Journal of Legal and Cultural Analytics (JLCA)
Vol. 3, No. 3, 2024 : 289 - 298

Cybersecurity Law Exploration: Personal Data Protection in 2023

Titis Pandan Wangi Reformasi[1*], Hasrul Buamona[2]
Fakultas Hukum, Universitas Widya Mataram, Yogyakarta
Corresponding Author: Titis Pandan Wangi Reformasi
reformasi.law2023@gmail.com

ARTICLEINFO

Keywords: Cybersecurity, Law, Data Protection

Received : 17 June
Revised : 02 July
Accepted: 04 August

ABSTRACT

In the ever-evolving digital era, an in-depth exploration of the cybersecurity legal framework is a must. This article examines the background and discussion of personal data protection in 2023. It provides a comprehensive overview of the current cybersecurity landscape, identifying key trends and threats faced by individuals, businesses, and governments. The focus then shifts to regulatory and compliance analysis, exploring potential changes and evaluating the adequacy of current regulations. Next, we outline the latest technologies used in data protection, detailing the role of artificial intelligence (AI) to blockchain in strengthening cybersecurity. Ethical aspects are also highlighted, exploring how efforts to improve security can be balanced with individuals' right to privacy and preventing abuse of power by authorities. Through analysis of key cases in 2023, this article highlights real-world experiences related to personal data breaches. From here, readers can gain a deeper understanding of how cybersecurity law is evolving and addressing the ever-growing threats in this digital era. This article aims to provide a holistic view, educating readers about the current challenges and innovations in personal data protection and contributing to a deeper understanding of the field.

DOI : https://doi.org/10.55927/jlca.v3i3.10376
E-ISSN 2961-807X
https://journal.formosapublisher.org/index.php/JLCA

INTRODUCTION

Data security and confidentiality become very crucial when data has value. For example, protecting people's personal data as citizens is a must because the data can be used by unauthorized parties for criminal activities, which in turn makes the data owner responsible. Aspects of data security involve elements such as privacy (confidentiality), integrity (consistency), authenticity, availability, and access control (Mirna, Judhariksawan, & Maskum, 2023).

Pasal 28G ayat (1) of the 1945 Constitution of the Republic of Indonesia is the philosophical foundation underlying the development of technology in Indonesia. The full nomenclature of Pasal 28G ayat (1) of the 1945 Constitution of the Republic of Indonesia states: "Everyone has the right to protection of themselves, their families, their honor, their dignity, and their property under their control, and has the right to a sense of security and protection from the threat of fear to act or not to act, all of which are human rights." However, navigating the intersection of human rights, cyber law, and online freedoms shows the substantial impact of technology on society's ethical and legal frameworks. Analysis of research groups, most cited works, and keyword trends reveals a picture in which experts from various disciplines collaborate to address the complex challenges and opportunities arising from the digital era. Terms such as "Internet Freedom", "Surveillance", and "Digital Era" reflect widespread concerns in this discussion. This calls for the urgent need to adapt legal frameworks, policy considerations, and ethical guidelines to the dynamic digital context. As technology continues to reshape the landscape, human rights principles must be implemented consistently in the digital realm (Supriandi, Khairunnisa, & Putra, 2023).

LITERATURE REVIEW

The rapid development of technology certainly contributes to the increase in criminal cases, especially hacking crimes which are often referred to as cybercrime. Based on data disclosed by the Ministry of Communication and Information (Kominfo), Indonesia ranks third in the number of cybercrime cases in the world, after Ukraine. Some examples of recent cases involve data leaks from BPJS, BRILife, KPAI, Bank Jatim users, the Police Database, IndiHome customers, PLN users, and others (Firdaus, 2022).

One of the cybercrime activities related to negative content can be classified into several types, including:

1) Violation of confidentiality, integrity, and availability of data and computer systems (violation of confidentiality, integrity, and availability of data and computer systems);
2) Violation related to computers (violation related to computers);
3) Violation related to content or negative content (violation related to content);
4) Violation related to copyright (violation related to copyright).

