

CHAPTER I

INTRODUCTION

A. Background

The development of global society in the 21st century is marked by increasingly intensive integration of digital technology in various sectors of life. The digital revolution has fundamentally changed the patterns of interaction between individuals, organisations and countries. These changes have not only affected economic and social aspects, but also had a major impact on international legal and political governance. In this context, the law is required to adapt quickly in order to regulate the new dynamics arising from the massive use of information technology, communication, and digital data throughout the world.

Digital technology has now become a global phenomenon that has a broad impact on almost all aspects of human life, including in the context of international relations. Digitalisation is not merely understood as technical progress, but rather a fundamental transformation that brings countries into a new network of interconnections without geographical boundaries. The presence of technologies such as artificial intelligence (AI), the Internet of Things (IoT), big data, and cloud computing has changed the way countries interact, trade, and manage human resources and information.¹ These changes have significantly shaped a new order in increasingly complex and dynamic international relations.

¹ Vera Maria, Sherla Dara Rizky, & Aisar Muhammad Akram, 2024, Mengamati Perkembangan Teknologi dan Bisnis Digital dalam Transisi Menuju Era Industri 5.0, Wawasan: Jurnal Ilmu Manajemen, Ekonomi dan Kewirausahaan, Vol. 2 No. 3, p. 176-179

This has extended to the realm of international relations, which includes global trade, digital diplomacy, cyber security, and cross-border law enforcement. Digitalisation has facilitated faster and more efficient interactions between countries, but on the other hand, it has also presented new challenges, such as an increase in cross-border cybercrime, threats to data privacy, and difficulties in law enforcement.

These changes have significantly shaped a new order in international relations that is increasingly complex and dynamic. This has extended to the realm of international relations, which includes global trade, digital diplomacy, cyber security, and cross-border law enforcement. Digitalisation has facilitated faster and more efficient interactions between countries, but on the other hand, it has also presented new challenges, such as the rise of cross-border cybercrime, threats to data privacy, and difficulties in law enforcement in virtual spaces.² This situation highlights the need for a responsive and innovative international legal response, prioritising the strengthening of global regulations and collaboration between countries in addressing increasingly complex cross-border issues.

On the other hand, developments in digital technology also pose new challenges to the protection of individual rights. The use of surveillance technology and data monitoring systems by various parties, including governments and companies, has raised concerns about the potential misuse of personal data and violations of privacy rights in the digital space. Reports from Freedom House show that

² Diana Setiawati, Ibrahim Sholahudin, Nur Isa Herda A, Harjuna Nurfattah, Nilam Arum Sari, & Sabrina Diyang A.P., 2023, *Transformasi Teknologi dalam Hukum Dagang Internasional: Regulasi dan Penyelesaian Sengketa di Era Digital*, Borobudur Law and Society Journal, Vol. 2 No. 5, p. 222

more and more governments are strengthening their control over technology companies and forcing them to comply with online censorship and surveillance policies.³ This finding reflects a global trend in which freedom of expression and privacy rights on the internet are increasingly under threat. This situation illustrates two sides of technological progress: on the one hand, technology provides enormous benefits to modern life, but on the other hand, it also expands the potential for state surveillance of its citizens. This situation highlights the importance of establishing international legal instruments that not only focus on combating cybercrime, but also ensure the protection of human rights, particularly the right to privacy, in the digital age.

In the context of international law, cybercrime has become one of the main challenges in the era of digital globalisation due to its transnational nature. The development of information and communication technology has created a cyberspace that is no longer limited by national borders, allowing criminals to carry out attacks from anywhere without having to be physically present at the victim's location.⁴ This situation demonstrates that national legal systems are inadequate to deal with cybercrime that crosses national borders. Differences in regulations between countries and the absence of strong international agreements create legal loopholes that are often exploited by criminals. Therefore, closer international cooperation is needed through the establishment of global legal instruments, harmonisation of policies between countries, and

³ Freedom House, "Freedom on the Net 2021", p. 2.

⁴ Clara Ignatia Tobing, Tiofanny Marilyn Surya, Liris Roesa Selvias, Stepania Rehulina Girsang, Putri Berliana Azzahra, Lustri Yolanda Purba, Mahezha Agnia Putera, dan Nurrahman Rusmana, 2024, "Globalisasi Digital dan Cybercrime: Tantangan Hukum dalam Menghadapi Kejahatan Siber Lintas Batas," *Jurnal Hukum Sasana*, Vol. 10, No. 2, p. 107

collaboration in law enforcement so that cross-border cybercrime can be dealt with effectively and fairly.

The inability of national legal systems to deal with cross-border cybercrime is the main reason for the need for integrated international regulations. In the last two decades, the issue of cybercrime has become one of the important agendas in international legal forums. This dynamic shows that countries are beginning to realise that cyber threats cannot be dealt with unilaterally, but require a collaborative and cross-jurisdictional approach to maintain legal stability and protect human rights in the digital space. These countries face challenges in the form of differing legal definitions, law enforcement procedures, and uneven technological capabilities. These limitations make it difficult to effectively investigate, prosecute, and extradite cybercriminals. Therefore, international cooperation and the harmonisation of norms through international legal instruments are essential to overcome these obstacles and optimise the global fight against cybercrime.⁵

International efforts to regulate cybercrime actually began in the early 2000s with the birth of the Budapest Convention on Cybercrime (2001), which was adopted by the Council of Europe as the first international instrument regulating cross-border cybercrime. However, due to its regional nature and lack of compliance from non-European countries, in practice there are still various loopholes in its implementation.⁶ Thus, con, the United Nations drafted the UN Convention on Cybercrime as a step to strengthen existing

⁵ Ibid., p. 108

⁶ Heryanto Kawisen, Rafael Agrerio Firera, Alpon Siyus, dan Pelagia Melati, (Oktober 2025), "Analisis Efektivitas dan Tantangan Hukum Internasional dalam Penanggulangan Kejahatan Siber Lintas Negara secara Global," JATI (Jurnal Mahasiswa Teknik Informatika), Vol. 9, No. 5, p. 8613

international legal instruments. This convention contains provisions on the harmonisation of definitions of cybercrime, procedures for cooperation between countries, and mechanisms for information exchange and joint investigations. This initiative is an important milestone in building a multilateral framework that is more adaptive to technological developments in the effort to combat cybercrime.

