RLJ Ratio Legis Journal
ISSN 2830-4624
published by
Master of Law, Faculty of Law
Universitas Islam Sultan Agung

Security Cyber Law Based on Pancasila Justice and Sustainable Development in the Field of Human Resources: A Cyber Law Perspective

Dewo Wishnu Setya Kusuma
Faculty of Law, Sultan Agung Islamic University, Semarang, Indonesia, E-mail: dewowishnuSetyaKusuma.std@unissula.ac.id

Abstract. *The digital era brings new opportunities and challenges, including in the realm of cybersecurity. The Indonesian National Police (Polri), as one of the key institutions in Indonesia, needs to strengthen its cybersecurity measures to protect its data, information, and systems. This journal discusses cybersecurity within the context of Pancasila justice and sustainable development in the field of human resources (HR), with a focus on cyber law. This study employs qualitative methods through a literature review and in-depth analysis. The research findings indicate that cybersecurity must be realized by upholding the values of Pancasila justice, such as divinity, humanity, unity, democracy, and social justice. Sustainable development in the HR sector of Polri is key to enhancing capacity and capability in facing cyber threats. Cyber law plays a crucial role in regulating and protecting the digital space, ensuring justice for all parties. In conclusion, cybersecurity based on Pancasila justice and the sustainable development of Polri's HR is a strategic solution for achieving a secure, just, and sustainable digital space.*

Keywords: *Digital; Institutions; Security.*

1. Introduction

In the digital era, it has brought major changes in various aspects of life, including in terms of cybersecurity. The development of information and communication technology has provided many benefits, such as easy access to information, increased business efficiency, and transformation of public services. However, on the other hand, the digital era also presents new challenges in the form of increasingly complex cyber threats. In Indonesia, the challenges in cybersecurity are increasingly complex with the increasing number of cyber attacks targeting personal data, government systems, and critical infrastructure.

These cyberattacks not only cause significant financial losses, but also threaten national security and individual privacy. Citizens' personal data, including sensitive information such as identity, medical records, and financial data, are prime targets for cybercriminals. In addition, attacks on government systems and critical infrastructure, such as power grids, transportation, and healthcare, can result in major disruptions that impact the well-being of the wider community. Cybersecurity is not just about technology, but also about how policies and regulations can protect society in a fair and sustainable manner.[1].

In this context, cybersecurity policies must be designed to ensure that all citizens receive equal protection and that their rights are respected. This is important to prevent discrimination and ensure that all levels of society have equal access to cyber protection.[2].

Pancasila, as the state ideology of Indonesia, provides a strong ethical and moral foundation for forming a just cybersecurity policy. The values contained in Pancasila, such as divinity, humanity, unity, democracy, and social justice, must guide the development of policies and regulations in this area. The principle of social justice contained in Pancasila demands equal protection for all citizens, without discrimination. This means that cybersecurity policies must be designed to protect all citizens, regardless of their social, economic, or geographic background.

In addition, sustainable development in the field of human resources (HR) emphasizes the importance of developing relevant and sustainable skills to deal with cyber threats. Quality and sustainable HR development is very important to create a workforce[3], which is able to address cybersecurity challenges. This includes ongoing training, formal education, and certification programs that can improve the workforce's competency in cybersecurity.

This study aims to explore how the principles of Pancasila and sustainable development can be applied in cybersecurity policies and cyber legal regulations in Indonesia. The main focus of this study is on the development of human resources capable of facing cybersecurity challenges, and how legal regulations can support this effort. Using a qualitative approach and normative analysis, this study will analyze various existing policies and regulations, and evaluate how the principles of Pancasila justice and sustainable development can be integrated to create a safer and more equitable digital environment.

In an effort to improve cybersecurity in Indonesia, it is important to consider the legal aspects that govern the use of technology and data protection. Cyber legal regulations must be designed to address various cyber threats, ensure fairness for

[1] Yuliastuti Anggun, et al., Analysis of the “Tinder Swindler” Phenomenon on Online Dating Applications Using Lifestyle Exposure Theory”, Journal of Criminology, 6 (2), 2022, pp. 169-170.

