JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 200-214
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Balancing human rights and cybersecurity: Analyzing Indonesia's legal framework

Ampuan Situmeang[1*], Ninne Zahara Silviani[1], Satria Unggul Wicaksana Prakasa[2], David Tan[3], Emiliya Febriyani[1]

[1] *Universitas Internasional Batam, Indonesia*
[2] *Universitas Muhammadiyah Surabaya, Indonesia*
[3] *King's College London, United Kingdom*

*Corresponding Author: *ampuan.situmeang@uib.ac.id*

Abstract

Introduction to the Problem: Indonesia has been continuously developing its legal framework regarding many aspects of digital spaces, including cybersecurity, in the quest of maximizing the potentials of Industry 4.0. However, this rapid development of legal framework must be analyzed thoroughly to make sure that it's in line with the principles of human rights.
Purpose/Study Objectives: Drawing from international standards of human rights, this research focuses on analyzing the cybersecurity legal framework in Indonesia, and how the laws and regulations related to it fare against international standards of human rights.
Design/Methodology/Approach: Using the normative legal research method, this research analyzes secondary data in the form of primary Indonesian and international law sources to evaluate the protection of human rights in the midst of this legal development.
Findings: Findings of this research show that the legal framework in Indonesia does leave many rooms for potential human rights abuse, with normative loopholes and underestimation of potential issues regarding the denial of human rights, within digital spaces.
Paper Type: Research Article
Keywords: Human Rights; Cybersecurity; International Standards

Introduction

In the modern digital landscape, it is imperative to examine the myriad implications that digital transformation has introduced into the lives of individuals (Hutauruk et al., 2023; Setiyawan & Prakasa, 2021). The incorporation of digital technologies into everyday life has yielded substantial benefits for society; however, it has also

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 200-214

introduced a range of challenges that pose potential threats to the interests of numerous users within the digital realm (Tan et al., 2024; Yuspin et al., 2022). Indonesia, Southeast Asia's largest economy (Kusdarjito, 2019), and a rising digital powerhouse (Hermawan et al., 2019), finds itself at the crossroads of this issue. Relevant high-profile cases such as the breach of privacy right in a data breach case involving (Ayu & Nasution, 2023) and the right to freedom of expression (Pane & Siregar, 2024) have also emerged, amplifying the urgency analyze the issue within the broader perspective of cybersecurity as a normative aspect. This is mainly because of the role that cybersecurity plays, which includes safeguarding network data, software, and even physical structures against illicit access or modification that come from the digital spaces (Masyhar & Emovwodo, 2023).

As Indonesia continues its growth as a digital powerhouse in Southeast Asia, socio-economic changes and implications brought by this development have become increasingly important to be analyzed (Kunasegaran et al., 2024). In the context of cybersecurity, there's an ongoing effort to improve digital governance and ensure security of many electronic systems in Indonesia, to improve government surveillance in the digital environment, which can have far-reaching human rights consequences (Fatihah, 2021). It is essential to delve into the real-world scenarios to understand the tangible effects of these laws and the challenges they pose to human rights (Farida, 2022).

A pivotal aspect of this discourse is the compatibility of Indonesia's cybersecurity laws with established international human rights standards (Ishak & Manitra, 2022). The global community, through various treaties and conventions, has set forth principles that nations are expected to adhere to, encompassing rights such as privacy, freedom of expression, and access to information. Analyzing domestic laws using international standards as the benchmark is important, as it can not only contribute to the academic sphere but also highlight profound real-world implications for both policymakers and citizens (Czuryk, 2022).

The existing literatures have highlighted the development of cybersecurity and how it impacts human rights. A study emphasizes the importance of promoting a cybersecurity culture that aligns with human rights principles (Gcaza & von Solms, 2017). The study argues that after a government has made efforts to provide free internet access to its citizens, there is a need for corresponding national cybersecurity efforts to protect individuals' rights. This perspective emphasizes the importance of continued responsibility, where government agencies are responsible in making sure that the infrastructure for the digital age can be used safely.

Another study that focuses on the human right to personal data protection in Indonesia and its global impact argues that the promulgation of new data protection laws in Indonesia is crucial in the era of globalization and emphasizes the need for a paradigm shift in recognizing data protection as a tool for the fulfillment of human

Article History
Submitted 24 April 2024 - Revision Required 11 August 2024 - Accepted 24 October 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 2, 2024, pp. 200-214
P-ISSN: 1412-6834
E-ISSN: 2550-0090

rights (Mendy, 2023). Another study connected the concept of human rights with digital space, by recontextualizing it through cybersecurity (Brantly, 2022). The findings of this study also highlighted how algorithms can be used against the interests of its users, for the benefit of its maker.