As a continuation of these efforts, the 2024 UN Cybercrime Convention is an important step in the development of international law designed to strengthen inter-state collaboration in dealing with the dynamics of cybercrime. This convention contains comprehensive provisions, including investigation procedures, mechanisms for the extradition of perpetrators, cross-border data exchange systems, and procedures for digital evidence that are relevant to the latest technological developments.⁷ Therefore, this convention serves as an effort to establish global standards that can be adopted by member states, thereby creating harmony in the definitions, procedures, and legal approaches to cybercrime. Although it is considered a significant achievement, a number of criticisms remain, particularly regarding the potential threat to privacy and civil liberties due to the increased surveillance capabilities of the state and law enforcement agencies.⁸

The emergence of the 2024 United Nations Convention on Cybercrime marks a major shift in the international legal approach to cyber governance. Unlike the Budapest Convention on Cybercrime,

⁷ Karine Bannelier, 2025, "Risks and Opportunities of the UN Cybercrime Convention for the UNTOC & the Fight against Transnational Organized Crime: A First Assessment," *Transnational Criminal Law Review* 4, no. 1, p. 140-155.

⁸ Murdoch Watney ,2025, "The Legal Pitfalls to Ratification of the United Nations Convention Against Cybercrime," in *Proceedings of the 24th European Conference on Cyber Warfare and Security, ECCWS 2025 (Academic Conferences International)*, p. 717.

which more closely represents the regional perspective of Europe, this new convention was designed through a more inclusive process under the coordination of the United Nations. This inclusivity broadens global participation and allows for different legal views on the balance between cyber security, law enforcement, and the protection of human rights. law, and different policy priorities in shaping international cyber regulations. The emergence of the 2024 United Nations Convention on Cybercrime marks a major shift in the international legal approach to cyber governance. Unlike the Budapest Convention on Cybercrime, which more represents the European regional perspective, this convention has varying levels of interest, legal capacity, and policy priorities in shaping international cyber regulations.⁹

In the development of international cyber law, differences in approach between countries are natural because each legal system has its own characteristics and factors that influence that legal system, such as legal substance, institutional structure, and legal culture of society, which are important elements in determining the success of the implementation of an international convention.¹⁰ The effectiveness of international digital legal instruments depends heavily on the ability of signatory states to balance security aspects with the protection of human rights, including the right to privacy. Therefore, if one of these factors is not balanced, the implementation of conventions such as the 2024 UN Convention on Cybercrime may face obstacles in practice, especially in countries that are still trying to align their legal systems with international standards. The process

⁹ Metehan Durmaz, 2024, "The new UN Cybercrime Convention: aims and pitfalls", <https://smex.org/the-new-un-cybercrime-convention-aims-and-pitfalls/>

¹⁰ Soerjono Soekanto, 2007, Faktor Faktor yang Mempengaruhi Penegakan Hukum, RajaGrafindo Persada, Jakarta, p. 5.

of forming this convention reflects a legal compromise between various systems and national interests at the global level, not as an ideological battle, but as a process of harmonising international law in cyberspace.

These differences of opinion have raised global concerns about the direction of international cyber governance and the protection of fundamental rights in the digital space. Human rights organisations, such as ARTICLE 19, warn that the UN Convention on Cybercrime could potentially give states broader powers to regulate online activities and conduct surveillance without adequate safeguards for privacy and freedom of expression.¹¹ In addition, criticism also came from the Electronic Frontier Foundation (EFF), which assessed that this convention has too broad a scope and has the potential to be used to restrict freedom of expression and individual privacy in the digital space. The EFF specifically highlighted the provisions in Chapter V governing international cooperation in cybercrime investigation and enforcement, which it deemed problematic because it allows for the exchange of data and electronic evidence between countries for various types of crimes without clear restrictions and without strong guarantees of human rights protection. such as Article 35 on the exchange of information and direct assistance between countries, which can be carried out without adequate judicial oversight, while protective provisions such as the principles of necessity and proportionality are not explicitly applied in this chapter, along with a number of other articles that have

¹¹ ARTICLE 19. 2024. "UN Cybercrime Convention: A blueprint for human rights violations", 18 Oktober 2024. Available at: <https://www.article19.org/resources/un-cybercrime-convention-a-blueprint-for-human-rights-violations/>

¹¹ Lihat Universal Declaration of Human Rights, 1948, Article 12.

the potential to lead to abuse of authority and threats to digital privacy.¹² This situation illustrates the growing challenge of balancing cybersecurity and the protection of individual rights in the digital age.

This criticism indicates that the drafting of the convention has not fully prioritised the protection of personal data in the enforcement of cyber law. In fact, the protection of personal data is an integral part of the right to privacy recognised in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).

Article 12 UDHR states:

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”¹³

Article 17 ICCPR similarly provides that:

“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. Everyone has the right to the protection of the law against such interference or attacks.”¹⁴

These two provisions affirm that every individual has the right to protection from arbitrary interference in their private life, family,

¹² Katitza Rodriguez, 2024, “EFF’s Concerns About the UN Draft Cybercrime Convention,” Electronic Frontier Foundation (EFF), <https://www.eff.org/deeplinks/2024/07/effs-concerns-about-un-draft-cybercrime-convention>

¹³ See Universal Declaration of Human Rights, 1948, Article 12.