[2] Mansur, DMA, & Gultom, E., (2009), Cyber Law, Legal Aspects of Information Technology, 2nd edition, Bandung: Refika Aditama, p. 122

[3] Crumpracker, M., & Crumpracker, J. M. (2007). Succession Planning and Generational Stereotypes: Should HR Consider Age-Based Values and Attitudes a Relevant Factor or a Passing Fad?. Public Personnel Management, p. 349-359.

all parties, and support the development of competent human resources in this field.[4]. Thus, this research is expected to provide a positive contribution in the development of policies and regulations that are able to address the challenges of cyber security threats effectively.[5], while still upholding the values of Pancasila and the principles of sustainable development.

2. Research Method

This study uses a qualitative method with a normative analysis approach. Data were collected through a literature study that includes legal documents, government policies, academic literature, and reports from related organizations. The normative analysis approach is used to assess existing cyber law regulations in Indonesia, as well as their relevance to the principles of Pancasila justice and sustainable development goals.

Research steps include:

1. Collecting data from relevant secondary sources, including laws, government regulations, and cybersecurity-related policies.

2. Content analysis of these documents to identify the principles of Pancasila justice that have been integrated into cybersecurity policies and regulations.

3. Evaluation of cybersecurity policies and regulations against sustainable development goals, especially in human resource development.

4. Drawing conclusions and recommendations based on research findings.

The data obtained were analyzed descriptively and interpretively to produce a deep understanding of cyber security in the context of Pancasila justice and sustainable development in the field of Polri human resources.[6].

3. Results And Discussion

3.1. Cyber Security

Cybersecurity is the effort to protect data, information, and systems from unauthorized access, use, disclosure, alteration, or destruction. Cyber threats can be malware, phishing, ransomware, cybercrime[7], and others. Cybersecurity is an important issue in the digital era because more and more human activities are carried out online. Personal data and information, financial data, and other important information are stored in digital systems and are vulnerable to cyber attacks.

[4] Bennett, S., Maton, K., & Kervin, L. (2008). The 'Digital Natives' Debate: A Critical Review of the Evidence. British Journal of Educational Technology, p. 775-786.

[5] Wibowo Mia Haryanti, et al., “Phishing threats to social media users in the world of cyber crime”, JOEICT (Jurnal Of Education And Information Communication Technology), 2017, p.5.

[6] Cahyono, H., & Susanto, D., "Effectiveness of Training Programs in the Police Environment", Journal of Educational Management, 14 (2), 2018, pp. 110-125.

[7] Agus, F., & Hartono, T., "Implementation of Cyber Security Policy in Indonesia: Challenges and Opportunities", National Security Journal, 8 (3), 2021, pp. 145-162.

3.2. Pancasila Justice

Pancasila as the ideology of the Indonesian state contains fundamental values that are relevant to cybersecurity. Principles such as divinity, humanity, unity, democracy, and social justice can be integrated into cybersecurity policies to ensure inclusive and equitable protection for all citizens. Implementing these values in cybersecurity means ensuring equal access to cyber protection, no discrimination in handling cyber incidents, and efforts to involve all elements of society in maintaining digital security.

3.3. Sustainable Development in Human Resources

Sustainable development in the field of human resources (HR)[8]emphasizes the importance of developing skills and competencies that are relevant to the needs of the times, including in the field of cybersecurity. This includes formal education, vocational training, and ongoing certification programs to ensure that the workforce has the skills needed to address cyber challenges, with efforts to protect a person's interests by allocating a human right to act in the interests of those interests.[9]. The implementation of legal protection can be in the form of prevention (preventive) or in the form of forced action (repressive).[10].

1. Formal education

Indonesia needs to develop a curriculum that is relevant to cybersecurity at all levels of education, from elementary school to college. Elementary and Secondary Schools: Basic materials on cybersecurity can be included in the curriculum of Information and Communication Technology (ICT) subjects or other related subjects. Vocational High Schools (SMK): Expertise programs in the field of information technology can be developed to focus on cybersecurity, so that graduates have basic competencies in the field. Colleges: Study programs related to ICT such as Informatics Engineering and Computer Science[11]need to strengthen cybersecurity courses in its curriculum.

