

The Urgency of Privacy Protection in the Era of Digitalization: Challenges and Solutions to Cyber Crime Comparative Legal Studies

**Gracesy Prisela Christy, Maiercherinra Daud, Ni Putu Noni Suharyanti,
Christine Attang, Ade Batti'**

gpchristy@ukipaulus.ac.id

Faculty of Law, Universitas Kristen Indonesia Paulus
Faculty of Accounting , Universitas Kristen Indonesia Paulus
Faculty of Law, Universitas Mahasaraswati Denpasar
Faculty of Law, Universitas Kristen Indonesia Paulus

Article Info

Received: 2024- 03-2024

Revised: 2024-08-20

Accepted: 2024 -11-20

Keywords:

*Legal Protection; Cyber
Security, Personal Data
Leakage, Cybercrime,
Digital Transactions.*

Abstract

The Industrial Era 4.0 in Indonesia is characterized by automation and easy connections. Technological advances have had a major impact on changes in people's habits. According to Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, every person has the right to protection of himself, his family, his honour, honor and dignity, as well as the property he controls. The ease of transactions using online payment media has triggered cyber crimes such as data theft, hacking and system break-ins which are increasing along with the increasing use of digital technology. Cybercrime, such as personal data leakage, identity theft, and financial loss, can have a major impact on society and organizations. The research method used is normative juridical. The conclusion of this research is the effectiveness of implementing laws to protect personal data in Indonesia, how these regulations can ward off cyber crimes which are increasingly widespread in Indonesia based on applicable laws and regulations from the threat of fear of doing or not doing something that is a human right." This can be corrected by adopting several personal data regulations from several developed countries which have proven effective in preventing public data leaks which pose a very high risk to banking and company accounts. The formulation of Effective Regulations on the protection of personal data from Cyber Crime must consider the Essence and Scope of Personal Data, the principles of data protection, the obligations of the managing organization, the rights of Individuals, Supervision and law enforcement and the Harmonization of integration with applicable witnesses such as: administrative fines, Restrictions or Prohibitions on Operations, criminal liability, civil damages, and publication of violations.

I. Introduction

The Industry 4.0 era in Indonesia is characterized by automation and easy connections. In the Industrial Revolution, the word "revolution" means "very rapid change", and "industry" means the effort to carry out production. Thus, the word "revolution" means "very rapid change", and "industry" means "the effort to carry out production. It has changed the way people work; Previously, they worked "manually", now they are moving towards "digitalization" or "automation"

Indonesia was shocked by the emergence of company advertisements that have 25 million customer data and are ready to be sold. The data can generally be classified based on income, type of work and deposit records which range from hundreds of millions. The types of data offered include mobile phone number and complete address data and not infrequently customer banking transaction records. This is traded freely with a variety of price ranges, ranging from a price of one hundred thousand to millions of rupiah. Especially with the obligation for every citizen of Indonesia to register by using NIK personal data in using telecommunication services.

The protection of people's personal data managed by telecommunications is not clearly explained how the form of protection is. When it comes to personal data protection in Indonesia today, the need to protect it is not proportional to the need for society to protect it. This is also recognized by academics. In addition, although there are thirty existing laws related to the protection of personal data, it is still rare for cases to be filed in court regarding the intrusion of a person's privacy.

In this case, there is no specific law regulating personal data in Indonesia, but there are several articles scattered in several laws that reflect personal data protection. This does not provide legal certainty for the public in obtaining protection for their personal data. It is very important to regulate personal data because it regulates the collection, use, disclosure, transmission, and security of personal data. In general, the arrangement of personal data is to ensure that between the protection of individual personal data is necessary because governments and businesses need the collection and processing of data for reasonable and lawful purposes.

Taking into account all the risks and possible breaches that exist, this study will study how Law Number 11 of 2008 concerning Information and Electronic Transactions regulates personal data. The author will investigate whether current regulations are sufficient to provide Indonesia for the Industrial Revolution 4.0 and how Indonesia should create specific regulations to protect personal data.