¹⁴ See International Covenant on Civil and Political Rights, 1966, Article 17.

home, and communications. Privacy is a fundamental right that not only protects personal space, but is also a prerequisite for freedom of expression and protection against abuse of power. Therefore, in the context of regulating cybercrime, it is very important to maintain a careful balance between the need for law enforcement and the protection of individual rights so that there are no widespread violations of human rights.¹⁵

From the perspective of international human rights law, the right to privacy is not an absolute right. Restrictions on this right can only be imposed in accordance with the principles of legality, necessity and proportionality. These principles are explained in detail in General Comment No. 16 of the United Nations Human Rights Committee regarding Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which emphasises that any interference with private life must have a valid legal basis, be necessary for a legitimate purpose such as maintaining public security, and be proportionate to that purpose.¹⁶ Such restrictions can only be accepted within the framework of a democratic society that upholds the protection of human rights. Thus, legal measures taken to combat cybercrime must be strictly limited to what is absolutely necessary and must not undermine the essence of individual rights, particularly the right to privacy and freedom of expression in the digital space.

¹⁵ Nur Azizah Qurrotuaini, 2024, "Hak Privasi sebagai Hak Konstitusional di Era Digital: Kajian Yuridis dalam Perspektif Hukum Siber," *STAATSRECHT: Jurnal Hukum Kenegaraan dan Politik Islam* 4, no. 2, p. 237-239.

¹⁶ Human Rights Committee, General Comment No. 16: The Right to Respect of Privacy, Family, Home and Correspondence (Art. 17), U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988).

The protection of human rights remains a general norm that binds all countries, including in the handling of cybercrime. Special instruments such as cybercrime conventions cannot be separated from the obligations of states under the international human rights regime. The principle of *lex specialis derogat legi generali* explains that when there are two international legal norms governing the same issue, one general and one specific, the specific norm applies as an exception to the general norm. This principle serves to ensure that specific agreements are always interpreted within the framework of international law as a whole, not separately.¹⁷ Thus, the implementation of provisions in international agreements on cybercrime should not ignore the fundamental values of human rights as the foundation of the global legal order.

However, international legal instruments aimed at strengthening global cooperation in combating cybercrime are not entirely risk-free. As seen from the dominance of a number of large countries in the formulation of previous conventions, there is a possibility that these instruments will be used selectively for the political or national security interests of each country. In practice, some countries with weak legal systems and privacy protection standards have the potential to exploit this legal framework to expand digital surveillance practices under the pretext of law enforcement or cyber security. Such international legal instruments, if not accompanied by strong principles of accountability and oversight, could become a basis for

¹⁷ Malcolm N. Shaw, *International Law*, 9th ed. (Cambridge: Cambridge University Press, 2021), p. 95.

legitimising excessive data collection practices that threaten the rights to privacy, freedom of expression, and public participation.¹⁸

A number of analysts believe that this risk is exacerbated by structural weaknesses in the UN Convention on Cybercrime. This instrument still relies heavily on the national laws of each country and does not contain explicit obligations regarding the application of the principles of legality, necessity and proportionality, which are important for preventing abuse of power. The absence of strong human rights protection mechanisms in the convention could potentially justify governments conducting intrusive surveillance and data collection in the name of national security, ultimately threatening individuals' rights to privacy and civil liberties.¹⁹

Digital surveillance practices legitimised through international instruments pose a major challenge to the protection of human rights and civil liberties, both nationally and globally. This situation highlights the need for every country to have a strong and clear legal basis for regulating the protection and restriction of privacy rights in a manner that is proportionate to legal principles and human rights standards.²⁰ Thus, strengthening regulations and enforcing human rights principles in international cyber cooperation is crucial to ensure that global legal instruments do not become a means of abuse of

¹⁸ Kusumaputra A., Sudarsono, Fadli M., & Sukarmi, 2023, "Cyberstate: An Alternative to Building Legal Unification Bringing about Legal Order in Cybersociety," RJOAS: Russian Journal of Agricultural and Socio-Economic Sciences, Issue 7(139), p. 7–8

¹⁹ Katitza Rodríguez, 2024, "The UN Cybercrime Convention: Analyzing the Risks to Human Rights and Global Privacy," Just Security, available at: <https://www.justsecurity.org/98738/cybercrime-convention-human-rights/>

²⁰ Wahyudi Djafar, Bernhard R. F. Sumigar, & Blandina L. Setianti, 2016, *Perlindungan Data Pribadi: Usulan Pelembagaan Kebijakan dari Perspektif HAM*, ELSAM, p. 2.

power, but rather function as mechanisms that truly protect the basic rights of individuals in an increasingly complex digital age.

In the context of national law, the development of cyber law in Indonesia began with the enactment of Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which became the main legal basis for the use of information technology. The development of information and communication technology has changed people's behaviour and created a borderless world, which on the one hand has driven the advancement of human civilisation, but on the other hand has also opened up opportunities for various forms of legal violations in the digital space.²¹ This regulation then became the forerunner for the establishment of a national cyber law regime covering various aspects, including personal data protection, which has gained increasing attention with the passing of Law No. 27 of 2022 on Personal Data Protection (PDP Law) as a more comprehensive legal instrument oriented towards the protection of human rights. This law regulates the basic principles in the collection, processing, storage, and dissemination of personal data, including the obligation of data controllers to ensure the security and integrity of the data they manage.²² The enactment of this law is a historic milestone because, for the first time, Indonesia has comprehensive regulations that specifically govern the principles, obligations, and mechanisms for protecting the personal data of its citizens.

²¹ Teguh Prasetyo dan Rizky P.P. Karo-Karo, 2020, *Pengaturan Perlindungan Data Pribadi di Indonesia: Perspektif Teori Keadilan Bermartabat*, Bandung: Penerbit Nusa Media, p. 12.

²² See Law No. 27 of 2022 of the Republic of Indonesia concerning Personal Data Protection

Institutionally, the PDP Law mandates the establishment of an independent supervisory authority tasked with ensuring compliance with data protection principles and handling disputes arising from privacy violations. The presence of this institution is expected to strengthen national data governance while increasing the accountability of electronic system operators, both in the public and private sectors. However, to date, the implementation of the PDP Law still faces various challenges, ranging from sectoral policy adjustments and law enforcement capacity to low public awareness of digital privacy rights.²³

The relevance of the PDP Law becomes increasingly apparent when linked to discussions on the 2024 UN Cybercrime Convention, which on the one hand aims to strengthen international cooperation in combating cybercrime, but on the other hand raises concerns about the potential expansion of cross-border data collection practices without adequate protection guarantees. In this context, the PDP Law plays an important role as a domestic legal safeguard that can ensure that international cooperation mechanisms under the convention do not violate citizens' constitutional rights to privacy.