2. Training and Certification

In addition to formal education, training and certification programs for IT professionals need to be improved to ensure that they have skills that are in line with the development of cyber threats. The government can work with professional education and training institutions to organize cybersecurity training

[8] Agung, A., & Santoso, B., "Development of Police Human Resources to Face National Security Challenges", National Security Journal, 11 (2), 2020, pp. 87-100.

[9] Satjipto Rahardjo, Other Sides of Law in Indonesia, Kompas, Jakarta, 2003, p. 121.

[10] Ridwan HR, State Administrative Law, Raja Grafindo Persada, Jakarta, 2014, p. 274.

[11] Dewi, A., & Sukardi, A., "The Influence of Digital Literacy on Cyber Security among Adolescents", Journal of Education and Technology, 9 (3), 2018, pp. 88-101.

programs.[12]relevant and quality. The National Cyber and Crypto Agency (BSSN) can play an active role in developing competency standards and certification in the field of cybersecurity[13]. The private sector can also play a role by providing training programs for its employees to increase cybersecurity awareness and skills.[14].

3. Cyber Law Regulation in Indonesia

Cyber law regulation in Indonesia has undergone significant development in recent years. The rapid development of information and communication technology has driven the need for an adequate legal framework to regulate various aspects related to the digital world, including cybersecurity. One of the main regulations that is the basis for regulating cybersecurity in Indonesia is Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE).

The ITE Law not only regulates electronic information and transactions, but also covers various other aspects related to cyberspace, such as personal data protection, handling cybercrime, and responsible use of information technology. This law aims to provide legal certainty, protection for information technology users, and encourage the growth of the digital economy in Indonesia.

Since its enactment, the ITE Law has undergone several revisions to adapt to new dynamics and challenges that have emerged in the digital era. For example, the changes in 2016 emphasized several articles related to the distribution of electronic information and electronic transactions, as well as strengthening protection for victims of cybercrime. These developments demonstrate the Indonesian government's commitment to dealing with increasingly complex and diverse cyber threats, as well as ensuring that existing regulations remain relevant to technological developments.

More than just a legal document, the ITE Law also requires effective implementation and support from various parties, including the government, law enforcement, the private sector, and the wider community. This collaboration is important to create a safe digital ecosystem, where all parties can participate and contribute positively. In this context, socialization and education about the ITE Law are very important so that the public understands their rights and obligations, and can use information technology wisely and responsibly.

Overall, cyber law regulations such as the ITE Law play a crucial role in maintaining the security and stability of cyberspace in Indonesia. By continuing to evaluate and

[12]Chandra, S., & Ramdani, R., "The Role of Government in Developing Cyber Security Regulations", Journal of Public Administration, 14 (2), 2021, pp. 220-235.

[13]Effendi, M., "Legal Protection of Personal Data in the Digital Era", Journal of Law and Justice, 16 (2), 2019, pp. 187-204.

[14]Basuki, E., "Cyber Security Improvement Strategy in the Digital Era", Journal of Information and Communication Technology, 15 (1), 2020, pp. 50-63.

adjust these regulations, it is hoped that Indonesia can better face cyber challenges and create a safer and more conducive digital environment for all.

Source https://news.okezone.com/read/2018/09/05/512/1946620/usut-judi-online-solo-terkait-jakarta-polda-jateng-gandeng-cyber-crime-bareskrim

The ITE Law regulates various matters related to cybersecurity, such as misuse of information, illegal access, and disruption of electronic systems. However, there is a need to update and refine this regulation to better suit the dynamics of ever-evolving cyber threats.[15].

4. Comprehensive Legal Framework

In addition to the ITE Law, there needs to be a more comprehensive legal framework that focuses not only on the enforcement aspect, but also on prevention and education. The ITE Law is an important first step in dealing with cybercrime and regulating electronic transactions. However, with the development of technology and increasing cyber threats, existing regulations must continue to be refined and expanded in scope.

A comprehensive legal framework should include several key elements. First, there needs to be a more serious effort in preventing cybercrime. This can be done through the development of national cybersecurity standards that can be adopted by various sectors, both public and private. These standards should include best

[15] Graham JH Smith. 2007, Internet law and regulation Thomson Sweet, London, p. 13.

practices in network security, data encryption, and protection against cyberattacks. In addition, the government needs to provide incentives for companies that implement high security standards, as well as conduct regular audits and assessments to ensure compliance.