Talking about the rules for protecting personal data in the implementation of electronic systems will inevitably ignore the responsibilities and responsibilities that electronic system operators have. Chairman of the National Consumer Protection Agency (BPKN) Ardiansyah Parman stated that consumers of electronic platforms often do not receive adequate compensation or protection from electronic system operators in cases of data leaks. This is shown by previous cases where accounts were taken over and hijacked, but

the system operator did not provide compensation to the victims. This means that the electronic system operator is responsible for the protection of the data of platform users as controllers or processors. The protection of personal data in electronic systems is also related to the rights of data subjects. There is no strong legal umbrella that regulates the implementation of electronic systems that comprehensively regulate aspects of personal data protection. As a result, the principles of personal data protection have not been properly applied in the operation of electronic systems.

2. Research Method

In this study, the author uses a normative and empirical juridical approach.

a. Normative Juridical Approach

the approach is based on the main legal material by examining theories, concepts, legal principles and laws and regulations related to this research.

b. The empirical juridical approach

is research by going directly to the field on the object of research to collect primary data obtained directly from the object of research through observation and interviews with related respondents or sources.

3. Results and Discussion

A. Personal data protection in Indonesia's laws and regulations

According to Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, everyone has the right to the protection of themselves, their family, honor, dignity, and property under their control. They are also entitled to a sense of security and protection from the threat of fear of doing or not doing what is considered a human right. Danrivanto Budhijanto stated that "The protection of personal rights or private rights will increase human values, improve the relationship between individuals and their communities, increase independence or autonomy to exercise control and obtain appropriateness, as well as increase tolerance and distance from discriminatory treatment and limit government power."

Data protection is often associated with privacy. Allan Westin first defined privacy as the right of individuals, groups, or institutions to determine whether or not their information will be communicated to others. Therefore, Westin uses the term "privacy information" to define privacy, which relates to personal information. In addition, data protection is a fundamental human right. Some countries have considered data protection to be a constitutional right, or as a "data habeas", a person's right to have their data secured and to be justified in the event of an error with their data. With different histories and cultures, Albania, Armenia, the Philippines, Timor Leste, Colombia, and Argentina have recognized the role of data protection that can facilitate democratic processes and have guaranteed its protection in their constitutions.

In terms of the implementation of electronic systems, there are currently several arrangements in the form of government laws and regulations as well as ministerial regulations, consisting of: a. Law No. 11 of 2008 jo. Law No. 19 of 2016 concerning Electronic Information and Transactions ("ITE Law"); b. Government Regulation No. 80 of 2019 concerning Trade Through Electronic Systems ("PP 80/2019"); c. Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions ("PP 71/2019"); and d. Regulation of the Minister of Communication and Information Technology No. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems.

In the context of Indonesia, Decision No.5/PUU-VIII/2011, the Constitutional Court also wrote that the right to privacy is part of human rights (derogable rights) and the scope of the right to privacy includes information or right to information privacy, also called data privacy (data protection). The delegation regulation of the ITE Law, Government Regulation Number 82 of 2012 concerning Electronic System and Transaction Operators, contains the definition of personal data, namely certain individual data that is stored, maintained, maintained true and protected (Article 1 number 27).

The regulation on personal data protection in the ITE Law is also covered in Article 26 paragraph (1) where the use of information through electronic media must obtain approval from the person concerned and Article 26 paragraph (3) regarding the deletion of information and/or electronic documents that are no longer relevant. In PP 80/2019 itself, regulations on personal data protection are covered in Chapter XI Articles 58-59. Broadly speaking, PP 80/2019 stipulates personal data protection rules on how personal data is stored in accordance with applicable standards. These standards include honest and lawful data collection, accurate and up-to-date data storage, processing as intended, not transmitting personal data outside of Indonesia except with the same protection, and erasure. The rights of data subjects and the concept of data processors are not regulated in the ITE Law and PP 80/2019.