Furthermore, the alignment between the PDP Law and international legal instruments such as the UN Cybercrime Convention is important for Indonesia as a country that is active in global cyber cooperation. The harmonisation of national policies with international standards not only strengthens Indonesia's position in digital diplomacy, but also ensures that cyber law enforcement cooperation is carried out while respecting fundamental individual

²³ Muhamad Adri Rinjan, 2025, "Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia" *Jurnal Analisis Hukum* 8 no. 1, p. 77-80.

rights. Thus, the PDP Law not only serves as a national instrument to protect personal data, but also as a form of Indonesia's commitment to upholding human rights principles in the digital realm and preventing the potential misuse of global legal instruments that could threaten the privacy of citizens.

Although the main focus of this research is global, this issue also has important relevance for Indonesia, which is currently strengthening its legal framework for personal data protection and cyber security. As a country participating in the drafting of the UN Cybercrime Convention, Indonesia needs to ensure that its cyber policies remain in line with the human rights principles guaranteed by the constitution and international law. Thus, the results of this study are also expected to contribute normatively to democratic and accountable national cyber policies.

B. Problem Statement

Based on the background that has been explained, so the writer decides that the research question are:

1. What is the potential of the 2024 UN Cybercrime Convention to undermine the protection of personal data?
2. How does the 2024 UN Cybercrime Convention affect data protection under Indonesia's Personal Data Protection Act?

C. Purpose and Benefits of Research

Based on the above problem formulation, the objectives of this study are as follows:

1. Analysing potential weaknesses in the United Nations Cybercrime Convention 2024 regarding personal data protection, particularly in relation to the expansion of state

authority in digital surveillance and cross-border data exchange.

2. Examining the relationship between the United Nations Cybercrime Convention 2024 and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) to identify conformity, overlap, or potential conflicts of norms in personal data protection regulations.

This research is expected to provide the following theoretical and practical benefits:

1. Theoretical Benefits

Theoretically, this research is expected to contribute academically to the development of international law studies, particularly in the field of cyber law and personal data protection. By critically analysing the UN Cybercrime Convention 2024, this research can enrich the legal literature on the relationship between international law and national law in the regulation of digital security and privacy rights. In addition, the results of this study can also be used as a reference for further research discussing the harmonisation of international and domestic legal norms in the context of data protection in the digital age.

2. Practical Benefits

In practical terms, the results of this study are expected to provide input for the Indonesian government, particularly institutions with authority in the field of cyber law and personal data protection, in considering Indonesia's position on the 2024 UN Cybercrime Convention. This research can be used as a consideration in the regulatory harmonisation process if

Indonesia decides to ratify the convention. In addition, the results of this study can also provide a broader understanding for the public, legal practitioners, and policy makers regarding the importance of maintaining a balance between law enforcement efforts against cybercrime and the protection of individuals' fundamental rights to their personal data.

D. Research Originality

Table 1.1 Research Originality

1.	Author Name	: Loviéty Ananda Junianty Amir	
Writing Title		: The Relationship Between International Law and Cybersecurity and Personal Data Protection	
Categories		: Skripsi	
Year		: 2024	
College		: Hasanuddin University	
Description		Previous Research	Research Plan
Issues and Problems		1. How does international law regulate cybersecurity and personal data protection? 2. Has Indonesia adopted international standards in dealing with data leaks, such as the	1. What is the potential of the 2024 UN Cybercrime Convention to undermine the protection of personal data?

	BPJS Kesehatan case, why are there still weaknesses in the national legal system that result in weak protection of people's personal data?	2. How does the 2024 UN Cybercrime Convention affect data protection under Indonesia's Personal Data Protection Act?
Methods	: Normative	Normative
Results and Discussion	: This study shows that international law has regulated the protection of personal data through various conventions such as Convention 108 and the European Convention on Human Rights (ECHR), but Indonesia has not	

	ratified and implemented them effectively. This has resulted in the resolution of data breach cases (such as BPJS) not running optimally. The author also found that national regulations such as the ITE Law and Government Regulation No. 71 of 2019 are still partial in nature and do not provide comprehensive protection for individual privacy. The discussion explains that the weakness of the national cyber security system is caused by	
--	--	--

	overlapping institutional authorities, the absence of independent oversight, and a lack of balanced law enforcement between privacy rights and national security. The author recommends that Indonesia immediately adopt international legal standards such as Convention 108+ to strengthen the personal data protection system and prevent human rights violations in the digital realm.	
--	---	--

2.	Author Name : Muhammad Nur Faizin
----	-----------------------------------

Writing Title	: Legal Review of Personal Data Protection in the Digital Age From a Positive Law Perspective	
Categories	: Skripsi	
Year	: 2024	
College	: Islam Sultan Agung University	
Description	Previous Research	Research Plan
Issues and Problems	1. How does the rapid N N development of digital technology pose a threat to the security of people's personal data? 2. Are national laws such as the Electronic Information and Transactions Law, Government Regulation No. 71 of 2019, and the Personal Data Protection Law of 2022 sufficient to protect citizens' right to privacy in the digital age? Why are there still overlaps and weaknesses in the implementation of	1. What is the potential of the 2024 UN Cybercrime Convention to undermine the protection of personal data? 2. How does the 2024 UN Cybercrime Convention affect data protection under Indonesia's Personal Data

	positive laws regarding personal data protection in Indonesia?	Protection Act?
Methods	: Normative	Normative
Results and Discussion	: This study found that Indonesia's positive legal system in protecting personal data is still partial and lacks effectiveness. Existing laws such as the Electronic Information and Transactions Law, Minister of Communication and Information Technology Regulation No. 20 of 2016, Government Regulation No. 71 of 2019, and Law No. 27 of 2022 overlap and do not provide clear legal certainty. Law enforcement is also	

	not yet optimal due to the limited capacity of law enforcement agencies in handling cases of digital privacy violations. In his discussion, Faizin highlighted that weak legal protection lies not only in regulations, but also in implementation, enforcement, and public awareness of the importance of personal data. This study emphasises the need to develop a comprehensive national legal instrument that is capable of regulating personal data protection in a comprehensive manner and adapting to global information technology developments.	
--	---	--