Second, education and raising public awareness about cybersecurity should be a priority. Intensive education campaigns need to be conducted to raise public understanding about the importance of cybersecurity. Training programs should be aimed not only at IT professionals[16], but also to the general public, including children and adolescents who are vulnerable to cyber threats. Integrating cybersecurity curriculum into the formal education system can help build a generation that is better prepared to face digital challenges.

Third, personal data protection must be strengthened. In addition to existing regulations, additional regulations are needed that regulate in detail how personal data must be protected and how violations of privacy must be handled. Effective monitoring mechanisms and strict sanctions need to be implemented to ensure that personal data is not misused by irresponsible parties.

Fourth, international collaboration is also an important part of a comprehensive legal framework. Cybercrime is often cross-border, so cooperation with other countries in terms of information exchange, law enforcement, and the preparation of international standards is essential. Indonesia must actively participate in international forums that discuss cybersecurity and contribute to the formulation of global policies.

Finally, periodic evaluation and revision of regulations must be carried out to adapt to technological developments and the ever-changing modus operandi of cybercrime. Government, academics, and industry practitioners need to work together to identify gaps in existing regulations and develop innovative solutions.

Overall, in addition to the ITE Law, a more comprehensive legal framework that includes aspects of prevention, education, data protection, international collaboration, and regulatory evaluation is a much-needed step. Thus, Indonesia can be more effective in maintaining cybersecurity and protecting the interests of all its citizens in this increasingly complex digital era., there needs to be a more comprehensive legal framework that not only focuses on the aspect of enforcement, but also on prevention and education.[17].

5. Divine and Human Values in Cyber Security

Godly values can be implemented in cybersecurity by encouraging the use of information and communication technology (ICT) ethically and morally, which

[16] Junaidi, F., "Analysis of the Implementation of the ITE Law in Law Enforcement in Indonesia", Journal of Law and Public Policy, 14 (2), 2020, pp. 77-92.

[17] Decision of the Constitutional Court in case Number 50/PUU-VI/2009 concerning the judicial review of Article 27 paragraph (3) of the ITE Law.

means directing the development and use of technology to support the spiritual and moral values of society. This can be done in various ways, one of which is by limiting and monitoring content that violates religious and cultural norms, such as pornography, hate speech, and material containing violence or fraud. The government and internet service providers must work together to identify and block content that is not in accordance with Godly values. In addition, efforts are also needed to educate the public about the importance of ethics in the use of ICT, including how to interact positively and respect differences in cyberspace.

The development of policies and regulations that support the moral use of ICT is also important. This includes the creation of laws that prohibit the spread of negative content and strict law enforcement against violators. In addition to law enforcement, there needs to be initiatives to create a positive digital environment, such as awareness campaigns on healthy and safe internet use, and the development of applications and platforms that promote religious and moral values.

Furthermore, the education sector has a crucial role in instilling Godly values in the use of ICT. The curriculum in schools can include lessons on digital ethics and social responsibility in cyberspace, so that the younger generation grows up with a strong understanding of how to use technology wisely and morally. In addition, religious communities can also play an active role in providing guidance and advice on the use of ICT in accordance with their religious teachings.

With this comprehensive approach, Godly values can be effectively integrated into cybersecurity, creating a digital ecosystem that is not only technically secure but also in line with the moral and spiritual values of Indonesian society.

moral by limiting content that violates religious and cultural norms[18]. Developing internet usage ethics that are in line with religious values.[19]. Humanitarian Values emphasize the importance of protecting human rights (HAM) in the digital space that ensures equal access to information and technology for all citizens. With this concept, it will create a mechanism for handling cyber incidents that upholds justice and proportionality.[20].

[18] Effendi, M., "Legal Protection of Personal Data in the Digital Era", Journal of Law and Justice, 16 (2), 2019, pp. 187-204.

[19] Andi Hamzah, 1987, Criminal Aspects in the Computer Sector, Sinar Grafika, Jakarta, p. 47.

[20] Dewi, A., & Sukardi, A., "The Influence of Digital Literacy on Cyber Security among Adolescents", Journal of Education and Technology, 9 (3), 2018, pp. 88-101.