Thus, the author decided to formulate the problem of this research as follows:

1. How is cybersecurity law related to personal data protection?

METHODOLOGY

This writing applies a qualitative research method with a literature approach, relying on relevant theories to understand the role of cyber security in overcoming negative content information in order to achieve national information resilience. Through this research method, it is expected to produce ideas as a result of data processing and analysis, with a focus on the quality aspect of data sources. Arief Furchan (1992), a leading researcher, explains in his work, "Introduction to Qualitative Research Methods," that qualitative methods are a research process that produces descriptive data, either in the form of speech, writing, or behavior that can be observed from the research subjects themselves.

RESEARCH RESULT AND DISCUSSION

1. Landscape Cybersecurity Tahun 2023

Here are some fundamental elements related to Internet of Things (IoT) and cybersecurity regulations in Indonesia:

a. The National Cyber and Crypto Agency (BSSN) is an organization dedicated to the protection and defense of cybersecurity in the country. BSSN serves as the primary government entity entrusted with the coordination and oversight of cybersecurity initiatives in the Republic of Indonesia. This entity plays a key role in the formation of national policies and laws related to the field of cybersecurity.
b. Indonesia has implemented data protection legislation, embodied in the Draft Law on Personal Data Protection, with the aim of regulating the handling of personal data. These restrictions have a significant impact on Internet of Things (IoT) devices involved in the collection and processing of personal data.
c. Regulatory oversight of telecommunications and IoT connectivity is carried out by the Ministry of Communication and Information (Kominfo). Standards and regulations are set by the regulatory body for IoT connectivity providers.
d. Indonesia has recently implemented a Cybersecurity Law that includes rules regarding the protection of critical information infrastructure (CII). Internet of Things (IoT) devices integrated into critical infrastructure may be subject to different security requirements.
e. Industry-specific regulations exist in Indonesia for many industries, including banking and finance, healthcare, and transportation, which may apply to IoT devices operating in these sectors. Often, these requirements include elements related to cybersecurity and data protection.
f. The Indonesian government, together with industry stakeholders, has created IoT security standards with the aim of promoting the development and implementation of secure IoT devices.
g. Indonesia is actively involved in international efforts and partnerships related to cybersecurity and IoT security, demonstrating its commitment to harmonizing with global efforts aimed at addressing these issues (Adnyana et al., 2023).

2. Latest Technology in Data Protection

Cybersecurity policy, especially in Indonesia, was first initiated in 2007 with the issuance of the Regulation of the Minister of Communication and Information Technology No.26/PER/M.Kominfo/5/2007 concerning the Security of the Utilization of Internet Protocol-Based Telecommunication Networks. This regulation was later revised through the Regulation of the Minister of Communication and Information Technology No.16/PER/M.KOMINFO/10/2010, which was then updated with the Regulation of the Minister of Communication and Information Technology No.29/PER/M.KOMINFO/12/201. One of the provisions stipulated in the regulation is the establishment of ID-SIRTII, an abbreviation of the Indonesia Security Incident Response Team on Internet Infrastructure, which is a team entrusted by the Minister of Communication and Information Technology (Kominfo) to support the supervision of internet protocol-based telecommunications network security. The duties and functions of ID-SIRTII involve monitoring, early detection, early warning of threats and disruptions to the network. This team also coordinates with related parties, both domestically and abroad, in carrying out telecommunications network security tasks based on internet protocols. In addition, ID-SIRTII is responsible for operating, maintaining, and developing database systems, compiling catalogs and syllabi related to the process of securing network utilization, providing information services related to security threats and disturbances, and acting as a contact point with related institutions regarding telecommunications network security based on internet protocols.

ID-SIRTII also has the task of compiling a work program to carry out work related to the security of internet protocol-based telecommunications networks. The current legal framework for cybersecurity in Indonesia is based on Law No. 11 of 2008 on Information and Electronic Transactions, Government Regulation on the Implementation of Electronic Systems and Transactions No. 82 of 2012, and circulars and ministerial regulations. In an effort to ensure legal certainty in the development of cybersecurity, various programs have been implemented, including the initiation of laws and regulations related to cybersecurity such as Law No. 11 of 2008 on Information and Electronic Transactions, Government Regulation on the Implementation of Electronic Systems and Transactions No. 82 of 2012, and the preparation of a national cybersecurity framework (Usman, 2021). In addition, in Presidential Regulation Number 74 of 2017 concerning the E-Commerce Road Map, provisions related to cybersecurity involve 3 programs, 3 activities, and 5 outputs, with the Ministry of Communication and Information and the Coordinating Minister for Political, Legal and Security Affairs as the parties responsible. However, with the presence of the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara : BSSN) as the person in charge of national cybersecurity, the role of the Coordinating Minister for Political, Legal, and Security Affairs was transferred to BSSN. This division of tasks makes Kominfo responsible for the supervision program, increasing public awareness, and developing a national supervision system model. Meanwhile, BSSN is

responsible for the electronic transaction security improvement program (Silalahi, Miftach, & Surryanto, 2019).