E. Theoretical Basis

1. Theoretical Basis on Data Protection in the 2024 UN Cybercrime Convention

a. Human Rights Theory

Human rights theory asserts that every individual has inherent rights from birth that cannot be revoked by anyone, including the state. One of these fundamental rights is the right to privacy and personal data protection. The right to privacy is a fundamental right guaranteed by Article 12 of the UDHR and Article 17 of the ICCPR. Both instruments affirm that every individual has the right to protection from arbitrary interference with their private life, family, home and correspondence. The Human Rights Committee, through General Comment No. 16 (1988), emphasises three main principles of privacy restrictions, namely:

1. Legality, restrictions must be based on clear laws.
2. Necessity, restrictions must be necessary for legitimate purposes such as public security.
3. Proportionality, measures must not be excessive in relation to the objectives sought.²⁴

These principles, when applied in practice, demonstrate that privacy protection is not only related to the individual's right to be free from state interference, but also reflects the extent to which a democratic state respects the

²⁴See Human Rights Committee, General Comment No. 16: The Right to Respect of Privacy, Family, Home and Correspondence, 1988.

civil liberties of its citizens. Thus, the right to privacy has a broader social dimension, as it is a prerequisite for citizens' participation in democratic life without fear of surveillance or misuse of personal data.

In the context of modern legal thinking, privacy protection cannot be viewed solely as an individual right that stands alone, but rather as an integral part of civil liberties that form the foundation of democratic participation. Maintaining Privacy Amidst Digital Threats emphasises that the responsibility for protecting personal data does not lie solely with individuals, but is also the obligation of the state to establish a strong regulatory framework and encourage collaboration between the state, society and the private sector in protecting the privacy of its citizens in the digital space.²⁵

b. Data Protection Theory

Personal data protection is a legal principle that gives everyone the right to control their personal information. This principle emphasises that individuals must have the freedom to determine how their personal data is collected, used and disseminated. With this protection in place, no party, whether the state, an institution or a company, may use data arbitrarily.²⁶

²⁵ Nurul Huda dkk., 2024, *Data Pribadi, Hak Warga, dan Negara Hukum: Menjaga Privasi di Tengah Ancaman Digital* (Bandung: Widina Media Utama).

²⁶ Sarah Eskens, 2019, *The Personal Information Sphere: An Integral Approach to Privacy and Related Information and Communication Rights*, (Tilburg Law School), p. 1116.

Data protection is not only a matter of technical regulations, but also part of respecting human rights that guarantee the freedom and dignity of every individual in the digital age. Personal data protection is also an important indicator of respect for human dignity, because data is a digital representation of individuals in the public sphere. When personal data is misused, it is not only information that is harmed, but also a person's moral integrity and personal freedom.

In international and national law, personal data protection is based on universal principles set out in various legal instruments such as the OECD Guidelines (2013), the EU General Data Protection Regulation (GDPR) (2018), and the UN Guidelines for the Regulation of Computerised Personal Data Files (1990). These principles include:

1. Lawfulness and Fairness, data processing is carried out lawfully and fairly.
2. Purpose Limitation, data is used only for specific and legitimate purposes.
3. Data Minimisation, data collected is limited to what is necessary.
4. Accuracy, data must be accurate and up to date.
5. Storage Limitation, data must not be stored longer than necessary.
6. Integrity and Confidentiality, data must be kept secure.

7. Accountability, data controllers are responsible for every stage of data processing.²⁷

These principles indicate that data protection is not only about individual rights, but also institutional legal responsibility to ensure that data management is conducted fairly, transparently, and proportionally. In the national context, regulations regarding personal data protection are comprehensively regulated through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law emphasises that personal data is any data about a person who is identified or can be identified individually.

Personal data protection is also an important issue in international cooperation, especially in the context of cybersecurity and cross-border law enforcement. The 2024 UN Cybercrime Convention aims to enhance collaboration between countries in combating cybercrime, but on the other hand, it has the potential to conflict with the principle of privacy protection. The theory of personal data protection is based on the assumption that personal information is a fundamental human right that cannot be compromised. This protection requires states to regulate, supervise, and enforce policies that guarantee data security without neglecting the individual's right to privacy.

In the context of this study, the theory of personal data protection is used as a normative analytical framework

²⁷ Mutiara Aisyah, 2025, "7 Prinsip GDPR yang Perlu Dipahami Siapa Saja", Cloud Computing Indonesia, <https://event.cloudcomputing.id/pengetahuan-dasar/7-prinsip-gdpr>

to assess whether the 2024 UN Cybercrime Convention respects the basic principles of data protection and is in line with international human rights obligations and Indonesia's national legal system (PDP Law).

c. Principle State Sovereignty

Modern international law is built on the principle of state sovereignty, which gives each state the authority to regulate its internal affairs without outside intervention. Sovereignty is a fundamental concept of international law that is absolute and indivisible, affirming that each state has full authority over its own territory and government.²⁸ An independent country that is not under the sovereignty of another country has the ability to freely engage in relations with other countries as a manifestation of its sovereignty. Thus, the independence of a country (legal independence) is characterised by the absence of other sovereign authorities over its territory, which places it on an equal footing with other countries in the international legal system.

State sovereignty was initially understood as the highest authority within a territory that guaranteed independence from external intervention. However, the development of digital globalisation has challenged this classic form of sovereignty. Sovereignty is no longer absolute, but is subject to moral and international legal

²⁸ Sefriani, *Hukum Internasional Suatu Pengantar*, (Jakarta:RajaGrafindo Persada,2014), p. 103-106

constraints, including the obligation to respect human rights.²⁹

Thus, these principles of international law form the basis for analysing how the 2024 UN Cybercrime Convention strikes a balance between national security interests and international obligations to protect individual rights.

d. The Concept of Cyber Sovereignty

Cyber sovereignty is a concept that asserts that every country has the right to regulate and control digital activities and information flows within its territory.³⁰ In the modern international legal system, the concept of cyber sovereignty remains contested. Countries such as China and Russia emphasise the importance of cyber sovereignty as a means of protecting national security and digital integrity. Conversely, the United States and the European Union favour a cyber freedom or free flow of information approach, which emphasises the free flow of cross-border data and information transparency.