Source https://www.google.com/search?q=judi+online+ J8AE&ved=0

6. Cyber Law Regulation and Its Implementation

Cyber legal regulations in Indonesia need to be strengthened and implemented effectively to support cyber security and human resource development.

a. Expansion of Regulation

Expanding the scope of cyber law regulations to cover various aspects, such as personal data protection, critical infrastructure security, and cybercrime. Updating existing regulations to adapt to technological developments and cyber threats.

b. Law enforcement

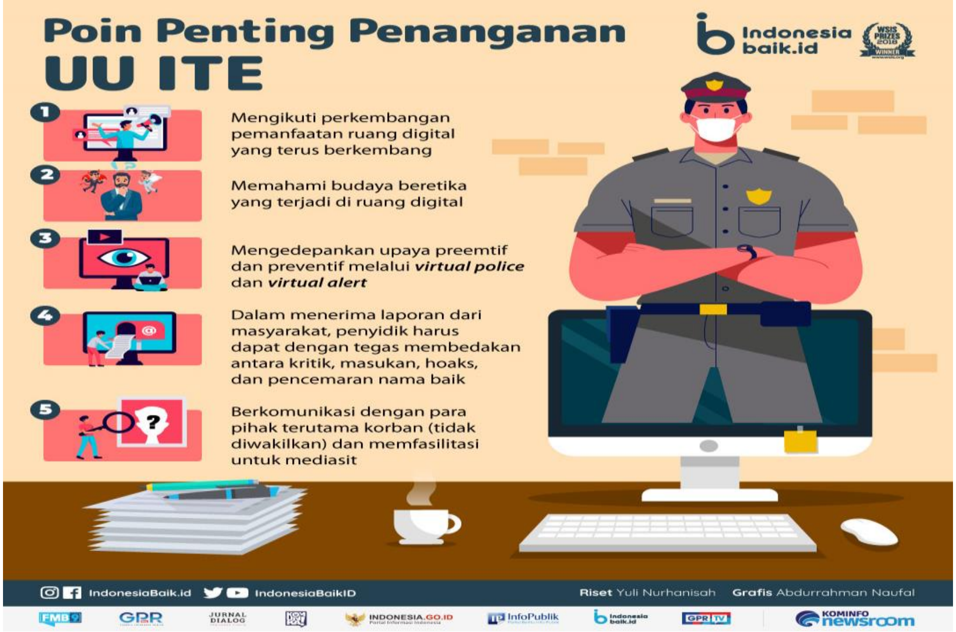
Strengthening law enforcement against cyber law violations by improving coordination between law enforcement agencies to increase the capacity and capability of law enforcement officers in handling cyber cases.

c. Cooperation and Coordination

Improving cooperation and coordination between stakeholders related to cyber security such as government, private sector, and civil society in working to combat cybercrime and sharing information about cyber threats.

7. Government Commitment to Strengthening Cyber Law Regulation

a. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law): The ITE Law is the main legal basis for cybersecurity in Indonesia, regulating various aspects such as electronic transactions, illegal content, and illegal access.



Poin Penting Penanganan UU ITE

1. Mengikuti perkembangan pemanfaatan ruang digital yang terus berkembang
2. Memahami budaya beretika yang terjadi di ruang digital
3. Mengedepankan upaya preemtif dan preventif melalui ***virtual police*** dan ***virtual alert***
4. Dalam menerima laporan dari masyarakat, penyidik harus dapat dengan tegas membedakan antara kritik, masukan, hoaks, dan pencemaran nama baik
5. Berkomunikasi dengan para pihak terutama korban (tidak diwakilkan) dan memfasilitasi untuk mediasit

Source https://indonesiabaik.id/infografis/penerapan-dan-penanganan-kasus-uu-ite

b. Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems: This regulation governs the implementation of electronic systems, including the obligation of organizers to implement an adequate cyber security system.[21].

c. Regulation of the Minister of Communication and Information Technology Number 13 of 2018 concerning Procedures for Organizing Communication and Information Networks: This regulation regulates the procedures for organizing communication and information networks, including aspects of cybersecurity.[22].

d. Regulation of the National Cyber and Crypto Agency Number 13 of 2018 concerning Cyber Security: This regulation regulates the implementation of cyber security, including the national cyber security strategy, the establishment of the National Cyber and Crypto Agency (BSSN), and the role of stakeholders in cyber security.[23].

