International Journal of Educational Review, Law & Social Sciences (IJERLAS)

International Journal of Educational Review, Law And Social Sciences (IJERLAS Journal) | ISSN (e): 2808-487X
Volumes 5 No. 4 (2025)

APPLICATION OF THE EXTRATERITORIAL PRINCIPLE IN CROSS-BORDER CYBER CRIME JURISDICTION RELATING TO PERSONAL DATA

Nopit Ernasari
Program Studi Ilmu Hukum, Fakultas Hukum Universitas Pamulang
Corresponding E-mail: dosen02988@unpam.ac.id

Received : 21 May 2025	Published : 14 July 2025
Revised : 30 May 2025	DOI : https://doi.org/10.54443/ijerlas.v5i4.3267
Accepted : 16 June 2025	Link Publish : https://radjapublika.com/index.php/IJERLAS

Abstract

The development of information technology has encouraged the occurrence of transnational cybercrime, especially those related to violations of personal data. In this context, the application of the extraterritorial principle is important to fill the jurisdictional gap and ensure that perpetrators do not escape legal responsibility simply because they are outside the territory of the victim's country. The extraterritorial principle is an important legal instrument that allows a country to enforce its laws against perpetrators outside its territorial territory, especially when its citizens' personal data becomes the object of attack. This study analyzes how the extraterritorial principle can be applied in jurisdiction against transnational cybercrime involving violations of personal data, and to what extent the territorial principle is effective in protecting citizens' personal data from the threat of cross-border cybercrime, as well as the importance of cooperation between countries. This study uses a normative juridical method with secondary data collected through literature studies in the form of laws and regulations, court decisions, books, journals and other scientific works related to the research topic. The results of this study are analyzed and then presented descriptively. The results of the study show that the application of the extraterritorial principle still faces various obstacles, ranging from jurisdictional conflicts to limited cooperation between countries. Nevertheless, this principle remains relevant and potential as part of a global legal strategy in dealing with cybercrime. Harmonization of international law and increased cross-country cooperation are needed to maximize the protection of personal data through the application of the extraterritorial principle.

Keywords: ***Extraterritorial Principle, Jurisdiction, Cybercrime, Personal Data***

INTRODUCTION

The Internet with its various new media platforms has become a ubiquitous social phenomenon. Like the telephone and television, the Internet has become a standard element in people's daily lives. The emergence of the Internet and the increasing use of information systems have brought about extraordinary changes in human life. The Internet with all its new media platforms has transformed growth in many countries, removing barriers to trade, and enabling people around the world to communicate, collaborate, and exchange ideas regardless of traditional barriers of class, geographic location, and time. The combination of the Internet, information systems, and interconnected people has created a global virtual realm. A new space that is virtual, but can meet the various needs of humanity, ranging from information needs, economic, social, political, and cultural interests. A space where almost all regions on planet earth can be connected and interact, namely cyberspace. (Nugroho, 2020). The development of information technology has made society also experience rapid and massive changes. In relation to the development of technology, the progress and development of information technology through the internet, human civilization is faced with new phenomena that are able to change almost every aspect of human life.(M. Arief Mansur, 2005)Many unexpected problems have arisen as a result of the rapid expansion of the internet, including significant legal disputes and conflicts for users. Due to its widespread use, the internet often raises legal problems, including: fraud, theft, hacking, and data destruction by viruses.(Zainal Arifin, 2023)

In this era, data/information is the most important commodity. Information becomes a commodity because it can be "traded" to gain profit either directly or indirectly from the use of the information/data. As a commodity, information is a new frontier in the concept of commercial transactions, starting from creating new commercial subjects whose value is difficult to know, to the need for in-depth discussion regarding the rights and obligations towards information as a commercial commodity.(Raymond T. Nimmer, 1992). Discussions on personal data

protection continue to increase, both at the international, regional and national levels. International and regional organizations issue recommendations that can be used as guidelines for member countries. These recommendations also influence the formation of personal data protection regulations in each country. Among them is The OECD Privacy Framework issued by the Organization for Economic Co-Operation and Development (OECD) in 1980 as revised in 2013. At the regional level in ASEAN, the Framework on Personal Data Protection was issued which was agreed upon at the ASEAN Telecommunications and Information Technology Ministers Meeting.

