mechanisms and comprehensive policy revisions (“Understanding Cybercrime: Phenomena, Challenges and Legal Response,” 2023).

The lack of stringent oversight and accountability measures further exacerbates the situation, leading to repeated failures in data protection protocols and creating an

environment where breaches occur with alarming frequency. This issue highlights the critical need for not only stronger regulatory frameworks but also better-trained personnel and more effective technological solutions to ensure data integrity and security (Joseph, 2018).

Ineffective Data Protection Policies

Personal data protection policies in Indonesia remain notably ineffective, despite the growing importance of safeguarding personal information in the digital age. Frequent and alarming data breaches in various sectors highlight significant weaknesses and gaps in the current legal and data protection systems that urgently need to be addressed. These breaches compromise individual privacy and pose substantial risks to national security and economic stability (Joseph, 2018).

Existing regulations lack the robustness and enforcement needed to prevent such incidents effectively. Furthermore, the absence of stringent oversight mechanisms and accountability measures exacerbates the situation, allowing repeated violations without adequate consequences. To comprehensively address these issues, it is essential to revise and strengthen legal frameworks, invest in advanced technological solutions, and ensure proper training for personnel responsible for data protection (Deng & Yan, 2021).

Public awareness campaigns and education on the importance of data security are also crucial in fostering a culture of vigilance and responsibility towards personal data protection in Indonesia.

Challenges in Society 5.0 Era

The main challenges in implementing cybersecurity in the Society 5.0 era include a lack of awareness and trained human resources in cybersecurity. Despite the critical need for robust cybersecurity measures, many individuals and organizations lack a comprehensive understanding of the risks and threats associated with digital technologies. This lack of awareness creates vulnerabilities that cybercriminals can easily exploit, leading to significant data breaches and security incidents. Additionally, there is a shortage of skilled professionals who are well-versed in the latest cybersecurity practices and technologies, making it difficult for organizations to effectively protect their digital assets and respond to emerging threats (Khatri et al., 2023).

However, there are significant opportunities in leveraging new technologies such as the Internet of Things (IoT) and artificial intelligence (AI) to strengthen cybersecurity in Indonesia. These advanced technologies offer innovative solutions for monitoring and managing cybersecurity threats more efficiently. For example, IoT devices can provide real-time data and insights that help identify potential vulnerabilities and prevent attacks before they occur. Similarly, AI can analyze large volumes of data and detect patterns indicating malicious activity, enabling quicker and more accurate responses to cyber threats. By investing in these technologies and integrating them into cybersecurity strategies, Indonesia can enhance its ability to safeguard digital infrastructure and protect sensitive information (Candra et al., 2021).

Moreover, fostering collaboration between the government, private sector, and academic institutions is crucial for addressing these challenges. Joint efforts can facilitate the development of comprehensive training programs and public awareness campaigns aimed at improving cybersecurity literacy among citizens and professionals alike (“Raising Awareness of Cybersecurity,” 2021). Such initiatives can help bridge the knowledge gap and ensure that individuals and organizations are better equipped to handle cybersecurity issues in the Society 5.0 era. Furthermore, regulatory frameworks need to be strengthened and updated to keep pace with technological advancements and evolving cyber threats. By taking a

proactive and collaborative approach, Indonesia can effectively address the cybersecurity challenges of the Society 5.0 era and create a safer digital environment for all (Candra et al., 2021).

Overall, the study emphasizes the critical need for improved regulations, increased awareness, and advanced technology to achieve better cybersecurity in Indonesia. Current regulations, while present, lack the necessary robustness and enforcement mechanisms needed to protect against cyber threats adequately. There is a pressing need to develop and implement more comprehensive and stringent regulations that can effectively address the evolving nature of cyber threats. Furthermore, these regulations should be regularly updated to keep pace with the rapid advancements in technology and the increasing sophistication of cyber attacks.