The effort to improve cybersecurity significantly affects national interests, individual privacy, and the overall integrity of information systems, which have been manifested mainly through the Electronic Information and Transactions (EIT) legal framework and the most recent one, Law No. 27 of 2022 on Personal Data Protection. This research seeks to analyze the implications of these relevant laws, particularly the cybersecurity provisions, on human rights. The analysis utilizes international standards as the benchmark, to highlight the current balance between cybersecurity measures and the protection of human rights in Indonesia's legislative framework. This analysis will compare the existing Indonesian legal framework with international human rights standards, to identify loopholes that can be used to benefit causes while sacrificing human rights.

Methodology

From the development of literatures, the lack of benchmarking effort to analyze the human rights implications of cybersecurity provisions in Indonesia can be identified as a substantial research gap. The urgency to analyze this research gap is of utmost importance as Indonesia goes deeper into the digital age and continues to become increasingly integrated with the digital environment. This research is done to analyze the existing research gap and shed more light into the human rights developments in Indonesia, within the digital space. For this purpose, this research employs the doctrinal legal research method, by primarily relying on normative analysis of the relevant legal frameworks (Disemadi, 2022). The analysis of this research dives into several conception of human rights, namely as freedom of expression, the right to privacy, right to data protection and rectification, and the right to self-determination.

To support the analysis, this research utilizes the statutory approach, thereby gathering and analyzing secondary data in the form of primary law sources. Normative analysis is typically done by analyzing the relevant legal norms within the existing legal framework, and how those legal norms interact with the key issues of cybersecurity and human rights (Tan, 2021). The data used in this research are collected through literature review and analyzed descriptively, as secondary data. These data include: Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 19 of 2016 on Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, Joint Decree of the Minister of Communication and Information Technology, Attorney General, and Chief of Police No. 229, 154, KB/2/VI/2021 of 2021, Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions, and Law No. 27 of 2022 on Personal Data Protection.

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 15, Issue 2, 2024, pp. 200-214

Results and Discussion

Deficiencies in Indonesia's Cybersecurity Legal Framework and Their Human Rights Implications

The Indonesian cybersecurity legal framework consists of key laws and regulations, including the Electronic Information and Transactions Law (EIT Law). The EIT Law was legislated in 2008, under the code Law No. 11 of 2008. This law was the start of Indonesia's agenda to develop digital spaces in Indonesia, making it a significant piece of legislation in Indonesia's history. cybersecurity in Indonesia. Despite no specific mention of cybersecurity, the law does contain generalized provisions related to data protection, surveillance practices, and internet content regulation, which can all be connected to cybersecurity (Eldem, 2020). It was then revised by Law No. 19 of 2016 on Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (Revised EIT Law), which was legislated to supposedly address issues regarding the first EIT Law (Rohmy et al., 2021).

The EIT Law was enacted as the first broad and far-reaching regulation that governs many aspects of digital transformation, that at the time, was beginning to heavily influence Indonesian society and outlook of Indonesia's future. It provides the foundation for the Indonesian legal system to address many digital issues such as electronic transactions, the proliferation of electronic systems, cybersecurity, and many other relevant aspects of digital governance. It's also made to ensure the protection of individual's rights and the interest of the country, particularly in the growing influence of digital technology.

The provision with the closest conceptual relationship with cybersecurity is the one in Article 26 paragraph (1), which states that *"unless otherwise stipulated by Laws and Regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned."* The Revised EIT Law introduced new provisions into Article 26. These new provisions include the requirement for electronic system operators to delete nonrelevant information at the request of the person concerned based on a court order and to provide the mechanism for deleting electronic information and/or electronic documents that are no longer relevant in accordance with the provisions of laws and regulations.

However, there have been concerns about the EIT legal framework, as it's thought to be capable of silencing individual's voices, and negatively impacting democracy in Indonesia (Setyaningrum et al., 2022). This concern stems from Article 27 Paragraph (3), which states that *"Every Person intentionally, and without the right to distribute and/or transmit and/or make accessible Electronic Information and/or Electronic Documents that contain insults and/or defamation."* This significant implication freedom of expression, became even more alarming as the government doubled down on its criminalization effort, by adding new explanations of the provision in Revised

Article History
Submitted 24 April 2024 - Revision Required 11 August 2024 - Accepted 24 October 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 2, 2024, pp. 200-214
P-ISSN: 1412-6834
E-ISSN: 2550-0090

EIT Law, which explicitly tied this provision with the criminal provision of defamation and/or slander, as governed in the Criminal Law Code.