8. Obstacles and Challenges in the Field

[21] Gunawan, R., "Cyber Security Challenges in Indonesia: A Literature Review", Journal of Information Technology and Information Systems, 13 (1), 2022, pp. 77-92.

[22] Aditya, R., "Analysis of the Implementation of the ITE Law in Cyber Law Enforcement in Indonesia", Journal of Law and Technology, 15 (1), 2019, pp. 45-60.

[23] Hadi, S., & Nurul, L., "Cybersecurity Governance: Best Practices for Indonesia", Journal of Management and Business, 10 (2), 2019, pp. 55-70.

Although cyber law regulations in Indonesia have experienced significant developments, there are still several challenges that need to be overcome, such as:

a. Lag in Following Technological Developments: Rapid technological developments often precede cyber law regulations, so existing regulations need to be updated regularly to ensure their effectiveness.

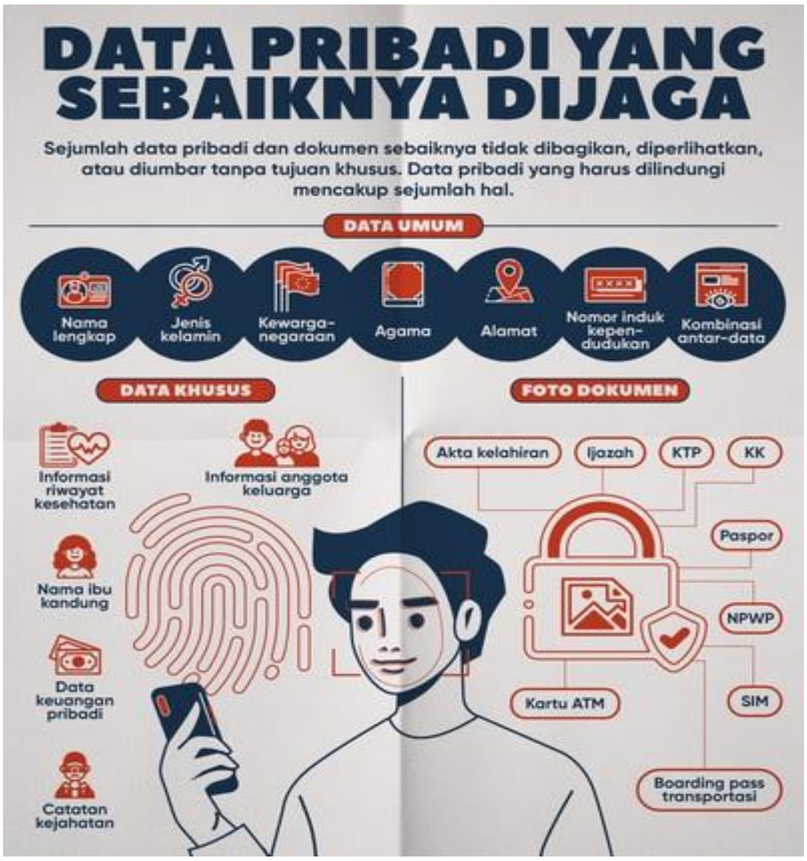
b. Lack of Technical Provisions: Some cyber law regulations are still lacking in detail in regulating technical provisions related to cybersecurity, so they need to be strengthened with more specific technical regulations.

c. Limitations of Law Enforcement: Law enforcement against cyber law violations is still hampered by various factors, such as lack of resources, less than optimal coordination between law enforcement agencies, and a weak legal culture.

9. Synergize Regulation, Pancasila Justice, and Sustainable Development

The synergy of regulations in the cyber legal order, Pancasila justice, and sustainable development is as follows:

a. Personal Data Protection: Cyber legal regulations on personal data protection must be in line with the values of humanity and social justice of Pancasila. This can be done by ensuring that personal data is processed responsibly, transparently, and accountably, and by providing the rights of personal data owners to control their data.