In the context of personal data protection, the terminology often used is "personal information" and "personal data". The United States uses the term personally identifiable information, while Europe uses the term personal data. In the current regulations in Indonesia, the terminology used is personal data. Personal data is defined as "any information relating to an identified or identifiable individual (data subject)" (OECD, 2013). The General Data Protection Regulation (GDPR) specifically describes the scope of personal data, including name, identity number, location data, online identifier, or one or more specific components related to the physical, physiological, genetic, mental, economic, cultural or social of a person. Furthermore, included in the scope of personally identifiable data in the GDPR is data that is unknown (pseudonymization) but with the use of additional information, is able to identify a person. Personal data protection is inseparable from the Lex Informatica norm which has been more manifested in communication and community interaction. A habit and continuous practice that has evolved into a legal institution is known in legal history as Lex Mercatoria or the law of merchants. Lex Mercatoria independently institutionalizes jurisdictional sovereignty and provides assurance to commercial actors about the true justice in their transactional relationships.(Harlod J. Berman, 1978)The thing in question has a similar identification with the formation of norms for the flow of information through technology and communication networks in forming the legal institution of Lex Informatica or Information Law. Lex Informatica must be understood as a consciously important need and needs to be understood as a consciously important need and needs to be recognized by policy makers and regulators in each country.

Lex Informaticahas a series of special characteristics that can flexibly advance the objectives of information management policies. The formulation of Lex Informatica as a regulation has avoided many difficulties with significant conflicts and uncertainties inherent in its legal resolution. Lex Informatica offers a modern way to deal with a legal regime, namely the regulation of internet content, the distribution and misuse of personal data, and the protection of intellectual property in the global network. Lex Informatica has three forms of special characteristics for establishing information management policies and the preparation of regulations in the information society.(Reidenberg, 1998)First, Lex Informatica as a technology regulation does not depend on national borders. Second, Lex Informatica allows for regulation customization with a variety of technical mechanisms. Third, Lex Informatica as a technology regulation benefits from the integration of independent enforcement and internal monitoring. From the explanation above related to Personal Data, the author will discuss how the extraterritorial principle is regulated and applied in jurisdictions against cross-border cybercrime involving personal data violations? And to what extent is the extraterritorial principle effective in protecting citizens' personal data from the threat of cross-border cybercrime?

RESEARCH METHODS

The method used to write this research is the juridical-normative research method. Normative juridical research is legal research conducted by examining library materials and secondary materials only through a review of laws and regulations and various literature related to the problems being studied.(Mamuji, 2013)The intended approach is carried out by using library research methods and comparative approaches. The conceptual method needed to research this is by using understanding through literature obtained from books, journals, and previous research results, so that the collection of data sources through books or printed or online media collected to be able to provide an overview of the results that will later become references in this writing.

DISCUSSION

Extraterritorial Principle Regulated and Applied in Jurisdictions Against Transnational Cybercrimes Involving Personal Data Breaches

The presence of the state through Law Number 27 of 2022 concerning Personal Data Protection (PDP) as Lex Digitalis Habeas Data in Indonesia, is a manifestation of the achievement of the goals of the Unitary State of the Republic of Indonesia as stated in the Preamble to the 1945 Constitution, namely to achieve order and justice which are classical functions of law, and function as a means of renewing society influenced by digital technology.(Budhijanto, 2023). Based on Law No. 27 of 2022 concerning Protection of Personal Data, personal data is data about an individual who is identified or can be identified individually or combined with other information

either directly or indirectly through electronic or non-electronic systems, while the Subject of Personal Data is an individual to whom Personal Data is attached.(Erlina Maria, 2020). The Theory of Personal Data Protection Law articulates Lex Digitalis Habeas Data as a law that regulates the area of personal data protection that takes place within the territory of a country related to the jurisdiction of the National Personal Data Protection Law, including regulating legal norms that are mandatory in nature. Lex Digitalis Habeas Data which is mandatory in nature is binding for national (domestic) substances as the purpose of forming legislation and is binding so as to ensure that personal data protection runs smoothly, quickly, or effectively.