a. Theory of Dignity Justice

Literally, Dignity Justice is made up of two words: "Justice" and "Dignity." KBBI defines "justice" as "just nature" and "dignity" as "the level of human dignity". The Theory of Dignity Justice emphasizes the institutional purpose of the law. In the Theory of Dignity Justice, the values of Pancasila are considered as *volksgeists*, or the soul of the nation, as the basis of law. In the context of legal systems and norms, the theory of Dignity Justice explains the basis of all legal sources from the aspects of certainty, justice, and benefit, as well as the concept of data processors. This theory shows that all existing legal systems and norms are actually based on the values and precepts of Pancasila. [11]

According to the Theory of Dignity Justice, the first precept of Pancasila talks about how the value of morality must be the basis of all legal principles. Then, the second precept states that only laws that uphold human rights (HAM) and recognize human dignity and dignity can create a dignified society. Law contains elements of values that develop in society, according to the third precept of Pancasila. According to the Theory of Dignity Justice, the fourth precept states that the law should prioritize the common good over personal interests. According to the Theory of Dignity Justice, the last precept states that the law should provide equal protection for all people.

Thomas Aquinas proposed justice by distinguishing justice into 2 groups, namely general justice (*justitia generalis*) and special justice. General justice is justice according to the will of the law, which must be fulfilled in the public interest, while special justice is justice on the basis of equality or proportionality. [11] Special justice is divided into 3 types, namely: 1) Distributive justice (*justitia distributiva*), which is justice that is proportionally applied in the field of public law in general. For example, the state will only appoint a person to be a judge, if that person has the ability to become a judge; 2) Commutative justice is justice that equates achievement and counterachievement; 3) Vindicative justice is justice in terms of imposing punishment or compensation in criminal acts. A person is considered fair if he is

sentenced to a corporal penalty or a fine in accordance with the amount of punishment that has been determined for the crime he committed.

b. Legal Certainty Theory

According to Gustav Radbruch, there are three main values in law: justice (*gerechtigheit*), utility (*zweckmassigkeit*), and certainty (*rechtssicherheit*). If the value of certainty is not fulfilled in the legal system, then there will be chaos because the system is not decisive. In the application and enforcement of the law, legal certainty must be guaranteed to ensure consistency and clarity in the implementation of the law without including the subjectivity factor of the existing circumstances or situations. Legal certainty according to Jan Michiel Otto defines it as the possibility that in a given situation:

1. There are clear (clear), consistent and easily obtainable rules published by and recognized by the state;
2. The ruling agencies (the government) apply these legal rules consistently and also submit and obey them;
3. Residents in principle adjust their behavior to the rules;
4. Independent and unthinking judges apply the rules of law consistently when they resolve legal disputes;
5. The judicial decision was concretely implemented.

Legal certainty, according to Sudikno Mertokusumo, is a guarantee that the law must be implemented correctly. Legal certainty requires legal regulation efforts carried out by the authorities and authorities, so that the law has a juridical aspect that can guarantee that the law functions as a regulation that must be obeyed.

To realize the principle of equality before the law without discrimination, legal certainty is also needed. Because the word "certainty" has a close relationship with the principle of truth, in the context of legal certainty, the word "certainty" is something that can be strictly dissected in formal legal logic.

B. Effective regulatory formulation in maintaining the security of personal data privacy in Indonesia and Other Countries

The Internet eliminates the boundaries of place and time, two important legal principles. The chances of crime through computer networks increase when information systems are connected to the Internet. Law enforcement faces difficulties because of this. The punishment of most countries has not reached cyberspace. Today, almost all countries around the world are struggling to create laws that support the Internet.