These differing views highlight the tension between the principles of state sovereignty and human rights in the digital context. On the one hand, cyber sovereignty is necessary to protect national security from cyber attacks and foreign influence. On the other hand, an approach that

²⁹ Fajri Matahati Muhammadin, *Rezim Hak Asasi Manusia dan Kedaulatan Negara dalam Hukum Internasional* (Jakarta: INSISTS, 2017).

³⁰ Sefriani, *Hukum Internasional Suatu Pengantar*, (Jakarta: RajaGrafindo Persada, 2014), p. 103-106

places too much emphasis on state control can open the door to restrictions on citizens' freedom of expression and privacy. In the context of personal data protection, the concept of cyber sovereignty has two contradictory sides.

On the one hand, this principle strengthens the protection of a country's digital sovereignty, especially against the dominance of foreign technology companies (Big Tech) that control cross-border data flows.³¹ Through policies such as data localisation, countries can ensure that their citizens' personal data is stored and managed within their national jurisdiction. This approach helps prevent data misuse by external parties and strengthens national security. However, on the other hand, cyber sovereignty has the potential to become a tool for justifying excessive surveillance by the state of its citizens.

2. Theoretical Basis on Digital Sovereignty and Legal Harmonization with Indonesia's Personal Data Protection Act

a. The Concept of Legal Harmonization

Legal harmonisation is an important concept in modern international law, serving to bridge the gap between national legal systems and international legal provisions. In the era of digital globalisation, harmonisation is not only a technical necessity, but also a strategic requirement for countries to adapt their legal systems to global dynamics without losing national

³¹ Gábor Hulkó, János Kálmán, & András Lapsánszky, 2025, The Politics of Digital Sovereignty and the European Union's Legislation: Navigating Crises, Frontiers in Political Science, Vol. 7, p. 2–3.

sovereignty. The process of institutionalising legal harmonisation can be categorised into three main forms:

1. Horizontal coordination, which is a pattern of parallel relationships between national legal systems that seek compatibility without creating a hierarchy between countries.
2. Vertical subordination, where international legal provisions have a higher status and are binding on national law.
3. Recursive interaction, which is a continuous reciprocal process between international and national legal systems to dynamically and continuously adjust legal norms.³²

In applying these models in the era of globalisation and digitalisation of law, all three models can function simultaneously depending on the issues and characteristics of the policies being regulated. For example, in the field of cyber security and cross-border crime, a horizontal coordination approach is often used because it involves equal cooperation between countries without having to submit to a particular legal system. Conversely, on issues such as international trade or cross-border consumer protection, the vertical subordination approach is more dominant due to the existence of international provisions that serve as a common reference. Recursive interactions are

³² Gregory Shaffer, 2013, "Transnational Legal Ordering and State Change", Cambridge University Press, p. 42

important in adaptive sectors, such as the digital economy or electronic transactions, which require continuous regulatory updates to keep pace with technological developments and global needs.³³

From this perspective, legal harmonisation does not aim to standardise all legal rules applicable in various countries, but rather to find a minimum point of compatibility that allows different legal systems to interact and work harmoniously. The main objective of this process is to establish common basic legal principles, strengthen cooperation between countries, and ensure legal certainty in the implementation of international obligations without eliminating the distinctive characteristics and independence of national laws. In other words, legal harmonisation serves to maintain a balance between the universal nature of international law and the legal autonomy of each country.

b. Rule of Law Theory

The theory of the rule of law is a fundamental concept in public law that asserts that state power must be exercised based on the law, not on the will of individuals or rulers. In this system, the law functions as an instrument to limit power so that the actions of the state are always subject to the principles of justice, certainty, and respect for human rights. According to Friedrich Julius Stahl, the rule of law (*Rechtsstaat*) has four key elements, namely:

³³ Syaiful Anwar and Johan Edi Nepri, 2025, "Harmonisasi Hukum Digital: Tantangan Global dan Strategi Adaptif Indonesia dalam Era Kedaulatan Siber," *Hutanasyah: Jurnal Hukum Tata Negara* 4, no. 1, P.78.

1. Protection of human rights
2. Division of powers
3. Government by law
4. An independent and impartial judiciary.

This view emphasises that the law is not only a tool for regulation, but also a tool for protecting people from the abuse of power. In other words, the rule of law is not merely a legalistic principle, but a moral and constitutional principle that guarantees individual freedom and social justice.³⁴

The rule of law is closely linked to the protection of human rights. The United Nations Secretary-General Report (2004) emphasises that:

“The rule of law is a principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-

³⁴ Jimly Asshiddiqie, 2012, “Gagasan Negara Hukum Indonesia”, (Jakarta: Badan Pembinaan Hukum Nasional), p. 2-3.

making, legal certainty, avoidance of arbitrariness and procedural and legal transparency.”³⁵

This means that the rule of law requires all state actions that impact individual rights to have a valid legal basis, be proportionate, and be subject to review through independent judicial mechanisms. In this context, the rule of law serves as a bridge between law and justice, ensuring that public policy does not violate human rights values. In relation to the right to privacy, the rule of law requires that any restriction on this right has a clear legal basis (legality), is carried out for a legitimate purpose (legitimate aim), and is proportional to the needs to be achieved. This is in line with the principles set out in General Comment No. 16 (1988) by the UN Human Rights Committee on Article 17 of the ICCPR, which emphasises the importance of clear legal limits on any interference with the private lives of citizens.