Law No. 27 of 2022 concerning Protection of Personal Data adopts an extraterritorial (virtual) jurisdiction regime as stated in Article 2 as follows:

(1) The Personal Data Protection Law applies to every person, public body, and international organization that carries out legal acts as regulated in the Personal Data Protection Law:
    a. Which is located in the legal territory of the Republic of Indonesia; and
    b. Outside the jurisdiction of the Republic of Indonesia, which has legal consequences:
        1. In the jurisdiction of the Republic of Indonesia; and/or
        2. For Personal Data subjects who are Indonesian citizens outside the jurisdiction of the Republic of Indonesia.

(2) Law No. 27 of 2022 concerning Protection of Personal Data does not apply to the processing of Personal Data by individuals in personal or household activities.

The types of personal data are contained in the Personal Data Protection Law, Article 4, as follows:

a. Personal data of a specific nature; and
   Specific personal data is personal data which, when processed, can result in a greater impact on the personal data subject, including acts of discrimination and greater losses to the personal data subject.
b. General Personal Data.
   As referred to in Article 44 of the Personal Data Protection Law, paragraph (1) letter a includes:
    a) Health data and information,
    b) Biometric data;
    c) Genetic data;
    d) Crime record;
    e) Child data;
    f) Personal financial data;
    g) Other data in accordance with the provisions of laws and regulations

(3) General personal data as referred to in Article 4 of the Personal Data Protection Law, paragraph (1) letter b includes:
    a) Full name;
    b) Gender;
    c) Citizenship;
    d) Religion;
    e) Marital status; and/or
    f) Personal data combined to identify an individual.

Personal data regulation is necessary because it regulates the procedures for collecting, using, disclosing, sending and securing personal data and is important in socio-political relations where there are two interests that are vis-à-vis conflicting, where on the one hand the community needs protection for the privacy of its personal data and on the other hand the government and business actors need data from the wider community to be processed and used for reasonable and lawful purposes.

Jurisdiction is defined as the legal power or competence of a state over persons, objects, or legal events. This jurisdiction is seen as a reflection of the basic principles of state sovereignty, equality of state status, and the principle of non-interference. Jurisdiction is seen as a vital and central form of sovereignty that can change, create, or end a legal relationship or obligation.(Shaw, 1986)

Jurisdiction is the power or legal competence of a state over people, objects or events (law). State jurisdiction cannot be separated from the principle of state sovereignty, a logical consequence of the principle of state sovereignty, because the state has sovereignty or supreme power within its territorial boundaries (territorial sovereignty).

Jurisdiction is a consequence arising from the recognition of the sovereignty of a state entity, where a political entity like a state must have both internal and external sovereignty. External sovereignty can be understood as having an equal stance with other countries in accordance with the principle of sovereign equality that we know

today.(Jawahir Thontowi, 2016)The consequence of this equality of status is that countries have several statuses such as:

a. A jurisdiction over its territory and the citizens inhabiting it;
b. The obligation for other countries not to interfere in affairs or problems occurring in the territory of other countries;
c. The emergence of obligations resulting from international customs and international agreements based on the will of the country itself.(Brownlie, Principles of Public International Law, 1990)

