

CHAPTER I INTRODUCTION

A. Background

The rapid expansion of digital technologies has fundamentally transformed governance structures of digitalization at both national and international levels. States increasingly rely on digital identity systems, biometric databases, cross-border data exchange mechanisms, and digital evidence processing frameworks to enhance administrative efficiency and strengthen transnational cooperation. The development of these sectors has influenced the formation of new legal instruments, including international law. In this regard, the United Nations Cybercrime Convention (Hanoi Convention) has become a new international legal instrument and was adopted by the General Assembly on 24 December 2024. This marks a historic milestone, and becomes the first legally binding international legal instrument specifically to strengthen global cooperation in the prevention and addressing of cyber-related issues.¹ This convention regulates various important aspects, such as the criminalization of certain acts in cyberspace, cross-border law enforcement cooperation, and the exchange of data and information.²

While the UN Cybercrime Convention offers potential benefits in international cooperation in addressing and combating cybercrime. Digitization poses serious challenges to the protection of human rights in the context of sovereignty, especially for indigenous peoples as a vulnerable group. In this context, international human rights are regarded as a fundamental freedom that cannot be curtailed under any circumstances.³ This provides a comprehensive picture of how the challenges of protecting indigenous peoples cannot be limited under any circumstances, including their right to security in the context of cybercrime. In this thesis, indigenous peoples are the primary focus because they tend to share common characteristics worldwide, including a lack of recognition from the governments of the countries where they live, economic and

¹ United Nations, 2025, *Depositary Notification C.N.196.2025.TREATIES-XVIII.16: United Nations Convention against Cybercrime; Strengthening International Cooperation*, 13 May, United Nations Treaty Collection, <https://treaties.un.org/doc/Publication/CN/2025/CN.196.2025-Eng.pdf>, accessed 23 February 2026.

² United Nations General Assembly, 2025, *Resolution A/RES/79/243*, adopted 19 December 2025, UN Doc. A/RES/79/243, <https://docs.un.org/en/A/RES/79/243>, accessed 23 February 2026.

³ M. Ashri, 2018, *Hak Asasi Manusia: Filosofi, Teori & Instrumen Dasar*, Makassar: Social Politic Genius (SIGn), p. 3.

political marginalization, and racial discrimination.⁴ Furthermore, the rights of indigenous peoples to sovereignty are an important basis for promoting advocacy and various efforts aimed at strengthening their autonomy and increasing their control over various aspects of life that impact their communities and cultural continuity.⁵ To date, It is estimated that there are around 476 million indigenous peoples in the world, spread across more than 90 countries and approximately 6.2% of the global population.⁶ Although they represent a small percentage of the global population, they inhabit and manage 25–30% of the Earth's land area, which is home to 80% of the world's biodiversity⁷ which indicates that the fulfilment of human rights for vulnerable groups such as indigenous peoples is still greatly needed.

The presence of the UN Cybercrime Convention poses new challenges for them because it introduces expansive surveillance powers, facilitates cross-border data sharing for various crimes, and lacks safeguards to protect. The possible overarching impact of this treaty is even broader than criminal justice, criminal law and human rights. Through discussions on cybercrime, negotiations revealed deep division between and polarization of UN member states on the issue of power and control in cyberspace.⁸ These provisions risk being misused by governments to suppress dissent, infringe on press freedom, and target marginalized communities, including Indigenous Peoples.⁹

As digital governance expands beyond domestic boundaries into transnational regulatory frameworks, questions arise about how international legal instruments balance security demands with the protection of human rights,

⁴ Arifiana, W. T. P., 2021, Penerapan Prinsip Free, Prior and Informed Consent Sebagai Upaya Perlindungan Hak Ulayat Masyarakat Adat Berdasarkan United Nations Declaration on the Rights of Indigenous Peoples (Studi Komparasi antara Indonesia dan Australia), Thesis, Yogyakarta: Universitas Gadjah Mada.

⁵ M. Hudson, S. R. Carroll, J. Anderson, D. Blackwater, F. M. Cordova-Marks, J. Cummins, et al., 2023, "Indigenous Peoples' Rights in Data: A Contribution toward Indigenous Research Sovereignty," *Frontiers in Research Metrics and Analytics*, 8: 1173805, <https://doi.org/10.3389/frma.2023.1173805>.

⁶ United Nations, 2025, "Background – International Day of the World's Indigenous Peoples," <https://www.un.org/id/node/81566>, accessed 28 February 2026.

⁷ United Nations, 2026, "Indigenous Peoples", *United Nations: Fight Racism*, [online], (<https://www.un.org/en/fight-racism/vulnerable-groups/indigenous-peoples>, accessed 17 March 2026).

⁸ T. Tropina, 2024, "This Is Not a Human Rights Convention!": The Perils of Overlooking Human Rights in the UN Cybercrime Treaty," *Journal of Cyber Policy*, 9(2): 200–220, <https://doi.org/10.1080/23738871.2024.2419517>.

⁹ Leo F. Lin, 2025, "The UN Cybercrime Convention: What It Means for Policing and Community Safety in Australia," *Australian Institute of International Affairs*, 30 January, <https://www.internationalaffairs.org.au/australianoutlook/the-un-cybercrime-convention-what-it-means-for-policing-and-community-safety-in-australia/>, accessed 23 February 2026.

especially for vulnerable groups such as indigenous peoples. Then, will the acceleration of digital technology, followed by legal instruments such as the UN Cybercrime Convention, be able to impact the development of indigenous peoples, or will it instead cause them to fall further behind and be exploited by certain parties.