Awareness is another crucial component emphasized by the study. Many individuals and organizations in Indonesia still lack a comprehensive understanding of the risks and consequences associated with cyber threats. This lack of awareness significantly contributes to vulnerabilities that cybercriminals can easily exploit (Widiasari & Thalib, 2022). Public awareness campaigns and educational programs are essential to improve understanding and foster a culture of vigilance and responsibility towards cybersecurity. By increasing awareness, individuals and organizations can be better prepared to recognize and respond to potential threats, thereby reducing the risk of data breaches and other cyber incidents (Chakraborty et al., 2023).

In addition to regulations and awareness, the study highlights the importance of leveraging advanced technology to enhance cybersecurity. Technologies such as the Internet of Things (IoT), artificial intelligence (AI), and machine learning offer innovative solutions for detecting and mitigating cyber threats (Apruzzese et al., 2022). These technologies can provide real-time monitoring and analysis of network traffic, identify patterns indicative of malicious activity, and automate responses to potential threats. Investing in these technologies and integrating them into cybersecurity strategies can significantly enhance the ability to protect digital infrastructure and sensitive information. Furthermore, continuous research and development in cybersecurity technology are vital to staying ahead of emerging threats and ensuring a resilient and secure digital environment in Indonesia (Candra et al., 2021).

Summary of Findings

The research summary indicates that the current application of administrative law in Indonesia has not been optimal in enhancing cybersecurity. Despite efforts to strengthen regulations, data breaches frequently occur, indicating weak implementation and enforcement of laws (Chintia et al., 2019). Additionally, personal data protection faces many challenges, including a lack of awareness and compliance from both private and public institutions. These challenges are increasingly significant given the rapid and sophisticated technological developments and the rising use of digital devices in various aspects of daily life. Therefore, continuous efforts to raise awareness and compliance with existing regulations are becoming more urgent (Amin et al., 2023).

In the Society 5.0 era, these challenges are becoming more complex with the deeper integration of technology into daily life. Society 5.0 envisions a highly connected society where data is crucial and must be well-protected. In this context, cybersecurity is key to maintaining data integrity and privacy (Anggen Suari & Sarjana, 2023). However, in Indonesia, there are still many shortcomings in this area. The government and private sector need to collaborate to strengthen cybersecurity infrastructure and ensure all parties adhere

to strict security standards. Only then can Indonesia fully leverage the potential of the Society 5.0 era without compromising the security and privacy of its citizens (Chintia et al., 2019).

Comparison with Previous Research

This study aligns with other research highlighting weaknesses in Indonesia's cybersecurity policies and personal data protection. Despite having regulations in place, the primary obstacles remain in their implementation and enforcement. Challenges include inadequate infrastructure, a lack of trained professionals, and poor coordination between agencies. Many institutions grapple with outdated systems incapable of countering modern cybersecurity threats. Furthermore, the critical shortage of cybersecurity experts hampers effective policy execution. Fragmented coordination among governmental and private entities leads to inconsistent regulation application. Addressing these issues requires a multifaceted approach, including policy reforms, infrastructure upgrades, and enhanced training programs.

The strength of this study lies in its literature review approach, providing a quantitative overview of the effects of existing regulations compared to descriptive or case-by-case studies. By aggregating data from multiple sources, this method offers a comprehensive understanding of how various factors influence cybersecurity and data protection outcomes. This approach identifies existing problems and suggests measurable solutions based on extensive data. For instance, the study can highlight specific regulatory gaps and recommend targeted interventions likely to be effective. Furthermore, the statistical techniques used in literature review help minimize biases and enhance the reliability of the findings, making the results more robust and applicable to policy-making processes (Rizal, 2019).

By offering a detailed analysis of the current state of cybersecurity and personal data protection, the study underscores the need for continuous monitoring and policy evaluation. Literature review enables the identification of best practices from different contexts, adaptable for implementation in Indonesia to improve cybersecurity resilience. The comprehensive nature of this research highlights the importance of stakeholder collaboration in tackling cybersecurity challenges, encouraging cooperation between government, the private sector, and civil society (Tanzilla et al., 2023).