However, from the cybersecurity point-of-view, concerns can also rise from how this provision might inadvertently undermine cybersecurity foundations. In the process of investigating and prosecuting alleged defamation cases, there may be increased pressure to expose personal data to identify individuals behind potentially defamatory posts. This could lead to weakened data protection practices and create vulnerabilities in systems designed to preserve user privacy and anonymity, even in legitimate contexts such as whistleblowing. Therefore, exceptions need to be made for such cases, to ensure that whistleblowing practices can be accommodated in the digital age, by mainly protecting the right to privacy to ensure the protection of whistleblowers.

The revision of this article came through its explanation, which was supposed to fix the problems regarding the criminalization of hate speech, but ended up strengthening the criminalization possibility with a more detailed explanation and direct mention of defamation as governed by the Criminal Law Code. Instead, the government attempted to fix problem using the Joint Decree of the Minister of Communication and Information Technology, Attorney General, and Chief of Police No. 229, 154, KB/2/VI/2021 of 2021. This step taken by the government didn't address the main issue with the EIT Law, which was the multiple interpretations of Article 27 paragraph (3). In fact, the existence of this Joint Decree indirectly acknowledges that the contents of the EIT Law are indeed problematic, and that the law needs to be revised (Syafaat et al., 2022). There are no other provisions in the EIT Law that has direct correlation with cybersecurity. Along with its revisions, the EIT Law doesn't even mention the word "security" in the context of cybersecurity.

A closely related regulation made to fill this legal gap is Government Regulation No. 82 of 2012 which was replaced by Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions (Government Regulation on Implementation of Electronic Systems and Transactions). This regulation covers both the hardware and the software side of digital technologies with Article 7 and Article 8. Article 7 paragraph (1) which states that *"Hardware used by Electronic System Operators must: a. meet the aspects of security, interconnectivity and compatibility with the system used; b. have technical support services, maintenance, and/or after-sales from the seller or provider; and c. has a guarantee of service continuity."* Article 8 states that *"Software used by Electronic System Operators must: a. guaranteed safety and reliability of operation as it should be; b. ensure continuity of service."*

A problematic issue comes from Article 96 letter a, which states that *"Termination of Access is made to Electronic Information and/or Electronic Documents as referred to in Article 95 with the classification of: a. violates the provisions of laws and regulations."* This provision refers back to other regulations, including the EIT Law and its Criminal

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 200-214

Law Code connection for defamation, which was found to be normatively flawed. As an implementing regulation, this regulation should have explained further on the criteria of the crimes it's related to, within the context of digital spaces. This was also a missed opportunity for the government to clear up the multiple interpretation issue of defamation as governed by EIT Law. This problem is further amplified by the existence of The Chief of Police's Telegram Letter No. ST/339/II/RES.1.1.1./2021, which only applies to the police force in its capacity to handle the legal processes regarding crimes like defamation as governed by EIT Law (Wijayanti & Kharisma, 2022). These developments ultimately showed that the government is too fixated on dealing with traditional issues while ignoring novel problems like cybercrime, which can threaten Indonesians in more aspects of life, including even businesses (Kurniawan, 2022).

The latest legal development in data protection is Law No. 27 of 2022 on Personal Data Protection (PDP Law). This law was made to complete the government's quest in developing legal framework for all aspects of data protection, including cybersecurity. This law has some mentions of cybersecurity issues, through Article 16 paragraph (2) letter e, Article 35, and Article 39. These articles emphasized the responsibility of personal data controller in making sure that personal data its storing is safely stored.

However, the relevant provisions do not regulate anything regarding how the security measures are to be developed and applied. These provisions also do not mention anything regarding third party cybersecurity firms, which can provide an extensive list of cybersecurity services for many personal data controllers (Schwarcz et al., 2022). This is a critical flaw as it exposes the fact that this law is not in line with the reality that most companies who control very large volumes of data often use third-party cybersecurity firms' services, due to the complexities of technical aspects needed to develop a mechanism capable of withstanding many forms of cybersecurity threats. A more concrete set of provisions for cybersecurity might need to be constructed, by grounding it on real-life practice of data controllers, focusing on a more comprehensive compliance for third party cybersecurity firms.