Since the adoption of the UNDRIP in 2007, various UN treaty bodies have increasingly cited it as a reference when assessing reports from State Parties. Some bodies have even urged states to comply with the principles of the UNDRIP and incorporate them into national law. In its evolution, the UNDRIP is now routinely used in general comments and recommendations issued by UN treaty bodies. In one of its most recent general comments, the Committee on Economic, Social, and Cultural Rights (CESCR) affirmed that states have a primary obligation to obtain free, prior, and informed consent (FPIC), particularly when the natural and cultural resources of Indigenous Peoples are potentially affected.¹⁰ On the other international legally binding instrument, one of the concerns is the absence of the principle of Free, Prior, and Informed Consent (FPIC) in the UN Cybercrime Convention as a basis principle for the collection, processing, and use of digital data related to Indigenous Peoples. The FPIC principle has developed into a fundamental international legal standard for indigenous peoples.¹¹ Instruments such as the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) and ILO Convention No. 169 explicitly recognize the right of indigenous peoples to give their free, prior, and informed consent before states or other parties make decisions that affect their territories, resources, and ways of life.¹² The absence of the FPIC principle in the UN Convention on Cybercrime indicates a legal gap between the international cyber legal framework and the framework for protecting the rights of indigenous peoples in the context of human rights, where these mechanisms repeatedly highlight challenges related to respecting and implementing the right to free,

¹⁰ International Work Group for Indigenous Affairs (IWGIA), 2024, *The Indigenous World 2024*, Copenhagen: IWGIA, p. 6.

¹¹ United Nations, 2007, *United Nations Declaration on the Rights of Indigenous Peoples*, adopted 13 September 2007, UNGA Res. 61/295.

¹² Kristen A. Peterson, 2013, "Free, Prior and Informed Consent: ILO 169 and UNDRIP," University of Colorado Law School, Colorado Law Scholarly Commons, available at <https://scholar.law.colorado.edu/free-prior-and-informed-consent/>, accessed 2 March 2026.

prior, and informed consent.¹³

The FPIC principle is understood as a principle of international human rights law that guarantees the right of Indigenous Peoples to give or withhold consent to measures that may affect their lands, territories, resources, or collective rights.¹⁴ Meanwhile, the concept of FPIC principle is a fundamental principle of ethical community-based and participatory research.¹⁵ Furthermore, the FPIC principle has normative and moral legitimacy within the framework of human rights, which implies a normative obligation for both states and corporations to respect the rights of indigenous peoples.¹⁶ The absence of provisions in this convention raises fundamental questions about the extent to which the Cybercrime Convention accommodates the protection of fundamental rights for indigenous peoples in global cyber governance and what the normative implications are of the absence of this principle.

Normatively, legal instruments that have implications for the possibility of cross-border and cross-jurisdictional violations should adopt elements of international human rights law in order to prevent fundamental human rights violations. The UN Convention on Cybercrime should not only strengthen international cooperation in combating cybercrime, but also ensure that such cooperation is carried out in accordance with established human rights standards. In this case, the recognition of the right to participation, accountability mechanisms, and consultation processes is a normative requirement in the FPIC landscape.

The practical implications of these normative requirements can be observed in several comparative cases. In Aotearoa New Zealand, Māori scholars and tribal authorities developed the concept of Indigenous Data Sovereignty in response to the international collection of genomic and cultural data without collective consent. The establishment of Te Mana Raraunga as a Māori data sovereignty network illustrates efforts to reclaim regulatory authority over digital

¹³ United Nations, *United Nations Declaration on the Rights of Indigenous Peoples*, Op.Cit., arts. 10, 11(2), 19, 28, and 29(2).

¹⁴ Human Rights Council, 2013, *Report of the Special Rapporteur on the Rights of Indigenous Peoples, James Anaya*, UN Doc. A/HRC/24/41.

¹⁵ T. D. Toubmourou, M. Siscawati, A. Utomo, H. Sinaga, S. Adelina, A. Ibni Albar, et al., 2025, "An Intersectionally Aware Process for Securing Free, Prior, and Informed Consent in Community-Based Research," *Development in Practice*, pp. 1–10, <https://doi.org/10.1080/09614524.2025.2543355>.

¹⁶ L. Klein, M. J. Muñoz-Torres, and M. Á. Fernández-Izquierdo, 2024, "Free, Prior, and Informed Consent: A Norm in Development or a Corporate Obligation?," *International Journal on Minority and Group Rights*, 31(5): 898–926, <https://doi.org/10.1163/15718115-bja10153>.

and biological data originating from Indigenous communities.¹⁷ Looking at several cases where human genome research has been conducted and occurred in indigenous communities in countries such as Canada, the United States, and South Africa, it is often carried out without a mechanism for collective consent from indigenous peoples.¹⁸ This dynamic not only undermines the autonomy of indigenous groups over their biological and digital data, but also reinforces structural inequalities in global research practices. This case shows how national laws and international scientific practices often recognize individual consent but ignore the collective dimension that is central to FPIC. This shows that in the context of biological and digital data, the absence of FPIC mechanisms can lead to structural exploitation. This is in line with the potential for cross-border data collection and exchange within the framework of the Cybercrime Convention.

Therefore, the Convention on Cybercrime, as part of the first legally binding international legal order, should be interpreted and implemented consistently with existing human rights obligations, including those relating to participation, consent, and protection of vulnerable groups such as indigenous peoples. It is important to critically examine how the United Nations Cybercrime Convention regulates or does not regulate the principle of Free, Prior, and Informed Consent (FPIC) in the context of protecting Indigenous Peoples. This analysis is relevant not only for assessing the compatibility of the convention with existing international human rights instruments, but also for examining the normative implications of the absence of FPIC regulations on the protection of indigenous peoples. Through this research, it is hoped that a more comprehensive understanding can be developed regarding the need for a more inclusive cyber law approach that is based on human rights and sensitive to the collective rights of indigenous peoples in the digital age. Based on the background, the following are the research questions that will be the main objects of study in this thesis.

B. Research Questions

The questions of this research include:

¹⁷ Health Research Council of New Zealand, 2023, *Driving Indigenous Data Sovereignty*, <https://www.hrc.govt.nz/making-a-difference/impact-stories/driving-indigenous-data-sovereignty> accessed 2 March 2026.