In conclusion, the literature review approach in this study provides a valuable framework for understanding and addressing the complex issues surrounding cybersecurity and personal data protection in Indonesia. The findings emphasize the need for improved regulations, better enforcement mechanisms, and increased investment in infrastructure and human resources. By leveraging the strengths of literature review, this research offers actionable insights for policymakers to develop more effective and sustainable cybersecurity strategies. As technology evolves, it is essential that policies are regularly updated to address emerging threats and protect the privacy and security of all citizens.

Strengths of the Literature Review Approach

The strength of the literature review approach lies in its ability to combine results from various studies, providing a more comprehensive and holistic view of the effectiveness of cybersecurity regulations and personal data protection measures. By aggregating data from multiple sources, this method allows for a more robust analysis, capturing nuances and variations that individual studies might miss (Yang et al., 2020). This comprehensive aggregation helps in understanding the overall impact and efficacy of different regulatory approaches and data protection strategies. Furthermore, this approach enables researchers to identify common patterns and trends that might not be visible in individual studies, thus

offering insights that are more accurate and applicable to real-world policy-making (Graeden et al., 2023).

This ability to discern patterns across multiple datasets allows for more accurate and relevant policy recommendations based on stronger and broader evidence. The literature review method can highlight which regulatory practices are most effective across different contexts and environments, thereby providing policymakers with well-founded guidance. Additionally, it can help in identifying gaps in current regulations and suggesting areas where further improvements are necessary. This evidence-based approach is crucial for formulating policies that are not only theoretically sound but also practically effective in enhancing cybersecurity and protecting personal data (Ogu et al., 2020).

By using statistical methods to combine data from various studies, this research can provide more precise effect estimates, essential for understanding the true impact of cybersecurity measures and data protection laws. These statistical techniques help reduce biases and inconsistencies that might be present in individual studies, leading to more reliable conclusions. This precision is critical for policymakers who need concrete data to support their decisions and ensure that the implemented regulations are effective and efficient. Ultimately, this contributes significantly to developing cybersecurity and personal data protection policies in Indonesia, fostering a safer and more secure digital environment (Amin et al., 2023).

Incorporating findings from diverse sources, literature review not only strengthens the validity of the conclusions but also enhances the generalizability of the results. This broader applicability ensures that the insights gained are relevant to a wide range of scenarios and can be adapted to different sectors and regions within Indonesia. This holistic view is essential for developing comprehensive strategies that address the multifaceted nature of cybersecurity threats and data privacy issues. In conclusion, the literature review approach is a powerful tool that significantly enhances the quality and reliability of research in cybersecurity and personal data protection, providing invaluable support for the formulation of effective policies in Indonesia.

Reflection and Implications

The study's findings underscore the relevance and importance of analyzing the application of administrative law in enhancing cybersecurity and evaluating personal data protection policies. The research has identified critical areas for improvement in existing regulations and enforcement practices. These insights provide a robust foundation for policymakers to enhance current policies, ultimately raising public awareness about cybersecurity and personal data protection. Additionally, the findings can motivate stakeholders to take concrete actions to strengthen the enforcement of related laws.

This research significantly contributes to enhancing cybersecurity and personal data protection in Indonesia. The insights gained are expected to provide valuable knowledge for policymakers, practitioners, and academics in this field. The study suggests that improving cybersecurity and personal data protection requires a holistic approach, involving collaboration among various sectors and stakeholders, including the government, private sector, and community. Thus, this research offers both theoretical and practical contributions, serving as a reference for developing more effective and efficient policies in the future.

Furthermore, the study highlights the importance of education and raising public awareness regarding cybersecurity and personal data protection. One of the main challenges identified is the lack of public awareness and understanding of the risks and impacts of personal data breaches. Therefore, the study advocates for comprehensive educational campaigns to improve public understanding of the importance of protecting personal data.

Enhanced education can lead to increased vigilance and proactive measures among the public, contributing to overall cybersecurity improvement in Indonesia.