The PDP Law also has some questionable provisions, all of which can raise several questions regarding human rights. One is Article 15, which denies all the rights of the owner of a private data as mentioned by previous articles, for some purposes: for the purpose of national defense and security interests; legal proceedings; public interest in the context of administering the state, the interest of supervising the financial services sector, monetary, payment systems, and financial system stability carried out in the context of administering the state; and statistical interests and scientific research. All of these reasons have the potentials to cause human rights abuse. While purposes such as national defense and security interests, and legal proceedings can be perfectly valid, other purposes remain questionable.

Article History
Submitted 24 April 2024 - Revision Required 11 August 2024 - Accepted 24 October 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 2, 2024, pp. 200-214
P-ISSN: 1412-6834
E-ISSN: 2550-0090

When it comes to "public interest in the context of administering the state", explanation of the article provided a valid reason by detailing key administrative processes. However, problem is found in the explanation of the state financial and monetary surveillance, which mentions banking, capital markets, insurance, financial institutions, pension funds, and financial technology. While these things are under the supervision of Bank Indonesia (BI), the Financial Services Authority (OJK), and the Deposit Insurance Body (LPS), there needs to be limitations as to how much data that a data controller can give to these government agencies. These government agencies are not responsible for data protection, and aren't specifically regulated by the government to protect the personal data of Indonesians. There's a need to streamline data governance to a specific body, much like how financial services are specifically overseen and regulated by the OJK, to ensure better collaborative efforts among relevant government agencies.

Furthermore, the financial bodies mentioned such as banks and insurance companies, also include the private ones. This opens the possibility of unlimited access without supervision, as these bodies aren't necessarily watched by the mentioned government agencies for their data privacy mechanisms. This essentially allows the commercialization of personal data, without the permission of the owners of personal data, which is relevant in this digital age for many digital marketing purposes through data analytics (Christl, 2017). It is a threat to privacy rights as the development of algorithm using data analytics is often times used for purely commercial purposes (Vladeck, 2023).

This issue is even more relevant as privacy concerns regarding Central Bank Digital Currency, an agenda that many countries around the world are currently pushing, are also starting to gain academic attention (Rennie & Steele, 2021). This problem can also be connected to the findings of a study that highlighted the connection of cybersecurity and human rights, where companies can take advantage of algorithm to manipulate human decisions, which can be detrimental on personal level (Brantly, 2022), mainly due to its significant implications on the right to self-determination.

Another purpose that denies the rights of the owner of a private data is statistical interests and scientific research. This is a serious threat to privacy rights as there's no further explanation provided by the PDP Law. Technically, these data fall into the category of secondary data, as it's not the result of a research conducted. Secondary data doesn't have a concrete legal definition, but the definition of primary data can be used to define it, which is governed by Article 40 paragraph (3) Law No. 11 of 2019 on National System of Science and Technology. Primary data is defined as *"authentic raw data in various forms obtained from Research, Development, Assessment and Application activities."* The use of personal data as secondary data for research without the permission its owner is detrimental to privacy rights, because research can take many forms and be conducted for various purposes. These purposes aren't

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 200-214

always in line with the noble pursuit of the betterment of humanity, making some of the existing research in the world of academics unethical (Bülow et al., 2021).

An even more peculiar provision is Article 33 letter a, which states that *"The Personal Data Controller must refuse to grant access to changes to Personal Data to Personal Data Subjects in the event that: a. endanger the security, physical health, or mental health of the Personal Data Subject and/or other people."* This is a rather strange provision because it explicitly states that personal data controller "must refuse" to grant access to changes to personal data. While this doesn't entirely close the possibility of changing medical data that are wrong, the mechanisms behind the process to correct a wrong data such as medical diagnosis or malpractice, can be further complicated by this provision.

The authority to judge on whether or not changing the personal data is dangerous for the person it belongs to is unclear. If there's medical institution's interest involved, the denial of this right can instead cause grave consequences to patients, as the medical institution can look for a way to protect its reputation, at the cost of the patient's right to data control and rectification. In the long run, this can damage the potential of using Big Data for medical research purposes, as incorrect data can significantly discredit research findings (Hoffman, 2018). More importantly, this can undermine data integrity that is already established by the existing cybersecurity system, rendering the efforts to enhance cybersecurity useless.