¹⁸ F Kabata, 2025, 'Indigenous Peoples' Human Genomic Sovereignty: Lessons for Africa' *Developing World Bioethics* 190 <https://doi.org/10.1111/dewb.12466> accessed 2 March 2026.

1. To what extent does the United Nations Cybercrime Convention (Hanoi Convention) address the principle of Free, Prior, and Informed Consent (FPIC) of Indigenous Peoples?
2. What are the implications of the absence of the FPIC principle in the Cybercrime Convention for the protection of Indigenous Peoples?

C. Research Objectives and Significance

Research objectives are expected to:

1. To understand the extent to which the Cybercrime Convention incorporates or reflects the principle of Free, Prior, and Informed Consent (FPIC) of Indigenous Peoples.
2. To understand the legal implications arising from the absence FPIC principle within the Cybercrime Convention in relation to the protection of Indigenous Peoples' rights.

This research is expected to provide both theoretical and practical contributions:

1. Theoretical Significance

This research is expected to contribute to the development of international law discourse by examining the intersection between international cyber law and Indigenous Peoples' rights. It enriches academic discussion on how human rights principles, particularly FPIC, should be integrated into emerging global regulatory frameworks such as the Cybercrime Convention.

2. Practical Significance

This research provides policy-oriented insights for lawmakers, international organizations, and state actors in ensuring that cybercrime regulations do not marginalize or undermine the rights of Indigenous Peoples. It also serves as a reference for advocacy efforts aimed at strengthening human rights safeguards within international legal instruments related to digital governance.

- a. For the Government, this research provides a critical legal analysis to guide the ratification process of the Hanoi Convention that aligns with national interests and constitutional obligations to protect indigenous peoples.

- b. For Indigenous Communities, it offers legal arguments and policy recommendations to advocate for better protection of their digital heritage, empowering them to use the Convention's mechanisms to combat the theft of their traditional knowledge, and increase awareness and understanding of the importance of the principle of Free, Prior and Informed Consent (FPIC) in the context of digital governance and cybercrime regulation. It may also support the recognition and protection of Indigenous Peoples' rights, particularly in relation to consent, participation, and decision-making processes affecting their digital and social interests.
- c. For Legal Practitioners and Law Enforcement, this research is expected to serve as a reference for legal practitioners in interpreting and applying international and national legal frameworks related to cybercrime and Indigenous Peoples' rights. It may assist legal practitioners in providing legal opinions, advocacy, and legal protection concerning cases involving the intersection of cybercrime enforcement and the principle of FPIC.

D. Research Originality

The validity of this research can be relied upon by the author because the research framework is directly rooted in the author's thinking, supported by books, theses, and legal journals that support the substance of this research. This research was conducted to discuss legal issues that have not been widely explored in previous studies, particularly those related to the relationship between the United Nations Cybercrime Convention, the concept of Free, Prior and Informed Consent (FPIC) Principle, and the protection of Indigenous Peoples.

Thesis

Author	Arifiana Triesedyawati Puspita Wardhani
Title	Penerapan Prinsip <i>Free, Prior and Informed Consent</i> Sebagai Upaya Perlindungan Hak Ulayat Masyarakat Adat Berdasarkan United Nations Declaration on the

	Rights of Indigenous Peoples (Studi Komparasi antara Indonesia dan Australia)	
Category	Thesis	
Year	2021	
University	Universitas Gadjah Mada	
Description	Previous Studies	Research Plan
Issues and Problems	Focus on the application of FPIC principles in protecting the customary rights of indigenous peoples based on UNDRIP and a comparison of implementation between Indonesia and Australia.	Focus on the absence of the FPIC principle in the United Nations Cybercrime Convention and its normative implications for the protection of indigenous peoples' rights in global cyber governance.
	Based on the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP), ILO Convention No. 169, as well as Indonesian and Australian national laws.	Identifying normative gaps in FPIC in the United Nations Cybercrime Convention and their impact on the protection of indigenous peoples' rights in the digital age.
Research Method	Normative	Normative
This study examines and compares how the principle of free, prior, and informed consent is applied as an effort to protect the customary rights of indigenous peoples in Indonesia and Australia. This study uses the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) as a benchmark, particularly Articles 10 and 19 of the		Result and Discussions

Declaration. This study is a qualitative study with a legal-normative approach and a comparative-descriptive nature, which describes empirical facts with a normative analysis tool, comparing the implementation of the principle of free, prior and informed consent in Indonesia and Australia, particularly in relation to the protection of customary rights in both countries. This study examines the case studies of the Merauke Integrated Food and Energy Estate (MIFEE) project in Papua, Indonesia, and the uranium mining project in Kakadu National Park, Northern Territory, Australia. The research data was collected through literature studies and other secondary data. The results of the study show that, first, neither Indonesia nor Australia has regulations that explicitly mention the principle of free, prior and informed consent. Second, the implementation of the FPIC principle in the field is still far from ideal as stipulated in the UNDRIP.	
---	--

As a point of comparison, this research refers to a previous undergraduate thesis written by Arifiana Triesedyawati Puspita Wardhani (2021) entitled *“Penerapan Prinsip Free, Prior and Informed Consent sebagai Upaya Perlindungan Hak Ulayat Masyarakat Adat Berdasarkan United Nations Declaration on the Rights of Indigenous Peoples (Studi Komparasi antara Indonesia dan Australia)”* from Universitas Gadjah Mada.¹⁹ The study adopts a normative legal research method with a comparative-descriptive approach, examining the implementation of the principle of Free, Prior and Informed Consent (FPIC) as a mechanism for protecting Indigenous Peoples’ customary land rights in Indonesia and Australia. The previous research primarily situates FPIC within the framework of the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP), particularly Articles 10 and 19, and focuses on land-based and resource-related issues affecting Indigenous Peoples. Its

¹⁹ W. T. P. Arifiana, *Op.Cit.*, p. 1.

analysis is grounded in empirical case studies, namely the Merauke Integrated Food and Energy Estate (MIFEE) project in Papua, Indonesia, and the uranium mining project in Kakadu National Park, Northern Territory, Australia. Through this comparative analysis, the study concludes that both Indonesia and Australia lack explicit legal provisions recognizing FPIC and that the practical implementation of FPIC in both countries remains far from the standards envisaged by UNDRIP.