Defense management plays a critical role in maintaining the sustainability of a country and its state, especially in developing policies and strategies that can be implemented both in peacetime and wartime situations. Within the framework of defense policy, managerial actions are needed because decisions regarding defense policies are made by various institutions involved in defense-related fields, including cyber defense. The establishment of Presidential Regulation No. 47 of 2023 concerning Cyber Security is an appropriate response to the ever-evolving cyber threats and is necessary to maintain cybersecurity stability. Its intention to address the supporting elements of defense policy, such as national cybersecurity strategy and cyber crisis management, is very good. However, various challenges must be overcome, starting from the strength and readiness of the national cyber infrastructure needed for implementation. This involves the capabilities of national cyber talent and managerial mechanisms implemented by policy makers, because decision-making in formulating cybersecurity policies involves stakeholders in different sectors. Therefore, effective strategic leadership is needed to scan and analyze the strategic impact of cyber threats, identify potential and actual threats, and formulate cyber defense policies and strategies. In addition, it is very important to implement the national cyber defense strategy efficiently and effectively through the implementation of defense policy management operations. In the future, studies can explore the effectiveness of the strategic leadership model in guiding the vision and mission of national cybersecurity regulations to achieve optimal results (Ramadhianto, Samuel, Toruan, Nefo, & Kertopati, 2023).

3. Ethical Challenges in Cybersecurity

The use of technology has become an integral element in modern human life. However, the use of technology also requires the adoption of good ethics to prevent negative impacts on society and the environment. In the context of the Islamic perspective, the application of technology must be carried out by paying attention to ethics that are in accordance with Islamic values and do not conflict with the teachings of the religion (Muin, 2023 in Wahyuni et al., 2015).

According to research by Zubair & Raquib (2020), Islam has a code of ethics in technology, namely as follows:

a) Dimensions and Goals of Islam:
   1) Islam has an absolute dimension and a well-defined goal, namely submission to the transcendent God, Allah.
   2) The ultimate goal of Muslims is to achieve the goal of their existence, namely submission to Allah.

b) Challenges for Muslims with Technology:
   1) Muslims currently face challenges, namely being distracted by technology so that they forget their ultimate goal.

c) Al-Ghazali's Ideas and Professions in the World:
   1) Al-Ghazali and Moad highlight that professions in the world are evolving and interconnected.

2) People lose themselves among these professions, forgetting the roots of the three basic needs: food, clothing, and shelter.

d) Example of a Tree and Branches of Technology:
   1) Moad uses the analogy of a tree to explain the role of technology as branches and divine knowledge as fruits.
   2) The branches (technology) are the means to an end, while the fruits (divine knowledge) are the end.

e) The Problem of Losing Focus on the End Goal:
   1) Problems arise when individuals focus too much on the branches (technology) and forget about the fruits (ultimate goals).
   2) Losing focus on the ultimate goal becomes an obstacle.

f) Role of the Maqasidic Approach:
   1) The Maqasidic Approach acts as a guiding compass for assessing technology in terms of consequences and goals.
   2) It presents a framework with definite goals to safeguard religion, life, intellect, wealth, lineage, and family relationships.

g) Ethical Approach to Social Media Technology in the Islamic Context:
   1) An ethical approach to social media technology requires a value framework that prioritizes fundamental or intrinsic values that are essential to achieving the goals of Islam.
   2) Instrumental or secondary values only help achieve those goals.

h) Examples of Implementation of the Ethical Approach:
   1) The development of features in social media should promote intrinsic values, such as having stronger and more sincere relationships.
   2) The design of social media technology should ensure that it does not harm intrinsic values, such as healthy family relationships.

i) Distinction Between Intrinsic and Secondary Values:
   1) The key to success is having a clear distinction between intrinsic and secondary values.
   2) Technology must support both values, with primary attention to intrinsic value.