Examining Indonesian Cybersecurity Laws Through the Lens of International Human Rights Standards

The expansion of many activities into the digital world has raised the importance of the rights to access the internet, have digital privacy, and be protected from cyber threats. With the rise of cyberattacks as a significant threat to many digital activities (Masyhar et al., 2023), cybersecurity becomes a key defense mechanism that can either protect individuals from undue surveillance or, if misused, can facilitate state or corporate surveillance (Disemadi & Budi, 2023). States have a responsibility to protect the safety and human rights of their citizens, both offline and online. This includes ensuring a secure digital environment where rights such as freedom of expression and privacy are upheld.

Human rights are universal and inalienable. with primary international instrument such as the Universal Declaration of Human Rights (UDHR), adopted by the United Nations General Assembly in 1948, giving basic principles that all nations must abide by (Suherman et al., 2023). Other significant instruments include the International Covenant on Civil and Political Rights (ICCPR) (Sullivan, 2016) and the International Covenant on Economic, Social and Cultural Rights (ICESCR) (Kwan, 2022).

It is crucial to ensure that cybersecurity measures and human rights protections, such as privacy and free expression, coexist without undermining one another. For this, there's a need to contextualize cybersecurity within the broader contestation over the

Article History
Submitted 24 April 2024 - Revision Required 11 August 2024 - Accepted 24 October 2024

JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 200-214
P-ISSN: 1412-6834
E-ISSN: 2550-0090

world order, international law, and human rights (Priyanto & Sardi, 2021). A comparative analysis of the Indonesian legal framework for cybersecurity and international standards of human rights is needed to analyze the adequacy of human rights protection for digital spaces in Indonesia.

Table 1. Benchmark Analysis of Indonesian Legal Framework for Cybersecurity Through the Lens of International Laws

Indonesian Primary Law Sources	Implication of Problems with International Human Rights Standards
EIT Law (Article 27 paragraph (3))	Universal Declaration of Human Rights (UDHR) (Article 19) International Covenant on Economic, Social and Cultural Rights (ICESCR) (Article 1 paragraph 1)
Government Regulation on Implementation of Electronic Systems and Transactions (**Article** 96)	Universal Declaration of Human Rights (UDHR) (Article 19)
PDP Law (Article 16 paragraph (2) letter e, Article 35, and Article 39)	Universal Declaration of Human Rights (UDHR) (Article 12) International Covenant on Civil and Political Rights (ICCPR) (Article 17)
PDP Law (Article 15 paragraph (1) letter d)	The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (Article 9 paragraph 2 letter a)
PDP Law (Article 15 paragraph (1) letter e)	The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (Article 9 paragraph 3) The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (Article 6)
PDP Law (Article 33 letter a)	General Data Protection Regulation (GDPR) (Article 5 paragraph 1 letter (d)) General Data Protection Regulation (GDPR) (Article 16)

Sources: Indonesian and international primary law sources

The EIT Law, particularly the provision in Article 27 paragraph (3), has long been criticized for its possible abuse of freedom of speech. This human right is enshrined in Article 19 of the UDHR (Rianarizkiwati, 2022). The article states that *"everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas*

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 15, Issue 2, 2024, pp. 200-214

through any media and regardless of frontiers." When the abuse is done for political purposes, this can also go against the provision of Article 1 paragraph (1) of the ICESCR, which states that *"All peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development."* The same implication of problem is also found in Article 96 Government Regulation on Implementation of Electronic Systems and Transactions. Both of these domestic provisions could lead to self-censorship and arbitrary content blocking, potentially stifling free expression and public discourse, thereby undermining the fundamental rights the relevant international instruments mentioned.

While PDP Law, the latest legal development for cybersecurity in Indonesia, is known to be designed based on EU's GDPR (Hutauruk et al., 2023; Setiyawan & Prakasa, 2021), there's no guarantee that the law can meet GDPR's standard, not just in the context of cybersecurity, but also in the context of human rights. Article 16 of the PDP Law has the same implication of problem as the previously mentioned articles, along with Article 17 of the ICCPR, which states that *"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."*

Article 15 paragraph (1) letter d and e also have been found to be problematic when analyzed through to The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (Article 9 paragraph 2 letter a and paragraph 3 respectively. Article 9 paragraph 2 of the CETS No. 108 states that *"Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of: a protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences."* Although Article 15 paragraph (1) letter d of the PDP Law essentially has the same intention with this, the provision in PDP Law doesn't mention the context of which the denial of rights of the personal data owner can be denied, and only mentions the financial bodies that can take these data, under the supervision of monetary government agencies that don't have the authority and capacity to analyze privacy issues. The vague cybersecurity framework displayed by the relevant Indonesian legal framework may lead to inconsistent implementation across different sectors, creating security gaps that malicious actors could exploit.