Unlike previous studies, this study has a significantly different scope and orientation. Previous studies examined FPIC in relation to customary land rights and natural resource exploitation in two national legal systems between Indonesia and Australia, while this study will focus on a legal analysis of the UN Convention on Cybercrime (Hanoi Convention) and its relation to the existence of the FPIC principle in the context of indigenous peoples across the countries. In addition, this study will take a normative-critical approach to legal gap analysis between the international cyber law regime and the indigenous peoples' rights protection regime. Furthermore, the object of this study will not focus on comparative studies between countries, but rather on the normative structure of international legal instruments in the United Nations Cybercrime Convention and its implications for indigenous peoples in general. By positioning the FPIC principle within the evolving landscape of international cyber regulation and examining its implications for Indigenous peoples, this study offers a distinct and novel contribution that clearly differentiates it from previous research.

Journal

Author	Tatiana Tropina	
Title	This is not a human rights convention”: the perils of overlooking human rights in the UN cybercrime treaty	
Category	Journal	
Year	2024	
University	Leiden University	
Description	Previous Studies	Research Plan
Issues and	Reviewing the formation	Reviewing the

Problems	and substance of the UN Cybercrime Convention, which is considered not to have been designed as a human rights instrument.	substance of the UN Cybercrime Convention from the perspective of protecting the rights of indigenous peoples.
	Reviewing human rights safeguards in the UN Cybercrime Convention in general	Analyzing the possible impact of the absence of the FPIC principle in the UN Cybercrime Convention on indigenous peoples.
Research Method	Normative	Normative
The results of the study show that the lack of consensus on the definition and scope of cybercrime is at the root of the differences in position among countries in the process of formulating the United Nations Convention against Cybercrime. The debate concerns not only cyber-dependent categories of cybercrime (such as illegal access or system destruction), but also cyber-enabled crimes that have traditionally been regulated in conventional criminal law. As analyzed by Tatiana Tropina in her article in the Journal of Cyber Policy, this conceptual ambiguity opens the door to an expansion of criminalization that potentially goes beyond the need to protect computer systems and data. Several countries are pushing for content-based crimes such as the dissemination of “false information,” insults against religious values, or extremism to be included in the scope of the convention. This approach signals a shift from protecting digital infrastructure to controlling expression in cyberspace. These findings		Result and Discussions

show that without strict limitations, the convention has the potential to become an instrument for legitimizing repressive practices at the domestic level. In fact, the principle of *nullum crimen sine lege* in international human rights law requires the formulation of clear, explicit, and unambiguous offenses. Thus, expanding the scope without strict normative parameters risks eroding standards for the protection of freedom of expression and the right to information. Problems arise when human rights protection clauses are not formulated comprehensively. In the final draft analyzed by Tropina, which has now become a convention, principles such as legality, necessity, and proportionality are not explicitly and in detail regulated, but are largely left to domestic law. This approach creates disparities in protection standards between countries and opens up opportunities for abuse of investigative powers, especially in countries with weak human rights protection systems. Overall, this study shows a structural tension between the goal of effective law enforcement and the obligation to protect human rights. Countries that push for broad coverage tend to prioritize national stability and security, while other countries and civil society organizations emphasize the importance of strong safeguards. Tropina's article shows that the argument "this is not a human rights convention" reflects the view that the convention is merely a technical instrument of law enforcement. However, this approach is problematic because every international criminal law instrument inherently has direct consequences for fundamental rights. Ignoring

the human rights dimension means ignoring the inherent nature of criminal law as an instrument of restriction on individual freedoms. The discussion in this journal emphasizes that the legitimacy of the convention depends not only on its effectiveness in combating cybercrime, but also on its ability to explicitly and operationally guarantee the protection of human rights. Without strengthening the principles of legality, proportionality, independent oversight, and limitations on the scope of criminalization, the convention has the potential to set a global precedent for the expansion of state power in the digital space.	
--	--

The point of comparison of Tatiana Tropina's published in the Journal of Cyber Policy, which critically examines the formation and substance of the United Nations Convention against Cybercrime (Hanoi Convention). Tropina's study adopts a normative legal approach, analyzing the drafting process, negotiating dynamics among states, and the structural design of the Convention. The central issue addressed concerns the absence of a clear consensus regarding the definition and scope of cybercrime, particularly the tension between narrowly defined cyber-dependent crimes and broader cyber-enabled or content-related offenses. The study demonstrates that conceptual ambiguity in the Convention's formulation opens the possibility for expanded criminalization, including the incorporation of content-based crimes such as the dissemination of "false information," extremism, or offenses against religious values. According to Tropina, this expansion risks transforming the Convention from a technical instrument aimed at protecting digital infrastructure into a framework that may legitimize domestic repression. Furthermore, the article highlights the insufficient articulation of human rights safeguards within the Convention, noting that fundamental principles such as legality, necessity, and proportionality are not comprehensively operationalized but instead largely deferred to domestic legal systems. Tropina concludes that there is an inherent structural tension between effective law enforcement and the protection of human rights, and that the Convention's legitimacy ultimately depends on its capacity to embed explicit and enforceable human rights guarantees.

The previous study focuses on the general human rights implications of the Convention and the risks of over criminalization, this research adopts a more specific normative orientation by examining the position of Indigenous Peoples within the evolving international cyber law regime. While Tropina critiques the Convention from a broad human rights perspective, this study seeks to assess whether the normative structure of the United Nations Convention against Cybercrime adequately accommodates the principle of Free, Prior and Informed Consent (FPIC) as a collective right of Indigenous Peoples. Employing a normative-critical method and legal gap analysis, this research will explore the disconnection between the cybercrime regime and the international legal framework governing Indigenous Peoples' rights, particularly in relation to data governance, cross-border information sharing, digital surveillance, and investigative cooperation.