In the 1945 Constitution of the Republic of Indonesia, Article 28G paragraph (1) states that "Everyone has the right to the protection of himself, family, honor, dignity, and property

under his power, as well as the right to a sense of security and protection from the threat of fear to do or not to do something that is a human right." This right is a development of the right to respect the honor, dignity, and property under his power.

In this case, in Decision No.5/PUU-VIII/2011, the Constitutional Court also stated that the right to confidentiality is one of the human rights (rights that should not be inviolated), and that the scope of the right to confidentiality includes the right to confidentiality of information (also known as the right to data confidentiality). Personal data is defined in Government Regulation Number 82 of 2012 concerning Electronic System and Transaction Operators (ITE), which means certain individual data that is stored, maintained, maintained, and protected in confidentiality (Article 1 number 27). Legislation such as Law No. 7 of 1992 concerning Banking as amended by Law No. 10 of 1998 concerning Banking and Law No. 36 of 1999 concerning Banking have regulated the protection of personal data in Indonesia.

Digital privacy has been a concern of international human rights law, which incorporates ideas from various declarations on human rights and individual freedoms. UN member states agreed to the right to privacy at the UN General Assembly in 2013. Member states are required to be honest and responsible when they obtain personal data. Indonesia's neighboring countries such as Singapore and Australia also have privacy laws. Australia adopted the Privacy Act in 1988, and Singapore adopted the Personal Data Protection Act in 2012. The European Union's General Data Protection Regulation (GDPR) will come into effect in May 2018.

Many types of cybercrime rely heavily on data security systems by cyber security such as privacy issues and the use of cryptographic technology (such as encryption) related to e-commerce applications. Each country has its own laws. For example, the United States banned the export of encryption technology. The laws that apply to the banking system in each country are also different. Law enforcement, or law enforcement, is a different matter.

C. Application of Personal Data Protection Laws of Other Countries that can be Applied in Indonesia

Legal instruments in the digital economy era must meet at least three requirements: (1) global; and (2) involving the economic community and individuals. First, the protection of privacy and personal data must be supported by cross-border arrangements; One example is the rule that the transfer of privacy and personal data to other countries can only be carried out with the specific consent of a country that has the same privacy and personal data protection. Second, in the era of the digital economy, the protection of privacy and personal data must be a top priority.

In the era of the digital economy, with all its unique attributes and rapid development, the country cannot just stand still; Instead, they have to do something more. Third, the

protection of privacy and personal data can encourage people to join society in the digital economy era. To determine the appropriate model of personal data protection arrangements, the authors look at the regulatory models in Asia and the European Union, in particular, as follows:

In general, the regulation in Indonesia can be seen from the personal data privacy ordinance of 1995 (PDPO) Hong Kong which consists of 6 (six) principles: 1) Limitations on Personal Data Collection The collection of personal data is limited to the lawful collection of personal data for purposes directly related to the functions of the collector. 2) Use and Disclosure of Personal Data This principle limits the disclosure of personal data to only for or directly related to the original purpose for which the personal data was collected, or where the data subject expresses consent. 3) Data Quality Obligations and Advice to Third Parties These Principles stipulate that every possible step is taken to ensure that personal data is accurate, including the purposes for which the data is used and any purposes directly related to it, as well as the deletion or use of inaccurate data. 4) Deletion and Destruction of Personal Data: According to this principle, personal data should not be kept for longer than is necessary to achieve a specific purpose—including a purpose directly related to it—or for purposes intended to be used or used in the future. 5) Data Security Obligations: Based on this principle, personal data controllers must do everything they can to prevent accidental access, processing, deletion, deletion, and unauthorized use. 6) In order to ensure transparency of the practices of "User Data", each person (not just the data subject) must have the ability to establish rules and practices relating to personal data, the types of personal data stored in "User Data", and the main purpose of using personal data.

a. EUROPE General Data Protection Regulation (GDPR);

It has been established to protect the right to privacy and regulate the protection of personal data or privacy. This rule is followed by additional rules. The EU regulation GDPR, a new set of laws passed in 2006, came into force on May 25, 2018 in the 28 EU member states (Avenue et al., 2018). The Regulation aims to improve the protection of personal data and ensure that this protection is applied consistently throughout the European Union.