Article 9 paragraph 3 of the CETS No. 108 states that, *"restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects."* Article 15 paragraph (1) letter e of the PDP Law completely ignores the potential risk and assumes that this provision can be implemented without

Article History
Submitted 24 April 2024 - Revision Required 11 August 2024 - Accepted 24 October 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 2, 2024, pp. 200-214
P-ISSN: 1412-6834
E-ISSN: 2550-0090

mentioning the importance of making sure that there's no risk involved in processing the personal data. This is also not in line with Article 6 of the CETS No. 108, which states that *"Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."* Such broad provision in support of government access could discourage whistleblowing and investigative journalism, potentially masking corruption or human rights abuses.

Furthermore, Article 33 letter a of the PDP Law is also found to be problematic when analyzed through the human rights standard provided by the GDPR, particularly Article 5 paragraph 1 letter (d) and Article 16 on the right to rectification. Article 5 paragraph 1 letter (d) states that *"(personal data shall be) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.* Article 16 states that *"The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."* As identified previously, Article 33 letter a of the PDP Law goes against the very principles implied by the provisions set by the GDPR. As cybersecurity systems are established to ensure data safety and protect the rights of individuals on their own data, a direct breach to the right to data control and rectification can not only render the cybersecurity systems useless, but also undermine their integrity due to this loophole of unethical data processing practice.

Conclusion

Analysis of this research found that beneath all the relevant provisions for cybersecurity, there's a significant imbalance between ensuring the application of cybersecurity measures and the protection of a number of human rights. The normative issues are also found to be not up to the standards of human rights set by key international instruments. This ultimately raise the urgency for legal reforms, particularly in the areas that overlap with issues directly connected with certain human rights. By drafting a legislation that specifically governs the key aspects of cybersecurity, Indonesia can have a legal framework that is leaning more towards the technical aspects of cybersecurity, leaving little to no room for potential loopholes. It's also worth revising the Indonesian legal framework for data protection, as it has its own weaknesses and even breaches of human rights, which can all undermine the broader effort to enhance cybersecurity. The limitation of this research is the technical analysis of cybersecurity, such as algorithm manipulation and other data-stealing mechanisms that are constantly evolving, which requires an in-depth from the field of computer science in collaboration with the field of law.

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 15, Issue 2, 2024, pp. 200-214

Acknowledgement

The authors would like to extend their sincere gratitude to Universitas Internasional Batam and Universitas Muhammadiyah Surabaya for their invaluable contributions to the publication of this article. We deeply appreciate the support provided throughout the research process. Our heartfelt thanks also go to all individuals and parties who offered their assistance, both morally and materially, making significant contributions to the successful completion of this article.

Declarations

Author contribution	:	Author 1: Conceptualized the research topic, designed the study framework, and wrote the introduction, literature review, conducted data analysis, and wrote the majority of the manuscript; Author 2: Conducted data collection and analysis, and contributed to the discussion section; Author 3: Contributed to the literature review supporting the theoretical framework of this article and assisted in the text drafting process; Author 4: Supported the study's methodology and contributed to the results section; Author 5: Conducted data collection and analysis, and contributed to the discussion section.
Funding statement	:	-
Conflict of interest	:	The authors declare no conflict of interest.
Additional information	:	No additional information is available for this document.

References

Ayu, S. S., & Nasution, M. I. P. (2023). Analisis kebocoran data privacy pada e-commerce tokopedia. *JUEB: Jurnal Ekonomi Dan Bisnis*, *2*(3), 21–24. https://doi.org/10.57218/jueb.v2i3.716

Brantly, A. (2022). Utopia lost – human rights in a digital world. *Applied Cybersecurity & Internet Governance*, *1*(1), 25-43. https://doi.org/10.5604/01.3001.0016.1238

Bülow, W., Godskesen, T. E., Helgesson, G., & Eriksson, S. (2021). Why unethical papers should be retracted. *Journal of Medical Ethics*, *47*(12), 1-6. https://doi.org/10.1136/medethics-2020-106140

Christl, W. (2017). Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. In *Cracked Labs, https://crackedlabs.org/en/corporate-surveillance*.

Czuryk, M. (2022). Restrictions on the exercising of human and civil rights and freedoms due to cybersecurity issues c. *Studia Iuridica Lublinensia*, *31*(3), 31–43. https://doi.org/10.17951/sil.2022.31.3.31-43

Disemadi, H. S. (2022). Lenses of legal research: A descriptive essay on legal research methodologies. *Journal of Judicial Review*, *24*(2), 289–304.