E. Theoretical Framework

In legal research, a theoretical framework serves as a conceptual foundation to analyze legal norms, interpret international instruments, and assess their coherence with established principles of international law. Theoretical frameworks are essential in normative legal research because they provide analytical tools to evaluate whether a legal instrument aligns with fundamental legal doctrines, human rights standards, and overarching principles recognized in international law. This research examines the United Nations Cybercrime Convention (Hanoi Convention) in relation to the principle of Free, Prior, and Informed Consent (FPIC) and the protection of Indigenous Peoples' rights. Accordingly, this research applies several principal theoretical frameworks:

1. Human Rights Safeguards Theory

The Human Rights Safeguards Framework functions as the primary analytical lens to assess whether the UN Cybercrime Convention procedural and substantive guarantees in accordance with international human rights standards. This is also reinforced by the importance of human rights safeguards written by Amartya Sen in his seminal work, "Elements of a Theory of Human Rights" (2004), which offers a strong antithesis to this legalistic view and argues that human rights are essentially ethical demands that transcend the boundaries of

positive law.²⁰ Therefore, the integration of the UN Cybercrime Convention into this theoretical principle would be most appropriate if it were examined using one of the standards of human rights itself, namely the FPIC principle.

2. Human Rights-Based Approach (HRBA)

This research employs a Human Rights-Based Approach (HRBA) as an analytical framework. HRBA is normatively grounded in international human rights law and emphasizes the principles of participation, non-discrimination, accountability, and the recognition of rights-holders.²¹ HRBA is a conceptual framework for the process of human development that is normatively based on international human rights standards and operationally directed to promoting and protecting human rights.²² HRBA is a method that applies five key working principles to advance human rights for all: meaningful and inclusive participation and access to decision-making; non-discrimination and equality; accountability and the rule of law for all; transparency and access to information, supported by disaggregated data.²³ In the context of the Cybercrime Convention, HRBA places individuals and groups, including indigenous peoples, as rights-holders and the state and its institutions as duty-bearers responsible for respecting, protecting, and fulfilling those rights. Through this framework, this study evaluates whether the Cybercrime Convention sufficiently incorporates the rights of Indigenous Peoples, particularly the principle of Free, Prior, and Informed Consent (FPIC).

3. Legal Pluralism Theory

Pluralism refers to a situation in which various legal systems and societal beliefs coexist.²⁴ Legal pluralism involves the simultaneous

²⁰ Sen, A., 2017. Elements of a theory of human rights. In *Justice and the capabilities approach* (pp. 221-262). Routledge.

²¹ Office of the United Nations High Commissioner for Human Rights, 2006, *Frequently Asked Questions on a Human Rights-Based Approach to Development Cooperation*, New York and Geneva: United Nations.

²² United Nations Development Group, 2003, *The Human Rights-Based Approach to Development Cooperation: Towards a Common Understanding among UN Agencies*, New York: United Nations.

²³ European Commission, 2025, "Human Rights Based Approach," 20 October, <https://wikis.ec.europa.eu/spaces/ExactExternalWiki/pages/50108948/Human+Rights+Based+Approach>, accessed 2 March 2026.

²⁴ William Twining, 2009, *General Jurisprudence: Understanding Law from a Global Perspective*,

engagement of various forms of law. This includes state law, international law, transnational law, customary law, religious law, indigenous law, and the laws of different ethnic or cultural communities.²⁵ In other words, it is important to examine this theory of legal pluralism because it considers various types of international, national, and customary legal instruments at the same time, including a review of the UN Cybercrime Convention on Indigenous Peoples around the world who have different customary laws and jurisdictions.

4. Classification of Cybercrime

The definition of cybercrime remains broad and has a very wide scope.²⁶ Furthermore, there is a rather complex issue in defining cybercrime, starting with the terminology, which uses many terms combined with other words beginning with the prefixes cyber, computer, internet, digital, or information.²⁷ This concept signifies a dynamic force that will evolve into increasingly complex forms as technology advances. Given the broad nature of cybercrime terminology, a clear and structured classification of cybercrimes is essential to provide conceptual clarity and ensure consistency in legal interpretation in this paper. This classification serves as an analytical framework in normative legal research, particularly in determining whether specific digital activities fall within the scope of cybercrime. Among the many existing definitions, The author has cited the Oxford Dictionaries as one of the sources for finding a comprehensive definition that is widely used by researchers, which states that cybercrime is criminal activities carried out by means of computers or the internet.²⁸ In other literature, cybercrime is also defined as a

Cambridge: Cambridge University Press, p. 131.

²⁵ Brian Z. Tamanaha, 2021, *Legal Pluralism Explained: History, Theory, Consequences*, Oxford: Oxford University Press, available at <https://doi.org/10.1093/oso/9780190861551.001.0001>, accessed 25 February 2026.

²⁶ Jonathan Lusthaus (University of Oxford), "Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?", *Annual Review of Law and Social Science*, Vol. 20, 2024, p. 380.

²⁷ Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, 2(2), 379–398. <https://doi.org/10.3390/forensicsci2020028>

²⁸ Oxford Learner's Dictionaries, "Cybercrime", Oxford University Press, 2026, <https://www.oxfordlearnersdictionaries.com/definition/english/cybercrime>, accessed April 18, 2026.

criminal offense committed online by exploiting electronic communication networks and information systems.²⁹

The distinction between cyber-dependent crimes and cyber-enabled crimes provides a fundamental framework for understanding the scope and nature of cybercrime.³⁰ This classification is crucial given the broad and ever-evolving nature of cybercrime, which cannot be confined to a single definition. Cybercrime refers to criminal acts that can only be committed through the use of computers, computer networks, or other forms of information and communication technology (ICT). In ICT research, this framework is viewed as a computer-based realm of information and communication. In this context, the virtual world is often regarded as a new reality in human life known as the internet.³¹ The existence of Information and Communication Technology (ICT) provides significant opportunities for the public to achieve greater effectiveness and efficiency in problem-solving, particularly in the fields of information and communication.³²

In this category, digital systems are not merely tools, but rather the primary targets and the environment in which these crimes occur. Activities such as hacking, the distribution of malware, and denial-of-service attacks are examples of this category, as they fundamentally depend on the existence of digital infrastructure. Without ICT, these crimes would not exist, which demonstrates their inherently technological nature.³³ In contrast, cyber-enabled crimes refers to conventional criminal activities that are facilitated, expanded, or enhanced through the use of digital technology. In these cases, ICT serves only as a tool, not as the target of the crime. Crimes such as fraud, identity theft, and data exploitation fall into this category, as these crimes can occur in both physical and digital contexts, but have a

²⁹ Jonathan Lusthaus, *Op.Cit.*, p. 380.