In its development, the principle of jurisdiction adapts to facilitate countries in responding to problems that occur in the global world. An example is transnational organized crime or organized crime between countries where the nature of the principles of jurisdiction can clearly hinder the enforcement of the crime. As Mann said, the problems of modern life create a reluctance to locate a fact, incident or event that causes a solution based on a focus based on territorial connections will not produce a solution that meets the needs of the country.(Mann, 1964) In general, international jurisdiction can be divided into 2, namely territorial jurisdiction and extraterritorial jurisdiction. Territorial jurisdiction is a law applied within the borders of a country, while extraterritorial jurisdiction is the jurisdiction of a country applied outside the borders of its country and on the high seas. The Extraterritorial Principle is a principle that adheres to the fact that a country's territory outside the country is recognized as its territory based on international law. If related to the context of the PDP Law, the PDP Law does not only apply to every legal subject in the legal territory of Indonesia, but also binds outside the territory of the Republic of Indonesia which has legal consequences:

1. In the jurisdiction of the Republic of Indonesia; and/or
2. For Indonesian citizen personal data subjects outside the jurisdiction of the Republic of Indonesia.

This indicates that the Personal Data Protection Law is closely related to state sovereignty, territory, and jurisdiction. Digital transformation has become a real manifestation of the impact on the very intense transfer of personal data between countries. Therefore, this Law applies the principle of extraterritorial jurisdiction in its provisions in Article 2 of the Personal Data Protection Law. This provision grants jurisdictional rights and authority to the state to apply this Law to all legal acts carried out outside the territory of the Republic of Indonesia but has an impact domestically.

The Effectiveness of the Extraterritorial Principle in Protecting Citizens' Personal Data from Cross-Border Cybercrime Threats

It is impossible to categorize cybercrime as domestic crime or only affiliated with one country's territory. The phenomenon of internetization has resulted in global network interconnection where even if one node/connection point is destroyed the network will still run with other nodes, which makes this structure a major force for perpetrators of cybercrime that is carried out transnationally.(Stahl, 2011). This interconnection results in several weaknesses in terms of prevention and enforcement, namely:(Rawat, 2021)First, the potential for global targets while connected to the internet and second, the disparity in domestic cybercrime regulations with weak international cooperation regarding enforcement and prevention of this type of crime results in one of the factors that make it difficult to enforce cybercrime. As one of the critics related to the enforcement of cybercrime states that the transnational nature of cybercrime represents a major challenge for world governments, because the shift from material and physical environments to immaterial or intangibles results in classical/traditional legal dogmas being unsuitable for application.(Gianpero Greco, 2021)

Extraterritorial jurisdiction speaks of the legal capacity of a country to exercise its sovereignty/authority outside its territory. At the implementation level, the application of the principle of extraterritorial jurisdiction will certainly encounter a number of obstacles, especially when it intersects with the jurisdiction of another country. The principle of extraterritorial jurisdiction may not be fully implemented because a country in reality cannot exercise its power in the territory of another country even though it has jurisdiction over a legal act, legal subject/object, and certain legal interests. The application of extraterritorial jurisdiction and intensive international cooperation is generally carried out for the investigation and enforcement of cyber crimes in the form of personal data theft. Regulations related to jurisdiction are an integral part of enforcement in the cyber field as a transnational crime. It is stated in Article 22 concerning jurisdiction where in addition to the application of jurisdiction in matters that are usually applied in general, this convention adheres to the principle of active personality in resolving the application of extraterritorial jurisdiction with the condition that there is dual criminality.

Regulations related to theft of personal data. This can be found in chapter 13 concerning the prohibition on the use of personal data in Law No. 27 of 2022 concerning the Protection of Personal Data in Article 65 which reads:

1) Every person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him/her with the intention of benefiting himself/herself or another person which may result in loss to the personal data subject.
2) Every person is prohibited from unlawfully disclosing personal data that does not belong to him/her.
3) Every person is prohibited from unlawfully using personal data that does not belong to him/her.

As well as Article 65 in the same law which reads:

1) Every person is prohibited from creating false Personal Data or falsifying Personal Data with the intention of benefiting themselves or others which may result in loss for others.