Article History
Submitted 24 April 2024 - Revision Required 11 August 2024 - Accepted 24 October 2024

P-ISSN: 1412-6834
E-ISSN: 2550-0090

https://doi.org/10.37253/jjr.v24i2.7280

Disemadi, H. S., & Budi, H. S. (2023). Enhancing trade secret protection amidst e-commerce advancements: Navigating the cybersecurity conundrum. *Jurnal Wawasan Yuridika*, *7*(1), 21–45. https://doi.org/10.25072/jwy.v7i1.608

Eldem, T. (2020). The governance of Turkey's cyberspace: Between cyber security and information security. *International Journal of Public Administration*, *43*(5), 452–465. https://doi.org/10.1080/01900692.2019.1680689

Farida, Q. 'Aini S. (2022). Implementation of assets confiscation in the corruption crime in Indonesia as additional criminals based of human rights perspective. *International Journal of Social Science and Human Research*, *5*(8), 3486–3491. https://doi.org/10.47191/ijsshr/v5-i8-18

Fatihah, C. Y. N. (2021). Establishing a legitimate Indonesian government electronic surveillance regulation: A comparison with the U.S legal practises. *Indonesia Law Review*, *11*(3), 231–248, https://scholarhub.ui.ac.id/ilrev/vol11/iss3/6/.

Gcaza, N., & von Solms, R. (2017). A strategy for a cybersecurity culture: A South African perspective. *Electronic Journal of Information Systems in Developing Countries*, *80*(1), 1–17. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x

Hermawan, I., Budiyanti, E., & Rivani, E. (2019). The impact of information and communication technology (ICT) on ASEAN trade flow. *Proceedings of the International Conference on Trade 2019 (ICOT 2019)*, 180–184. https://doi.org/10.2991/icot-19.2019.38

Hoffman, S. (2018). Big data analytics: What can go wrong. *Indiana Health Law Journal*, *15*(2), 227–246, https://doi.org/10.18060/3911.0048.

Hutauruk, R. H., Sudirman, L., Disemadi, H. S., & Tan, D. (2023). Convergence of consumer protection, investment law, and cybersecurity: An in-depth analysis of three-way legal intersections in investment app. *JURISDICTIE*, *14*(1), 127–153. https://doi.org/10.18860/j.v14i1.21180

Ishak, N., & Manitra, R. R. M. (2022). Constitutional religious tolerance in realizing the protection of human rights in Indonesia. *Journal of Human Rights, Culture and Legal System*, *2*(1), 31–44. https://doi.org/10.53955/jhcls.v2i1.24

Kunasegaran, M., Xing, Y., & Kunjiapu, S. (2024). Unveiling the impact of the digital economy on future employment: A comparison study among selected Southeast Asian Countries. *International Journal of Academic Research in Business and Social Sciences*, *14*(5), 1829–1840. https://doi.org/10.6007/IJARBSS/v14-i5/21725

Kurniawan, I. G. A. (2022). Digitalization of business law: Urgency and orientation of the industrial Revolution 4.0 and Society 5.0. *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, *5*(2), 253–265. https://doi.org/10.24090/volksgeist.v5i2.6847

Kusdarjito, C. (2019). China's belt and road initiatives and Indonesia's maritime fulcrum: Building scenarios for economic multipolarity in South East Asia. *Proceedings of the International Conference on Banking, Accounting, Management, and Economics (ICOBAME 2018)*, 42–47. https://doi.org/10.2991/icobame-18.2019.9

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 15, Issue 2, 2024, pp. 200-214

Kwan, T. H. (2022). Enforcement of the use of digital contact-tracing Apps in a common law jurisdiction. *Healthcare (Switzerland)*, *10*(9), 1–8. https://doi.org/10.3390/healthcare10091613

Masyhar, A., & Emovwodo, S. O. (2023). Techno-prevention in counterterrorism: Between countering crime and human rights protection. *Journal of Human Rights, Culture and Legal System*, *3*(3), 625-655. https://doi.org/10.53955/jhcls.v3i3.176

Masyhar, A., Utari, I. S., Usman, U., & Sabri, A. Z. S. A. (2023). Legal challenges of combating international cyberterrorism: The NCB Interpol Indonesia and global cooperation. *Legality : Jurnal Ilmiah Hukum*, *31*(2), 344–366. https://doi.org/10.22219/ljih.v31i2.29668