³⁰ Mike McGuire and Samantha Dowling, "Cyber crime: A review of the evidence", *Home Office Research Report 75*, 2013, p. 5.

³¹ Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar*, Jakarta: Prenada Media Group, (2013), p. 46.

³² N. K. Kadir, Judhariksawan, and Maskun, 2019, "Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes," *Fiat Justisia*, 13(4): 333–344.

³³ *Ibid.*, p. 6-8.

broader scale, speed, and reach when committed online.³⁴ This indicates that while the core essence of such crimes remains unchanged, digital technology significantly amplifies the scope of their impact. The distinction between these two categories is not merely descriptive but carries important legal implications. It provides a normative foundation for determining the threshold at which a digital activity can be classified as a cybercrime. Specifically, this prevents the overgeneralization of all digital activities as criminal acts, thereby ensuring that only activities involving unlawful conduct and falling within recognized categories can be legally classified as cybercrimes. Therefore, this framework is crucial in assessing evolving digital practices, particularly in contexts where the boundary between legitimate digital activities and potential cybercrimes remains a subject of ongoing discourse.

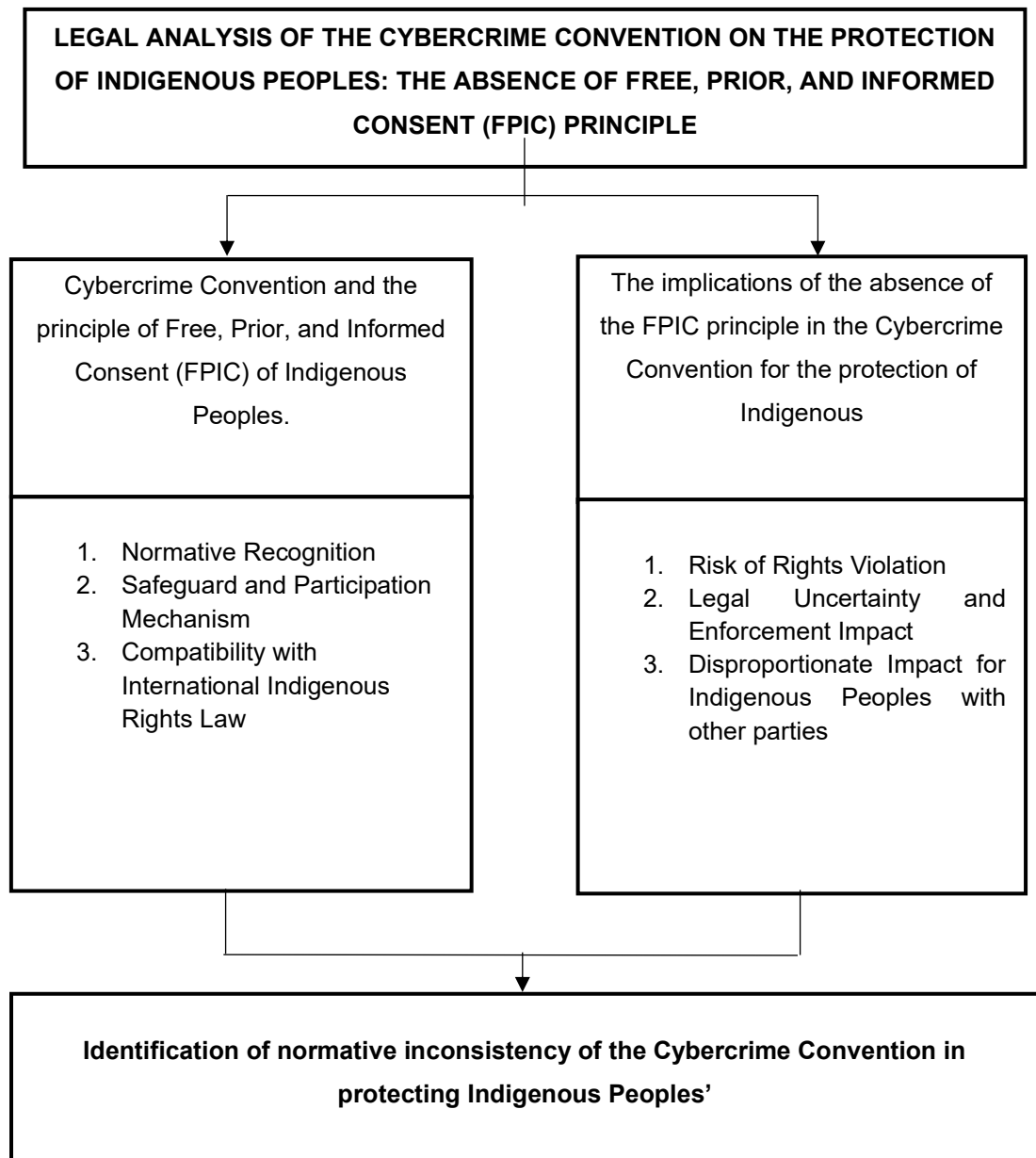
F. Analytical Framework

This research employs a normative legal analytical framework to examine the relationship between the United Nations Cybercrime Convention (Hanoi Convention) and the principle of Free, Prior and Informed Consent (FPIC) of Indigenous Peoples. The analysis is conducted by positioning FPIC as a recognized principle of international human rights law and assessing its relevance and protection within the international cybercrime legal regime for Indigenous Peoples. The analytical framework begins with an examination of the legal norms contained in the United Nations Cybercrime Convention, particularly provisions related to state authority in cybercrime prevention, investigation, and enforcement. This stage aims to identify whether and to what extent the Convention explicitly or implicitly accommodates the principle of FPIC in relation to Indigenous Peoples.