From this description, the theory of the rule of law becomes the normative basis for assessing the compatibility of the 2024 UN Convention on Cybercrime with the legal system and human rights protection in Indonesia. This principle emphasises that cyber law enforcement must uphold justice, legal certainty, and respect for human rights. Based on the principle of the rule of law, the state is expected to balance national security interests with individual privacy

³⁵ See United Nations Secretary-General, The Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies, Report of the Secretary-General, S/2004/616.

rights so that the application of cyber law does not threaten civil liberties and democratic values.

c. Principle of Proportionality

The principle of proportionality is a general principle in law that requires every state action, restriction of rights, or application of public policy to be balanced, reasonable, and not excessive in relation to the objectives to be achieved.³⁶ This principle serves as a measure for assessing whether a government action or law enforcement is in accordance with the principles of justice and the protection of human rights.

The principle of proportionality essentially requires a balance between legitimate aims and restrictions on individual rights imposed by the state. This principle consists of three main elements: (1) suitability or compatibility between the action and the aim; (2) necessity or the need to demonstrate that there are no other less restrictive alternatives; and (3) balancing or the balance between the benefits and the impact on individual rights.³⁷

In the context of this study, the principle of proportionality is used to analyse the extent to which the provisions of the 2024 UN Cybercrime Convention provide balanced digital surveillance powers that do not violate the right to privacy. If a state is given broad authority to access the personal data of its citizens or to conduct cross-border

³⁶ Wizdan Ulum, 2025, "Asas Proporsionalitas dalam Penegakan Hukum," Universitas STEKOM, <https://stekom.ac.id/artikel/asas-proporsionalitas-dalam-penegakan-hukum>

³⁷ Robert Alexy, 2014, "Constitutional Rights, Democracy, and RepresGiuridiche Vol. 3 No. 3, p. 199.

data exchange without clear legal restrictions, then such a policy can be considered disproportionate, as it poses a risk of violating the rights to privacy and freedom of expression.

In addition, this principle also serves to test the compatibility between the 2024 UN Cybercrime Convention and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The PDP Law emphasises that all data control must be carried out based on the principles of legal validity, purpose limitation, and proportionality of personal data use. Thus, the principle of proportionality serves as the normative basis for ensuring that the implementation of the convention does not conflict with the national legal system and Indonesian human rights values.

d. Principle of Accountability

The principle of accountability requires that every action taken by the state, public institutions, and personal data controllers be legally, administratively, and ethically accountable. This principle emphasises the importance of transparency and oversight mechanisms to ensure that all data management policies and activities are carried out responsibly. With this principle in place, it is hoped that the implementation of personal data protection will be in line with the principles of fairness, legal certainty, and the protection of human rights.³⁸

³⁸ Muhammad Akbar Eka Pradana dan Horadin Saragih, 2024, "Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi terhadap GDPR dan Akibat Hukumnya," *INNOVATIVE: Journal of Social Science Research*, Vol. 4 No. 4.

Accountability is an important component of modern legal systems and good governance. In the context of personal data protection, this principle is explicitly regulated in Articles 39–42 of Law No. 27 of 2022 on Personal Data Protection (PDP Law), which stipulates that data controllers must ensure data security and be accountable for any violations that occur.³⁹

This principle is also adopted in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), which state:

*“A data controller should be accountable for complying with measures which give effect to the principles stated above.”*⁴⁰

Thus, the principle of accountability not only requires laws governing data protection, but also ensures that there are mechanisms of responsibility and oversight to guarantee their implementation. Without accountability, laws lose their coercive power and tend to open the door to abuse of authority. In the context of the 2024 UN Cybercrime Convention, accountability is an important principle to ensure that international cooperation in cybercrime investigations is conducted transparently and can be audited by independent supervisory bodies. Countries that receive or process data must be accountable for the use of such data

³⁹ See Law No. 27 of 2022 concerning Personal Data Protection, articles 39–42.

⁴⁰ OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Publishing, 2013), p. 16.

and must provide guarantees that there will be no human rights violations in the process.

F. Framework of Thought

The research framework explains the relationship between the main research issues, problem formulations, and indicators used to address the issues under review. This research stems from the rise in cross-border cybercrime, which poses serious challenges to global security and human rights, particularly the right to privacy and personal data protection. In response to this phenomenon, the international community formed the United Nations Cybercrime Convention 2024 as an effort to strengthen cooperation between countries in combating cybercrime.