DATA PRIBADI YANG SEBAIKNYA DIJAGA

Sejumlah data pribadi dan dokumen sebaiknya tidak dibagikan, diperlihatkan, atau diumbar tanpa tujuan khusus. Data pribadi yang harus dilindungi mencakup sejumlah hal.

Source cnnindonesia.com%2Ftechnology%2F20211129113617-188-727308%2Finfographic-types-of-personal-data-that-are-best

b. Cybersecurity for Vulnerable Communities: Cyber legal regulations should pay special attention to groups of people who are vulnerable to cyber attacks, such as children, people with disabilities, and the elderly. This can be done by developing digital literacy and education programs that are tailored to their needs, as well as providing easily accessible cybersecurity infrastructure.

c. International Cooperation: Cyber law regulation must support international cooperation in combating cybercrime. This can be done by ratifying international legal instruments related to cybercrime, as well as actively exchanging information and cooperating on law enforcement between countries.

4. Conclusion

Cybersecurity is a crucial issue that needs to be prioritized in Indonesia, especially considering the rapid development of technology and increasing cyber threats. The application of Pancasila values of justice and the principles of sustainable development in cybersecurity policies and human resource development (HRD) can be a strategic solution to realize a safe, fair, and sustainable digital space. The values of Pancasila, which include divinity, humanity, unity, democracy, and social justice, provide a strong moral and ethical foundation for forming policies and regulations that are oriented towards the welfare of all Indonesian people. In the context of cyber law in Indonesia, comprehensive regulation and its effective implementation are the main keys to achieving the desired cybersecurity goals. Good regulation not only protects data and systems from cyber attacks, but also ensures that individual rights are protected and social justice is realized. This requires collaborative efforts from various parties, including the government, private sector, academia, and civil society, to build a cybersecurity ecosystem that is responsive to various challenges and threats in the digital era.

5. References

Anggun, Y., et al. (2022). Analysis of the “Tinder Swindler” Phenomenon on Online Dating Applications Using Lifestyle Exposure Theory. Journal of Criminology, 6(2), 169-170.

Anwar, R. (2018). Strategy for Implementing the ITE Law in Overcoming Cyber Crime. National Security Journal, 6(4), 87-104.

Arief, M. (2020). Cyber Security: Concepts, Threats, and Challenges in the Era of the COVID-19 Pandemic. Indonesian Law Journal, 13(2), 225-238.

Aziz, Z. (2020). Cyber Security Regulation in Indonesia: A Study of the ITE Law and its Impact. Journal of Legislation, 12(1), 33-49.

Darmawan, A., & Setiawan, A. (2019). The Relevance of Criminal Law in Combating Cyber Crime. Journal of Law, 22(1), 1-22.

Dewi, L. (2018). Legal Protection of Personal Data in the ITE Law. Journal of Criminal Law, 16(1), 33-50.

Dewi, S. (2015). Privacy of Personal Data: Legal Protection and Forms of Regulation in Indonesia. De Jure Journal, 15(2), 165.

Fadhil, M. (2018). Consumer Protection in Electronic Transactions According to the ITE Law. Journal of Economic Law, 10(2), 57-72.

Fajar, M. (2018). The Effectiveness of the ITE Law in Combating Cybercrime. Journal of Cyber Law, 9(1), 45-60.

Firmansyah, A. (2019). The Role of the ITE Law in Maintaining National Cyber Security. Defense Journal, 10(2), 151-167.

Hartanto, P. (2017). ITE Law and Challenges of Personal Data Protection. Cyber Law Journal, 5(3), 50-66.

Haryadi, B., & Nugroho, S. (2019). Personal Data Protection in Cyber Law: A Legal Analysis. Journal of Constitutional Law, 26(1), 1-22.

Hidayat, S. (2020). The Impact of the ITE Law on Freedom of Expression in Cyberspace. Social Journal, 9(3), 123-137.

Ismail, R. (2017). Cyber Security: A Review from a Criminal Law Perspective. Journal of Criminal Law, 20(1), 1-22.

Kartika, N. (2019). Challenges of the ITE Law in Dealing with Cybercrime. Journal of Legal Studies, 22(3), 201-218.

Kurniasari, R. (2017). ITE Law and the Right to Privacy in Indonesia. Journal of Constitutional Law, 7(1), 91-108.