4. Important Cybersecurity Cases in 2023

According to Ardiyanti (2016) in (Siti Sarifah Alia, 2014) stated that based on a series of events in recent years, it is clear that the level of cybersecurity in Indonesia is still weak. This phenomenon can be seen from the increasing number of incidents, including one of which was the hacking of a bank customer's debit card data. This incident occurred because of an attempt by hackers to penetrate the bank's customer card security system in mid-May 2014, which reflects significant cybersecurity vulnerabilities in Indonesia. An astonishing fact emerged from a report by the internet monitoring company, Akamai, which revealed that the level of internet crime in Indonesia had doubled. This data places Indonesia in the top position as a country that has the potential to be a target for hacker attacks, replacing China. Of the 175 countries investigated, Indonesia contributed 38 percent of the total targets for hacking

attacks on the internet. This figure continues to increase along with the increase in internet speed in Indonesia.

The impact of the lack of public awareness of data privacy and inadequate cybersecurity in Indonesia can be seen through several incidents of personal data leaks since 2020. Based on research from (CNN Indonesia, 2021), there were around 91 million user data and 7 million Tokopedia merchant data that were leaked and sold on Empire Market. In addition, around 1.2 million Bhineka.com user data were also leaked and sold on the darkweb. The 2014 voter data from the General Elections Commission (KPU) of 2.3 million were also revealed, and finally, the data of 100,002 BPJS Kesehatan participants was also leaked. This does not include the leak of millions of E-KTP data and information from the PeduliLindungi application. In fact, the National Cyber and Crypto Agency (BSSN), which is a cyber defense entity, was not spared from an attempt to leak personal data carried out by a Twitter account named Bjorka (Presidential Decree, 2021). This case of personal data leaks has caused various responses in society, especially in cyberspace (netizens). One of the platforms that records these responses is Twitter. From Twitter, people's responses to a topic create sentiment. This sentiment is interesting to analyze further (Nursiyono & Huda, 2023).

In addition, Indonesia also ranks high in the Southeast Asia region and is ranked 60th globally as a country that is vulnerable to the threat of cyber attack activities in cyberspace. Based on data released by Kaspersky Security Networks in 2022, there were almost 12 million online threats targeting users in Indonesia during the first three months of 2022. During the period from January to March 2022, Kaspersky managed to detect and stop 11,802,558 different cyber attack threats, which were spread via the internet and targeted computers of KSN (Kaspersky Security Networks) users in Indonesia. As many as 27.6% of digital technology users in Indonesia were targeted by cyber attack threats during that period (Astasia Utari et al., 2023).

The impact of industrial growth in the Industry 4.0 era is not only limited to the business and industrial sectors, but also includes security issues. Therefore, countries are faced with the demand to change the perception of security challenges from merely internal problems to global problems. In response, countries must adapt by redefining the legal, political, and strategic frameworks to deal with threats that suddenly emerge and have never been heard of before. The gap in addressing national security issues arises because developing countries have difficulty facing new challenges that arise in the Industry 4.0 era. New concepts such as cybersecurity and cyber law, as well as shifts in global interaction patterns towards regionalism and collective security, open up the potential for diverse risks at the national level. Difficulty in responding to these issues can result in exploitation and isolation of a nation, both in the context of international relations and at the individual level in a society exposed to cyber risks. To address the development of this national security agenda, a comprehensive strategic evaluation is needed. The key to future success is mastery of information technology that continues to develop (Binsar Simorangkir, Tri Legionosuko, 2023).

CONCLUSIONS AND RECOMMENDATIONS

Based on the above statement, it can be concluded that:

The importance of legal aspects in the context of cybersecurity to protect personal data in Indonesia in 2023. It can be seen that regulations and regulations, especially Presidential Regulation No. 47 of 2023, are an important foundation in maintaining cybersecurity and the privacy of individual information. With the National Cyber and Crypto Agency (BSSN) as a coordinating entity, the government is trying to address cyber threats with a more integrated approach.