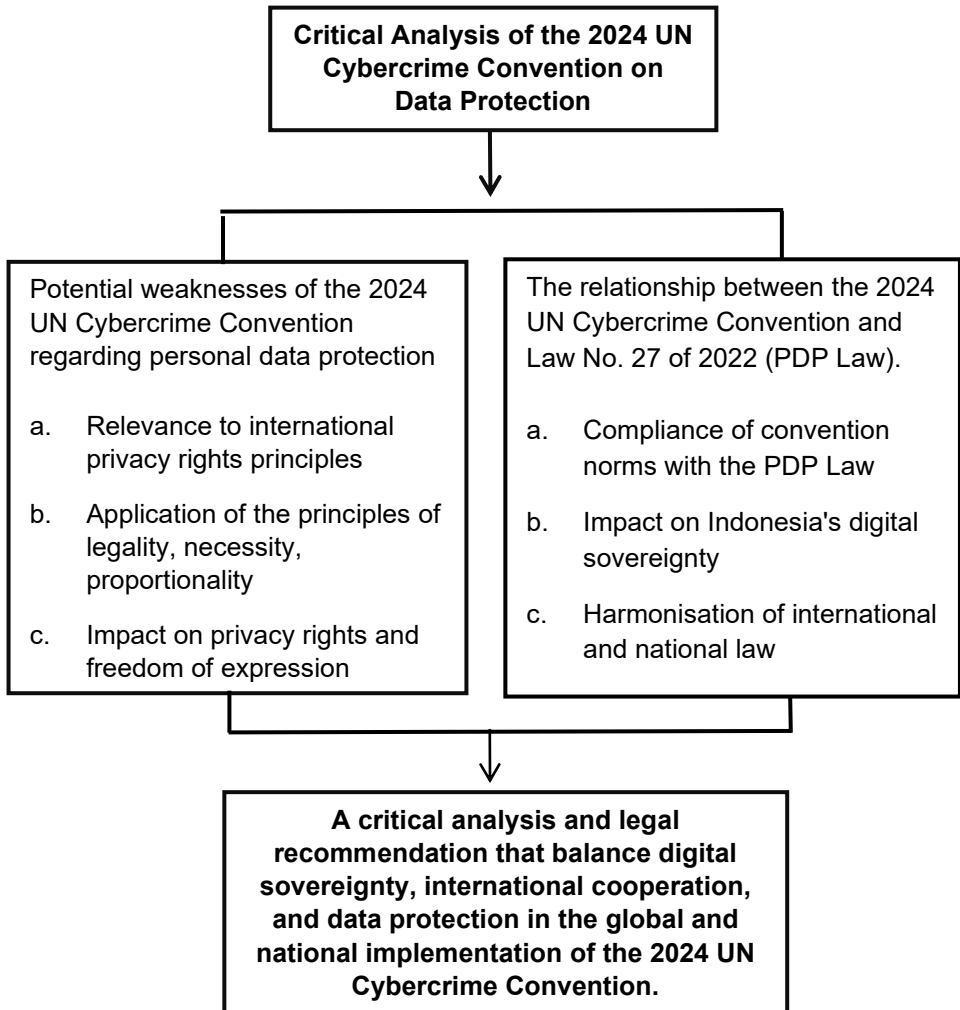
However, the existence of this convention raises a dilemma between the principle of state sovereignty and the protection of human rights. On the one hand, this convention is intended to maintain global security and increase the effectiveness of international cooperation. On the other hand, implementation that places too much emphasis on state control over digital space has the potential to threaten citizens' rights to privacy and freedom of expression. This reflects the tension between security interests and the protection of universal individual rights.

The first problem formulation focuses on the application and position of the principle of cyber sovereignty both in the global context and in Indonesia's national policy. The analysis is aimed at assessing how the UN convention affects the concept of digital sovereignty of participating countries, as well as how Indonesia can uphold its legal sovereignty in cyberspace without neglecting its international cooperation obligations.

The second problem formulation is directed at assessing the relevance of the 2024 UN Cybercrime Convention to personal data protection systems, both in an international framework and in the Indonesian context. This study covers the compatibility of the convention's provisions with the universally recognised principles of proportionality and accountability, as well as how this instrument can strengthen or threaten the protection of privacy rights at the global and national levels.

Through an analysis of these two issues, this study seeks to show that international cooperation in the cyber field must be carried out proportionally and in a manner that balances security interests, state sovereignty, and respect for human rights. The results of this study are expected to contribute to the development of fair international legal norms and strengthen the national legal system in facing the dynamics of digital globalisation.

Figure 1.1 Framework Chart



CHAPTER II

RESEARCH METHOD

A. Research Types and Approaches

This study employs a normative legal research method, which focuses on examining and interpreting the norms and legal rules that are currently in force. The analysis is conducted through the study of legal literature and secondary legal materials relevant to the research topic. Because this type of research relies mainly on written legal sources, it is often referred to as doctrinal research or library-based research.⁴¹

This method represents a key characteristic of legal research, as it views law as a set of norms that regulate social conduct. Accordingly, this study aims to analyse the legal framework governing personal data protection under the 2024 UN Cybercrime Convention and assess its compatibility with Indonesia's national legal system.

B. Type and Source of Legal Materials

1. Primary legal materials

Primary legal materials are sources of law that originate from official or governmental authorities. In this study, the author employs legislation, regulations, and international conventions as the foundational materials for conducting the research. The materials that used are:

- a. UN Cybercrime Convention 2024;
- b. Universal Declaration of Human Rights (UDHR) 1948;

⁴¹ Irwansyah, *Penelitian Hukum: Pilihan Metode dan Praktik Penulisan Artikel* (Yogyakarta: Mirra Buana Media, 2020), p. 42.

- c. International Covenant on Civil and Political Rights (ICCPR) 1966;
- d. Budapest Convention on Cybercrime (2001);
- e. Law No. 27 of 2022 concerning Personal Data Protection;
- f. Other international legal instruments governing privacy and cyber security rights.

2. Secondary legal materials

Secondary legal materials are legal materials sourced from scholars or legal experts, obtained by referring to their scientific works, such as legal journals, books, research results, and various other written legal documents. These secondary legal materials are used to provide explanations, analyses, and interpretations of primary legal materials.

C. Legal Materials Collection Technique

The techniques for collecting legal materials in this research are carried out by identifying and systematically examining all legal materials relevant to the research problem, particularly those concerning personal data protection within the framework of the 2024 United Nations Cybercrime Convention. This process is intended to ensure a strong normative foundation for analysing the relationship between international legal instruments and Indonesia's national legal system. The legal materials used in this study consist of primary legal materials and secondary legal materials. Primary legal materials include international conventions and national legislation that regulate cybercrime, the right to privacy, and personal data protection. These materials serve as the main reference for examining legal norms, state authority, and the legal implications of

implementing the 2024 UN Cybercrime Convention at the national level.

Secondary legal materials are derived from scholarly works such as legal textbooks, academic journals, research findings, and expert opinions related to international law, cyber law, human rights, and data protection. These materials are used to support legal interpretation, strengthen legal arguments, and provide critical perspectives on the primary legal materials. All collected legal materials are then classified based on their relevance to the research questions and analysed systematically to address the issues examined in this study.

D. Analysis of Legal Materials

The analysis in this study was conducted using primary and secondary legal materials relevant to the research topic. These materials were examined to obtain theoretical and practical insights concerning the regulation of personal data protection under international and national law. In conducting this process, the researcher examined and cited various legal materials, including national legislation, international conventions, and legal literature that support the legal analysis of this study. The legal materials analysed include legislation, international conventions, and legal literature, such as the UN Cybercrime Convention 2024 and Law No. 27 of 2022 on Personal Data Protection. All legal materials obtained were then analysed and systematically organised in accordance with the research questions raised in this study.