Article 5 of the GDPR of the European Union states that: (a). Personal data must be processed in accordance with the law, fairly, and transparently, (b) obtained in accordance with the purpose for which it is used, clear, specific except for the public, scientific, and research interests, (c) relevant and limited in accordance with the purpose for which it is used, (d) its accuracy is guaranteed, (e) its storage is limited, and (f) its security, integrity, and confidentiality are guaranteed.

Chapter III of the EU GDPR also provides for the right of personal data owners to know how the processing of their personal data is processed, the right to know about who collects their data, the right to amend and delete their data, the right to object to the processing of their

data, and the right to restrict their processing.

The EU GDPR's regulatory model, specifically Chapter VI, indicates an independent supervisory authority, which can be an institution or a commission. This authority is responsible for the arrangement of personal data protection in accordance with established regulations that are independent of outside influences and can serve as a medium for dispute resolution.

b. According to the Personal Data Protection Law Number 709 of 2010 (PDPA Malaysia);

Sections 5 to 12, there are seven principles governing the protection of personal data in Malaysia, namely: general principles of processing based on consent, notification and choice, disclosure, security, data integrity (retention and access). This law is more influenced by the EU Personal Data Protection Regulation than the OECD Guidelines or the APEC Framework. In Part 2 of Personal Data Protection Division 1, Section 5 of the Act regulates how data users manage their data in accordance with the Personal Data Protection Principles. They include general principles, notification and choice principles, disclosure principles, security principles, retention principles, and data integrity principles (Leong & Bakar, 2010).

c. JPCERT/CC (Japan Computer Emergency Response Team Coordination Center) is an operational center to deal with cyber threats in Japan

- **Cyber Security Strategy:** To deal with the growing cyber threats, the Japan government has created a comprehensive cyber security strategy. These strategies include increasing public awareness of cybersecurity, improving the ability to detect and deal with cyber threats, and increasing international cooperation in dealing with cyber threats.
- **National Cyber Security Center (NCSC):** The NCSC is the government agency of Japan responsible for coordinating and overseeing cyber security. The NCSC also serves as an operational center for dealing with cyber threats and provides advice and assistance to organizations and individuals in improving cyber security.
- **Cybersecurity Law:** Japan's strict laws on cyber security regulate the use of information and communication technologies and require companies to take adequate security measures to protect their data and systems. The government of Japan is working with the private sector to improve cybersecurity. This cooperation includes the development of better cyber security technology as well as training and education to increase awareness of cyber security. The goal of this effort is to increase public awareness of cyber threats and the importance of cyber security through

educational programs, training, and awareness campaigns.

- **Research and Development:** Japan has a variety of research and development institutes that focus on developing better cybersecurity technologies. These efforts include the development of threat detection technology, network security systems, and encryption technology.
- **International Cooperation:** Japan is working with other countries to improve global cyber security. These efforts include cooperation in dealing with cyber threats, information sharing, and developing international cyber security standards.
- **Some examples of cyber security systems in Japan are:**

Cyber Security Collaboration Center: The Cyber Security Collaboration Center is a place where government, the private sector, and academia work together to improve cyber security in Japan. This place allows for data exchange, development of cybersecurity technologies, and training and training.

National Institute of Information and Communications Technology (NICT): NICT is a research and development institution that focuses on the development of information and communication technology, including cybersecurity. NICT also serves as a research center to improve cyber security technology.

Overall, Japan's cyber security system is one of the most advanced and successful in the world, with a focus on cooperation, coordination, and the development of better cyber security technologies.