Kurniawan, B. (2016). Cyber Security: Concepts, Threats, and Challenges. Journal of Law and Society, 10(1), 1-22.

Lestari, D. (2019). The Impact of the ITE Law on Privacy and Security of Personal Data. Journal of Legal Science, 22(4), 123-139.

Mansur, DMA, & Gultom, E. (2009). Cyber Law, Legal Aspects of Information Technology, 2nd ed. Bandung: Refika Aditama.

Marzuki, A. (2019). Cyber Security: Concepts, Threats, and Challenges. Journal of Law and Technology, 12(1), 1-22.

Maulana, I. (2018). ITE Law: Case Study of Personal Data Misuse. Cyber Law Journal, 8(2), 89-105.

Murti, RK, & Djatmiko, S. (2018). Cyber Security: Concepts, Threats, and Challenges. Journal of Law and Society, 11(2), 1-22.

Nasution, H. (2019). ITE Law and Cybercrime Law Enforcement. Journal of Legal Studies, 21(4), 301-318.

Nugroho, S. (2017). Cyber Security: A Review from a Criminal Law Perspective. Journal of Legal Studies, 20(3), 1-22.

Pramono, A. (2020). Personal Data Protection in the Perspective of the ITE Law. Journal of Law and Technology, 12(3), 123-138.

Pratama, A. (2020). Implementation of the ITE Law in the Digitalization Era: Challenges and Solutions. Journal of Public Policy, 11(3), 78-92.

Pratomo, A. (2019). ITE Law and Cyber Security Challenges in Indonesia. Journal of Public Policy, 14(2), 89-104.

Purwanto, E. (2020). Cyber Law Policy in Indonesia: Implementation of the ITE Law. Journal of Law and Society, 12(1), 67-82.

Putra, B. (2021). Evaluation of the Implementation of the ITE Law in Combating Cyber Crime. Journal of Law, 18(4), 245-262.

Rachman, A. (2021). Case Study of the Implementation of the ITE Law in Cybercrime in Indonesia. Journal of Law, 14(2), 199-216.

Rahmawati, S. (2020). Review of the ITE Law in Handling Cybercrime. Journal of Legal Studies, 11(3), 179-194.

Ridwan, M. (2020). Personal Data Protection Policy in the ITE Law. Cyber Law Journal, 10(2), 123-139.

Rosadi, SD (2017). Principles of Personal Data Protection of Credit Card Customers According to National Provisions and Their Implementation. Jurnal Arena Hukum Universitas Brawijaya, 19(3), 209.

Santoso, H. (2020). Cybercrime Law Enforcement Based on the ITE Law.

Setiawan, I. (2017). Implementation of the ITE Law: A Case Study of Cyber Bullying in Indonesia. Journal of Criminology, 5(2), 99-113.

Setyawan, A. (2019). Legal Protection of Privacy in the ITE Law. Journal of Criminal Law, 15(3), 213-230.

Sudrajat, T. (2020). Cyber Law Policy in Indonesia: Analysis of the ITE Law. Journal of Law and Politics, 14(3), 215-232.

Suhartono, D. (2018). The Role of the ITE Law in Realizing Cyber Security. National Security Journal, 8(1), 75-89.

Supriyanto, H. (2017). Analysis of the Effectiveness of the ITE Law in Addressing Cyber Crime. Journal of Criminology, 6(1), 55-70.

Susanto, T. (2017). Analysis of Personal Data Protection in the ITE Law. Journal of Law and Technology, 7(2), 67-85.

Wibowo, Y. (2019). ITE Law: Protection and Law Enforcement in the Digital Era. Journal of Law and Society, 13(2), 143-160.

Widyastuti, N. (2020). ITE Law and National Cyber Security Challenges. Journal of Law, 14(1), 77-92.

Wijaya, H. (2018). Legal Review of Handling Cyber Crime Based on ITE Law. Journal of Criminology, 8(1), 101-115.

Yulianto, R. (2018). Implementation of the ITE Law in Supervising Internet Content. Journal of Public Policy, 13(2), 111-126.

Zain, M. (2018). The Role of the ITE Law in Handling the Spread of Hoaxes. Social Journal, 7(3), 145-162.