Mendy, O. (2023). Analyzing human right to personal data protection in Indonesia amidst its high global impact. *International Journal of Social Science And Human Research*, *6*(1), 58–62. https://doi.org/10.47191/ijsshr/v6-i1-09

Pane, R. S., & Siregar, K. M. (2024). Dialektika hukum kebebasan mengeluarkan pendapat: Kritik vs Hinaan. *Al-Adl : Jurnal Hukum*, *16*(1), 1–16. https://doi.org/10.31602/al-adl.v16i1.10238

Priyanto, G. A., & Sardi, M. (2021). The urgency of protecting netizen in freedom of speech on social media. *Media of Law and Sharia*, *2*(1), 76–91. https://doi.org/10.18196/mls.v2i1.11480

Rennie, E., & Steele, S. (2021). Privacy and emergency payments in a pandemic: How to think about privacy and a central bank digital currency. *Law, Technology and Humans*, *3*(1), 6–17. https://doi.org/10.5204/lthj.1745

Rianarizkiwati, N. (2022). Ius constituendum hak atas pelindungan data pribadi: Suatu perspektif hak asasi manusia. *Jurnal Hukum Sasana*, *8*(2), 324–341. https://doi.org/10.31599/sasana.v8i2.1604

Rohmy, A. M., Suratman, T., & Nihayaty, A. I. (2021). UU ITE dalam perspektif perkembangan teknologi informasi dan komunikasi. *Dakwatuna: Jurnal Dakwah Dan Komunikasi Islam*, *7*(2), 326. https://doi.org/10.54471/dakwatuna.v7i2.1202

Schwarcz, D. B., Wolff, J., & Woods, D. W. (2022). How privilege undermines cybersecurity. *SSRN Electronic Journal*, 1-61. https://doi.org/10.2139/ssrn.4175523

Setiyawan, R., & Prakasa, S. U. W. (2021). Indonesian online shopping practices in the COVID-19 Pandemic era: A study of culture and cybersecurity law. *Jurnal Hukum Novelty*, *12*(01), 29. https://doi.org/10.26555/novelty.v12i01.a16944

Setyaningrum, W., Morana, A. C., Vaizi, K. N., Damarina, R., Akbar, S. A., & Oktasari, S. (2022). Anticipation of the ITE Law and reconciliation of its forms freedom of expression through the e-hights website. *Jurnal Hukum Novelty*, *13*(2), 266–276. https://doi.org/10.26555/novelty.v13i2.a23799

Suherman, A. M., Yuliantiningsih, A., Afwa, U., Utami, N. A. T., & Basworo, H. (2023). Balancing sustainable fisheries and human rights protection: Indonesian experiences. *International Journal of Global Community*, *6*(2), 137–148,

Article History
Submitted 24 April 2024 - Revision Required 11 August 2024 - Accepted 24 October 2024

P-ISSN: 1412-6834
E-ISSN: 2550-0090

https://journal.riksawan.com/index.php/IJGC-RI/article/view/151.

Sullivan, C. (2016). Digital citizenship and the right to digital identity under international law. *Computer Law & Security Review*, *32*(3), 474–481. https://doi.org/https://doi.org/10.1016/j.clsr.2016.02.001

Tan, D. (2021). Metode penelitian hukum: Mengupas Dan mengulas metodologi dalam menyelenggarakan penelitian hukum. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *8*(5), 1332–1336, http://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/5601.

Tan, D., Disemadi, H., & Sudirman, L. (2024). Decoding the Special purpose acquisition companies: A new frontier in tech start-up financing. *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)*, *11*(1), 97-121. https://doi.org/10.22304/pjih.v11n1.a5

Vladeck, D. C. (2023). Consumer protection in an era of big data analytics. *Ohio Northern University Law Review*, *42*(2), 493–515, https://digitalcommons.onu.edu/onu_law_review/vol42/iss2/5/.

Wijayanti, P. T., & Kharisma, D. B. (2022). Analisis penerapan undang-undang ITE ditinjau dari legal drafting theory oleh teori formil Rick Dikerson. *Souvereignty*, *1*(4), 578–584. https://doi.org/10.13057/souvereignty.v1i4.72

Yuspin, W., Wardiono, K., Budiono, A., & Gulyamov, S. (2022). The law alteration on artificial intelligence in reducing Islamic bank's profit and loss sharing risk. *Legality : Jurnal Ilmiah Hukum*, *30*(2), 267-282. https://doi.org/10.22219/ljih.v30i2.23051