D. Effective Regulatory Formulation for the protection of personal data from Cyber Crime.

Based on the overall description above, the Formulation of Effective Regulations in the protection of personal data must consider several important things below, namely:

a. Essence and Scope of Personal Data:

There needs to be a clear and comprehensive definition of what falls under the category of personal data, including sensitive data such as health, financial, and location information. Scope must include all types of personal data, both structured and unstructured, digital and physical.

b. Data Protection Principles:

Regulations should establish basic principles such as lawful and transparent data collection, restrictions on data use, secure data storage, and individual rights to their

data. These principles must be applied consistently by all parties managing personal data.

c. Obligations of Data Processing Organizations:

Regulations must establish specific responsibilities and obligations for organizations that collect and process personal data, such as implementing adequate security controls, conducting risk assessments, and reporting data leakage incidents. This obligation must be accompanied by strict sanctions for violations.

d. Individual Rights:

Individuals must have clear rights, such as the right to access, correct, delete, or port their personal data. Mechanisms that are easily accessible and understandable by individuals must be provided to exercise these rights.

e. Supervision and Law Enforcement:

There needs to be an independent authority that has the authority to oversee compliance, investigate violations, and provide effective sanctions. Mechanisms for complaints and recovery of losses for individuals should also be available.

f. Integration Harmonization:

Regulations must be able to adapt to technological dynamics and be effectively applied internationally. International cooperation is needed to ensure harmonization and enforcement across jurisdictions.

E. With sanctions that can be applied to violators who are proven to have committed personal data theft as follows;

a. Administrative Denda:

Monetary fines imposed on organizations or individuals found to be in breach of data protection provisions. The value of the fine may vary, depending on the scale of the breach, the amount of data compromised, and the impact caused. Example: GDPR in the European Union can impose fines of up to 4% of an organization's total annual global revenue.

b. Operational Restrictions or Prohibitions:

The supervisory authority may temporarily suspend or prohibit certain data processing activities by the infringing organization. This action aims to force organizations to improve their data security practices.

c. Criminal Liability:

In case of intentional misconduct or resulting in substantial losses, criminal penalties may be imposed for the responsible parties, such as fines or imprisonment. The imposition of criminal penalties aims to provide a deterrent effect and punish serious offenses.

d. Civil Compensation Compensation:

Individuals who are harmed by the leakage of personal data can sue for civil damages against the responsible organization. Compensation can be in the form of reimbursement, loss payments, or other forms of recovery.

e. Publication of Violations:

Supervisory authorities may require the violating organization to publicize the violations that occurred and the corrective actions taken. The goal is to increase transparency and encourage other organizations to be more compliant.

4. Conclusion

The conclusions of this study are as follows:

- a. That the regulation of personal data protection in Indonesia is regulated in the electronic transaction and information law, the constitutional court also stated that the right to confidentiality is one of the human rights (a right that should not be inviolated), and that the scope of the right to confidentiality includes the right to confidentiality of information (also known as the right to data confidentiality). Personal data is defined in Government Regulation Number 82 of 2012 concerning Electronic Systems and Transaction Operators (ITE), which means certain individual data that is stored, maintained, kept correct, and protected (Article 1 number 27), this can certainly be perfected by the arrangements that have been put in place in Europe, Malaysia and Japan by forming a cyber security collaboration center, a research and development institution that focuses on the development of information technology and communication and focus on effective personal data protection.
- b. The formulation of Effective Regulations on the protection of personal data from Cyber Crime must consider the Essence and Scope of Personal Data, the principles of data protection, the obligations of the managing organization, the rights of Individuals, Supervision and law enforcement and the Harmonization of integration with applicable witnesses such as: administrative fines, Restrictions or Prohibitions on Operations, criminal liability, civil damages, and publication of violations