Subsequently, the analysis incorporates international human rights instruments, such as the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) and other relevant human rights standards, as normative benchmarks. Through this approach, the research evaluates the consistency between the cybercrime legal regime and international human rights law,

³⁴ *Ibid.*, p. 9-12.

focusing on the absence of explicit FPIC provisions and the potential normative gap arising from such absence. Furthermore, this research analyzes the implications of the identified normative gap for the protection of Indigenous Peoples. Based on the results of the normative analysis, this research draws conclusions regarding the extent to which the principle of FPIC is protected under the current international legal frameworks for indigenous peoples.

CONCEPTUAL FRAMEWORK

G. Operational Definitions

The operational definitions are formulated to establish clear boundaries for each variable used in this study. The formulation of these definitions aims to prevent differences in interpretation and ensure that the discussion remains focused and consistent with the established research focus. These definitions were compiled taking into account the needs of Legal Analysis of the United Nations Cybercrime Convention in Relation to the Principle of Free, Prior and Informed Consent (FPIC) of Indigenous Peoples in Indonesia, so that they are relevant to the framework and focus of the research discussed.

1. Cybercrime

Cybercrime is divided into two categories, Cyber-Enabled and Cyber-Dependent. These terms refer to all forms of criminal activity carried out by exploiting information technology, computer systems, or digital networks as tools, including activities such as the theft and misuse of personal or collective data, unauthorized access to electronic systems, and the use of technologies such as digital mapping without the consent of the relevant authorities.

2. Cyber- Enabled Crime

Cyber-Enabled Crime is a form of conventional crime whose commission is expanded, facilitated, or scaled up through the use of information and communication technology, where technology serves as a means to enhance the effectiveness of criminal acts, such as data theft and the exploitation of digital information.

3. Cyber- Dependant Crime

Cyber-Dependant Crime is a form of non-conventional crime that can only occur through the use of information and communication technology, in which computer systems, networks, or digital devices serve as both the primary means and the target of criminal activity, such as hacking, the distribution of malware, and attacks on cybersecurity.

4. United Nations Cybercrime Convention

The United Nations Cybercrime Convention refers to the international legal instrument adopted under the auspices of the United Nations that regulates the criminalization of cyber offences, international

cooperation, jurisdiction, and cross-border investigative measures. Operationally, the Convention is examined insofar as its enforcement mechanisms and regulatory provisions may affect the digital rights, autonomy, and collective interests of Indigenous Peoples.

5. Free, Prior, and Informed Consent (FPIC)

Free, Prior, and Informed Consent (FPIC) refers to the right of Indigenous Peoples to meaningfully participate, influence, and consent to legal or policy measures that may affect their collective rights, territories, resources, or digital interests.

6. Indigenous Peoples

Indigenous Peoples refer to distinct social and cultural communities possessing historical continuity, collective identity, and customary governance systems, whose rights and interests may be directly or indirectly affected by international cybercrime regulation and digital enforcement measures.

7. Protection of Indigenous Peoples' Rights

Protection of Indigenous Peoples' rights refers to legal, procedural, and institutional safeguards designed to prevent violations of their collective and individual rights, as well as mechanisms aimed at ensuring accountability, participation, and remedies in situations where cybercrime regulation or digital governance measures may impact them.

8. Digital Governance

In this research, digital governance refers to the system of rules, institutional practices, and enforcement mechanisms that regulate activities in cyberspace, including data management, surveillance, information exchange, and cross-border digital cooperation. It is understood as the regulatory environment within which state authorities exercise power in addressing cybercrime.

9. Cross-Border Data Access

Cross-border data access refers to the ability of law enforcement authorities to obtain digital data stored or transmitted outside their territorial jurisdiction. In this research, it is examined in relation to its

potential implications for jurisdictional authority, sovereignty, and the protection of collective rights of Indigenous Peoples.

10. Collective Rights

Collective rights refer to rights that are held and exercised by a group rather than by individuals alone. In this research, collective rights primarily concern the shared cultural, territorial, social, and decision-making interests of Indigenous Peoples that may be affected by international cybercrime regulation.

11. Procedural Safeguards

Procedural safeguards refer to mechanisms that ensure fairness, accountability, and oversight in the implementation of legal measures.

12. Digital Rights

Digital rights refer to the extension of fundamental rights and freedoms into the digital sphere. In this research, digital rights encompass issues of privacy, data protection, participation, access to information, and protection from disproportionate surveillance, particularly in relation to Indigenous Peoples.

CHAPTER II RESEARCH METHODOLOGY

A. Type of Research

In this research, the author will use research methods to bridge the gap between the issues raised. Research methods are defined as a set of rules, activities, and procedures used in a particular discipline.³⁵ This research adopts a normative legal research method, which focuses on the analysis of legal norms, principles, and doctrines contained in international legal instruments and national laws. This normative method, also known as research in law, is considered the most appropriate method in legal research.³⁶

B. Type and Sources

This study employs a normative legal research methodology using conceptual and statutory approaches. This approach was chosen to analyze the extent to which the provisions of the United Nations Cybercrime Convention relate to the principle of Free, Prior, and Informed Consent (FPIC), and also to examine the legal implications of the absence of explicit provisions regarding this principle for the protection of Indigenous Peoples. Within this framework, the study focuses on analyzing relevant legal norms, principles, and doctrines. A conceptual approach is used to gain a deeper understanding of the concept of FPIC as part of the human rights protection framework, particularly Indigenous Peoples' collective rights to self-determination, data sovereignty, and the management of traditional knowledge. This approach also allows researchers to examine the development of legal doctrines related to data sovereignty and how these concepts intersect with the interests of Indigenous Peoples in the digital context. Meanwhile, the legislative approach is used to examine various relevant legal instruments, both at the international and national levels, to identify whether or not the FPIC principle is recognized and the forms of protection provided.