The implications of this research indicate the need for reform in the application of administrative law and personal data protection policies. The findings suggest that more stringent policies and stronger law enforcement are required to address cybersecurity challenges in the Society 5.0 era (Anggen Suari & Sarjana, 2023). Additionally, enhancing education and public awareness is crucial to ensuring that all parties understand the importance of cybersecurity and personal data protection.

The research identifies several reasons for weaknesses in the application of laws and policies, including inadequate resources and infrastructure, as well as a lack of awareness and compliance from relevant institutions. The rapid development of technology often outpaces regulatory advancements, creating gaps in the cybersecurity and personal data protection systems.

Based on the research findings, recommended actions include strengthening law enforcement through increased resources and training for officers (Kusuma & Rahmani, 2022). Additionally, efforts should be made to enhance public awareness and education regarding the importance of cybersecurity and personal data protection. The government also needs to accelerate regulatory reform to keep pace with rapid technological developments and the complexity of challenges in the Society 5.0 era (Anggen Suari & Sarjana, 2023).

CONCLUSION

The findings of this research reveal the significant vulnerabilities in Indonesia's cybersecuri-ty infrastructure. Despite the existence of regulations, the implementation and enforcement of these laws are critically deficient. Frequent data breaches across both public and private sectors highlight the urgent need for substantial improvements in cybersecurity and personal data protec-tion.

This research contributes significantly to the fields of legal science and cybersecurity. Theo-retically, it enhances the literature on the intersection of administrative law, cybersecurity, and personal data protection in the digital era. Practically, it provides concrete recommendations for policymakers to fortify regulations and elevate public awareness about the importance of cyber-security and personal data protection. This is crucial for addressing the challenges presented by Society 5.0, where technology is deeply integrated into daily life.

However, there are limitations to this research. One major limitation is the reliance on exist-ing literature, which may not encompass all relevant aspects. Additionally, the research predomi-nantly focuses on policies and regulations, with less emphasis on the technical facets of cyberse-curity. These limitations highlight the need for further, more comprehensive research that inte-grates both technical and policy approaches to develop more robust cybersecurity.

REFERENCES

Adellya Salsabilla Hermawan. (2022). Penerapan Asas Asas Hukum Administrasi Negara Dalam Instrumen Pemerintahan Yang Baik. *Education : Jurnal Sosial Humaniora dan Pendidikan*, *2*(3), 58–67. https://doi.org/10.51903/education.v2i3.270

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

Amin, A., Batubara, A. K., Parent, P. A., Maha, S., Sinulingga, S., & Fauzi, I. (2023). PENATAGUNAAN DAN KEGUNAAN: PRINSIP-PRINSIP KEBIJAKAN UNTUK TRANSPARANSI BERBASIS INFORMASI. *Jurnal Network Media*, *6*(1), 1–11.

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142.

Annur, C. M. (2022). *Pelindungan Data Pribadi Warga RI Masih Tergolong Rendah*. https://databoks.katadata.co.id/datapublish/2022/08/09/pelindungan-data-pribadi-warga-ri-masih-tergolong-rendah

Apruzzese, G., Laskov, P., de Oca, E. M., Mallouli, W., Rapa, L. B., Grammatopoulos, A. V., & Franco, F. D. (2022). The role of machine Learning in cybersecurity. *Digit. Threat.*

Arham, M. R. H., & Risal, M. C. (2023). *PERLINDUNGAN DATA PRIBADI BAGI PENGGUNA MEDIA SOSIAL*. *3*(2).

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Candra, A., Suhardi, S., & Persadha, P. D. (2021). Indonesia facing the threat of cyber warfare: A strategy analysis. *Pertahanan*, *7*(3), 441.

Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial intelligence for cybersecurity: Threats, attacks and mitigation. In *Artificial Intelligence for Societal Issues* (pp. 3–25). Springer International Publishing.

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Rakhmawati S.Kom., N. A., M. Sc. Eng. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal of Information Engineering and Educational Technology*, *2*(2), 65.

Deng, X., & Yan, M. (2021). Research on the legal protection of personal information in the big data era. *J. Phys. Conf. Ser.*, *1883*(1), 012081.