References

- Haris, M. T. A. R., & Tantimin, T. (2022). Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia. *Jurnal Komunikasi Hukum (JKH)*, 8(1), 307-316.
- Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. *Jurnal Wawasan Yuridika*, 5(2), 177-199.
- Detik News. 2017. Begini Data Nasabah Diperjualbelikan. <http://news.detik.com/berita/2-340675/-beginidata-nasabah-diperjualbelikan>. diakses pada 27 November 2018.
- Dewi, Sinta 2017. Model Regulation For Data Privacy InThe Application Of Biometric Smart Card. *Brawijaya Law Journal*. Vol 4.
- Wahyudi. et.al. 2016. Perlindungan Data Pribadi: Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia. Jakarta. Elsam.
- Wahyudi Djafar dan Asep Komarudin, Perlindungan Hak Atas Privasi di Internet- Beberapa Penjelasan Kunci, Elsam, Jakarta, 2014.
- Christy, G. P. (2020). Penanggulangan Cyber-Terrorism Melalui Website Radikal Dalam Perspektif Demokrasi Pancasila. *Paulus Law Journal*, 1(2), 59-71.
- Peter Mahmud Marzuki, 2010, Penelitian Hukum, Kencana, Jakarta.
- Suparyanto dan Rosad (2015). (2020). Strategi Pemerintah Daalam Upaya Meningkatkan Partisipasi Masyarakat Menghadapi Tantangan Industri 5.0. *Suparyanto Dan Rosad (2015)*, 5(3), 248-253.
- Darmodihardjo, D., Hukum, P. F., & Indonesia, F. H. (2019). BAB II Tinjauan Pustaka Teori Keadilan Bermartabat. *Skripsi Universitas Kristen Satya Wacana*, 138-139.
- Sistem, P., Dikaitkan, E., Teori, D., Dan, K., Hukum, K., & Koswara, W. (2022). *Agustus 2022 86 Wenderlin Koswara, Implementasi Peraturan Perlindungan....* 7(2), 86-103.
- Dewi, S. (2017). Model Regulation for Data Privacy in the Application of Biometric Smart Card. *Brawijaya Law Journal*, 4(1), 117-128.
- Mutiara, U., & Maulana, R. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. *Indonesian Journal of Law and Policy Studies*, 1(1), 42.
- Nabila Fitri Amelia, Diva Maura Marcella, Hening Jiwa Semesta, Sabrina Budiarti, & Saskiana Fitra Usman. (2023). Implementasi Artificial Intelligence (AI) Dalam Pembentukan Peraturan Perundang-Undangan Di Indonesia. *Eksekusi : Jurnal Ilmu Hukum Dan Administrasi Negara*, 2(1), 56-70.
- Panjaitan, A. C. D., & Effendi, T. (2019). Simposium Hukum Indonesia. *Simposium Hukum Indonesia*, 1(1), 574-586.
- Christy, G., Lumentut, L., Daud, M., & Baho, D. (2021). The Phenomenon of Terrorism Crime and the Development of Technology in the Perspective of Human Rights. *Proceedings of the First International Conference on Economics, Business and Social Humanities, ICONES 2020*, 4.
- Mikolic-torreira, I., Snyder, D., Price, M., Shlapak, D., Beaghley, S., Bishop, M., Harting, S., Oberholtzer, J., Pettyjohn, S., & Weinbaum, C. (n.d.). *Exploring Cyber Security Policy Options in Australia Australia 's Cyber Security Strategy was designed to address cyber threats affecting national security , including.*
- Ukhanova, E. (2022). Cybersecurity and cyber defence strategies of Japan. *SHS Web of Conferences*, 134, 00159.
- Najib, W., Sulisty, S., & Widyawan. (2020). Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi*, 9(4), 375-384.
- A. Ann (2023). *Civil Law And Criminal Law Aspects Of Hoax News In*. 1-10. Pena Justisia: Media Komunikasi Dan Kajian Hukum, Vol.2, No.22, Desember, 2023
- Gracesy Prisela Christy. (2020). Penanggulangan Cyber-Terrorism Melalui Website Radikal Dalam Perspektif Demokrasi Pancasila. *Paulus Law Journal*, 1(2), 59-71.