To support a comprehensive analysis in this study, various types of legal materials were utilized, classified according to their level of authority and

³⁵ Kadarudin, 2021, *Penelitian di Bidang Ilmu Hukum (Sebuah Pemahaman Awal)*, Makassar: Formaci, p. 12.

³⁶ Irwansyah, 2020, *Penelitian Hukum: Pilihan Metode dan Praktik Penulisan Artikel*, Yogyakarta: Mirra Buana Media, p. 96.

function. This classification is essential to ensure that every argument constructed has a strong, systematic legal foundation and is academically accountable. By grouping legal materials into primary, secondary, and supporting sources, this study seeks to integrate authoritative sources with academic literature and conceptual references to gain a comprehensive understanding of the relationship between cybercrime regulations and the protection of Indigenous Peoples' rights. Thus, this categorization of legal materials serves not only as a foundation for conducting normative analysis but also as a framework for critically assessing the extent to which the principle of Free, Prior, and Informed Consent (FPIC) is accommodated both explicitly and implicitly in the legal instruments under study. Furthermore, the types and sources of legal materials used in this study can be outlined as follows:

1. Primary Legal Materials

Primary legal materials consist of binding and authoritative legal instruments that form the core basis of the analysis. These include:

- The United Nations Cybercrime Convention, in this research, refers to the international legal instrument adopted under the auspices of the United Nations that regulates international cooperation, criminalization, and law enforcement mechanisms in addressing cybercrime. Operationally, this Convention is examined through its normative provisions, including jurisdiction, cross-border data access, human rights safeguards, and international cooperation, insofar as these provisions affect the digital rights and interests of indigenous peoples. The United Nations Convention against Cybercrime was adopted by consensus through General Assembly resolution 79/243 of 24 December 2024.³⁷;
- United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) and International Labour Organization (ILO)

2. Secondary Legal Materials

Secondary legal materials are used to provide explanations, interpretations, and critical perspectives on primary legal materials,

³⁷ United Nations, *United Nations General Assembly Resolution A/RES/79/243 on the United Nations Convention against Cybercrime* (adopted 24 December 2024)

thereby supporting a more comprehensive legal analysis. These materials include:

- Academic Literature, scholarly books and peer-reviewed journal articles on international law, international human rights law, cyber law, and indigenous rights.
- Previous Scholarly Research, undergraduate theses, master's theses, and doctoral dissertations that examine cybercrime regulation, indigenous data protection, digital sovereignty, and related legal challenges;
- Doctrinal and Expert Writings, legal opinions and analyses by recognized scholars and experts in international law, particularly those addressing state sovereignty, cyber governance, indigenous rights, and collective data protection;
- Policy-Oriented Articles and Reports, publications issued by international organizations, research institutions, and policy bodies that provide contextual insights into global cybercrime governance and indigenous digital rights.

3. Supporting Legal Materials

Supporting legal materials are used to facilitate conceptual clarity and ensure terminological precision in the analysis. These materials include:

- Legal dictionaries, which are used to clarify and ensure the consistent interpretation of legal terminology and technical concepts related to international law, cyber law, and indigenous peoples' rights, particularly in addressing evolving terms within the digital context;
- Encyclopedias of international law, employed to obtain authoritative explanations of legal doctrines, principles, and the historical development of international legal norms relevant to indigenous rights and cyber governance;
- Legal indexes, bibliographies, and academic legal databases, utilized to identify, access, and cross-reference scholarly legal writings, journal articles, and authoritative commentaries that support the doctrinal analysis of Indigenous Digital Sovereignty;

- Official publications and websites of international organizations, including the United Nations.

C. Legal Material Collection Techniques

The data collection in this research is performed through a literature review method, which entails the systematic search and critical analysis of various sources such as statute, declaration, international covenant, international documents, books, previous research findings, academic magazines, scientific, and scholarly journals relevant to the research topic. This approach is applied to thoroughly examine the research problem. Legal materials are gathered by conducting data collection and identification of legal provisions, followed by categorizing and methodically organizing the legal materials according to the research issues. The process involves reading, analyzing, taking notes, and compiling reviews of the materials that are pertinent to the research questions. This method emphasizes a structured and logical approach to legal study, aiming to deliver an in depth and accurate analysis supporting well founded conclusions. The literature review method is especially appropriate for normative legal research that concentrates on the evaluation of legal regulations, doctrines, and related literature to produce valid and credible academic work.

D. Analysis of Legal Materials

The collected legal materials are analyzed using normative legal analysis. This method emphasizes the examination of legal norms, principles, and doctrines through a structured and reasoned interpretation of applicable legal instruments. The analysis is conducted by interpreting legal norms both systematically and contextually, in order to understand not only the textual meaning of the provisions but also their position within the broader framework of international law. A systematic interpretation is employed to examine the coherence and interrelation between provisions within the United Nations Convention on Cybercrime and other relevant international legal instruments, while a contextual interpretation is used to assess the purpose and underlying values of these norms, particularly in relation to human rights protection and Indigenous Peoples' rights.

This study employs a comparative approach by comparing the provisions of the UN Convention on Cybercrime with other international instruments, such as

the UN Declaration on the Rights of Indigenous Peoples (UNDRIP) and relevant International Labour Organization (ILO) standards, to identify the extent to which the principle of Free, Prior, and Informed (FPIC) are recognized or disregarded. Through this comparison, this study seeks to highlight inconsistencies, overlaps, or gaps between various legal regimes, particularly between the frameworks of cyber governance and the protection of indigenous peoples' rights.