DSG. (2023, February 14). *RED FLAG! Keamanan Data Digital Di Indonesia Sangat Buruk, Ini Peran Pemerintah.pdf*. https://digitalsolusigrup.co.id/red-flag-keamanan-data-digital-di-indonesia-sangat-buruk-ini-peran-pemerintah/

Firdaus, A. (2024). *Kasus Kebocoran Data Pribadi di Indonesia: 10 Kejadian Terbesar yang Perlu Diketahui*.

Graeden, E., Rosado, D., Stevens, T., Knodel, M., Hendricks-Sturrup, R., Reiskind, A., Bennett, A., Leitner, J., Lekas, P., & DeMooy, M. (2023). *A new framework for global data regulation*.

Iswandari, B. A. (2021). Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance. *Jurnal Hukum Ius Quia Iustum*, *28*(1). https://doi.org/10.20885/iustum.vol28.iss1.art6

Joseph, R. C. (2018). Data Breaches: Public Sector Perspectives. *IT Prof.*, *20*(4), 57–64.

Khatri, S., Cherukuri, A. K., & Kamalov, F. (2023). *Global Pandemics Influence on Cyber Security and Cyber Crimes*. https://arxiv.org/abs/2302.12462

Kusuma, A. C., & Rahmani, A. D. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). *Supremasi*, *5*(1), 46–63.

Ogu, E. C., Ogu, C., & Oluoha, O. U. (2020). 'Global cybersecurity legislation'—Factors, perspective and implications. *Int. J. Bus. Contin. Risk Manag.*, *10*(1), 80.

Paramitha, A., Sam, I., Fakhry, W., Muhammad, A., Sidiq, F., Hutrin, W., Mohamad, K., Muhtar, M. H., Taufik, A., Aziz, M., Saptono, Z., Syaiful, J., Ali, A., Suwandoko, R., Dika, J., Dian, Y., Khasanah, D., Munir, S., Sabar, H., & Gazali, M. (2024). *HUKUM ADMINISTRASI NEGARA*.

Raising awareness of cybersecurity. (2021, November). In *ENISA*. https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity

Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. *J. Cakrawala Huk.*, *10*(2).

Setiawan, A., Lusanjaya, G., & Kurnia, T. (2019). KESADARAN KEAMANAN PRIVASI DAN MASYARAKAT 5.0. *Journal of Accounting and Business Studies*, *4*(2). https://doi.org/10.61769/jabs.v4i2.467

Siburian, H. (2024). *PENGANTAR STRATEGI KEAMANAN SIBER INDONESIA.pdf*. https://www.bssn.go.id/strategi-keamanan-siber-nasional/

Susanto, S. N. H. (2019). Good Governance Dalam Konteks Hukum Administrasi. *Administrative Law and Governance Journal*, *2*(2), 205–217. https://doi.org/10.14710/alj.v2i2.205-217

Tanzilla, F. D., Hanita, M., & Widiawan, B. (2023). Cyber Security In Indonesia Post Establishment Of The Personal Data Protection Law. *International Journal of Progressive Sciences and Technologies*, *40*(2), 164. https://doi.org/10.52155/ijpsat.v40.2.5617

Understanding cybercrime: Phenomena, challenges and legal response. (2023). In *ITU*. https://www.itu.int/pub/D-STR-CYB_CRIME-2015

Widiasari, N. K. N., & Thalib, E. F. (2022). The impact of Information Technology development on cybercrime rate in Indonesia. *Journal of Digital Law and Policy*, *1*(2), 73–86.

Yang, A., Kwon, Y. J., & Lee, S.-Y. T. (2020). The impact of information sharing legislation on cybersecurity industry. *Ind. Manag. Data Syst.*, *120*(9), 1777–1794.

Yovita. (2016, Desember). *Indonesia sudah miliki aturan soal perlindungan Data Pribadi.pdf*. https://www.kominfo.go.id/content/detail/8621/indonesia-sudah-miliki-aturan-soal-perlindungan-data-pribadi/0/sorotan_media