The importance of legislation that supports the protection of personal data is also emphasized, with the Personal Data Protection Bill as an initiative that can provide a more comprehensive legal framework. This effort is directed at adapting regulations to technological developments and ever-evolving cyber threats. In addition, it also highlights cooperation between the public and private sectors, as well as active community participation, as important elements in facing cybersecurity challenges. Awareness of the risks and the role of each stakeholder is key to creating a robust ecosystem in protecting personal data.

Thus, this exploration of cybersecurity law provides an illustration that joint efforts, sophisticated regulations, and the involvement of all levels of society will be important foundations in maintaining the privacy and security of personal data in Indonesia in 2023.

ADVANCED RESEARCH

In writing this article, the researcher realizes that there are still many shortcomings in terms of language, writing, and presentation considering the limitations of the researcher's own knowledge and abilities. Therefore, for the perfection of the article, the researcher expects constructive criticism and suggestions from various parties.

REFERENCES

Adnyana, I. G., Thalib, E. F., Harum, M. A., Apriliani, M., Nagas, C., & Jawa, W. (2023). *A Discussion of Malware Attacks Targeting Smart Homes and Connected Devices : Investigating Cybersecurity Risks in Everyday Living*. *3*(1).

Ardiyanti, H. (2016). *Cyber-Security Dan Tantangan Pengembangannya Di Indonesia*. 95–110.

Astasia Utari, S., Ardia, V., Fitria, D., Muhammadiyah Jakarta, U., Ahmad Dahlan, J. K., Ciputat Tim, K., & Tangerang Selatan, K. (2023). How an Organization Should Implement Risk Communication in Response to Cyber Attack in Indonesia. *Journal on Education*, *05*(04), 14314–14328.

Binsar Simorangkir, Tri Legionosuko, S. D. W. (2023). Cyber Security Dalam Studi Keamanan Nasional: Politik, Hukum Dan Strategi. *Media Bina Ilmiah*, *9*(20), 409–416.

Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, *4*(2), 23–31. https://doi.org/10.52005/rechten.v4i2.98

Mirna, M., Judhariksawan, & Maskum. (2023). Analisis Pengaturan Keamanan Data Pribadi Di Indonesia. *Jurnal Ilmiah Living Law*, *15*(1), 16–30. Retrieved from https://ojs.unida.ac.id/livinglaw/article/view/4726

Muin, F. (2023). Hukum Islam Dan Teknologi: Adaptasi Hukum Islam Dengan Perkembangan Teknologi. *IDRIS: InDonesian Journal of Islamic Studies*, *1*(1), 97–113. Retrieved from http://yambus-lpksa.com/index.php/IDRIS/article/view/22

Nursiyono, J. A., & Huda, Q. (2023). Analisis Sentimen Twitter Terhadap Perlindungan Data Pribadi Dengan Pendekatan Machine Learning. *Jurnal Pertahanan & Bela Negara*, *13*(1), 1. https://doi.org/10.33172/jpbh.v13i1.1877

Ramadhianto, R., Samuel, T., Toruan, L., Nefo, S., & Kertopati, H. (2023). *Analysis of presidential regulations concerning cyber security to bolster defense policy management*. *4*(January), 84–93.

Silalahi, P. M., Miftach, F., & Surryanto, S. (2019). Sinergitas BSSN Dan Kominfo Dalam Meningkatkan Kesiapan Cyber Security Pada Sektor E-Commerce Di Indonesia. *Peperangan Asimetrik*, *5*(2), 19–30.

Supriandi, Khairunnisa, & Putra, W. U. (2023). Hak Asasi Manusia di Ranah Digital: Analisis Hukum Siber dan Kebebasan Online. *Jurnal Hukum Dan*

HAM Wara Sains, *2*(08), 690–703. https://doi.org/10.58812/jhhws.v2i08.604

Usman, B. F. (2021). Faktor-Faktor Yang Melatar Belakangi Kerjasama Indonesia Dengan Inggris Dibidang Keamanan Siber Tahun 2018. *Moestopo Journal of International Relations*, *1*(2), 107–114. Retrieved from https://journal.moestopo.ac.id/index.php/mjir/article/view/1484

Zubair, T., & Raquib, A. (2020). Islamic perspective on social media technology, addiction, and human values. *Journal of Islamic Thought and Civilization*, *10*(2), 243–267. https://doi.org/10.32350/jitc.102.14