In the event of theft or leakage of personal data, there is generally an obligation for the personal data controller to notify the owner of the personal data of this failure, known as Security Breach Notification, this is accommodated by Law No. 27 of 2022 concerning Personal Data Protection in Article 46 which reads:

1) In the event of a failure of Personal Data Protection, the Personal Data Controller is obliged to provide written notification no later than 3 x 24 hours to:
   a) Personal Data Subject; and
   b) institution.
2) The written notification as referred to in paragraph (1) must contain at least:
   a) Personal Data disclosed;
   b) When and how Personal Data is disclosed; and
   c) Efforts to handle and recover from disclosure of Personal Data by the Personal Data Controller.
3) In certain cases, the Personal Data Controller is obliged to inform the public about the failure of Personal Data Protection.

Regarding the failure of Personal Data Protection, this is explained as a failure to protect a person's Personal Data in terms of confidentiality, integrity and availability of Personal Data, including a breach of security, whether intentional or unintentional, which leads to the destruction, loss, alteration, disclosure or unauthorized access to Personal Data that is transmitted, stored or processed.

In this jurisdictional aspect, law enforcement officers experience various obstacles. There are several problems in dealing with cybercrime, namely as follows:

a. Cybercrime perpetrators are citizens who do not adhere to and apply the same laws as Indonesia

   In terms of jurisdictional aspects, especially in the case of cybercrime perpetrators who are citizens who do not adhere to and apply the same laws as Indonesia, this will make it difficult to combat transnational or cross-country cybercrime, while in terms of jurisdiction it has been regulated in Article 2 of Law Number 19 of 2016 amending Law Number 11 of 2008 concerning information and electronic transactions, namely: "This law applies to anyone who commits legal acts as regulated in this law, both in the jurisdiction of Indonesia and outside the jurisdiction of Indonesia which have legal consequences in the jurisdiction of Indonesia and/or outside the jurisdiction of Indonesia and are detrimental to the interests of Indonesia."

   The ITE Law has a jurisdictional scope not only for legal acts applicable in Indonesia and/or carried out by Indonesian citizens, but also applies to legal acts carried out outside the jurisdiction of Indonesia, either by Indonesian citizens (WNI) or foreign citizens (WNA) or Indonesian legal entities or foreign legal entities that have legal consequences in Indonesia, considering that the use of information technology for electronic information and transactions can be cross-territorial or universal.

b. Cybercrime perpetrators are citizens of countries that do not have diplomatic relations with Indonesia

   In terms of jurisdictional aspects, especially in this case, to combat transnational cybercrime, there will be difficulties, especially in cases of hacking where all countries in the world agree to prohibit this criminal act and each country makes laws to regulate and protect its citizens and their respective countries. In this case, investigators will have difficulties when handling cases of hacking crimes where the victims are Indonesian citizens or legal entities in Indonesia but the perpetrators are citizens of countries that do not have diplomatic relations with Indonesia. In this case, this will be an obstacle for cybercrime investigators in carrying out legal proceedings.

   In this obstacle, of course, the Indonesian government needs to consider things that allow cybercrime investigators in Indonesia to take action quickly considering that in cybercrime crimes, evidence/digital traces can be removed quickly and the perpetrators of cybercrime can get away without being caught by the law, especially in hacking cases that can cause losses to victims where the victims are not only individuals but also the state.(Prasetiyo, 2020)

CONCLUSION

The application of the extraterritorial principle in cross-border cybercrime jurisdiction related to personal data breaches, focusing on Law No. 27 of 2022 concerning Personal Data Protection (PDP) in Indonesia. The journal explains that the extraterritorial principle is regulated in Article 2 of the Personal Data Protection Law, which extends the reach of Indonesian law beyond its territorial territory. This provision applies to legal acts outside Indonesia that have legal impacts domestically, and the protection of personal data subjects of Indonesian Citizens (WNI) outside the territory of Indonesia. The application of this principle is driven by the transnational nature of cybercrime and the urgency of protecting personal data as a vital commodity in the digital era. The author asserts that the Personal Data Protection Law represents the Lex Digitalis Habeas Data law that is binding nationally and extraterritorially to ensure the effectiveness of data protection.

The effectiveness of the extraterritorial principle faces significant challenges. First, cybercrime is borderless and perpetrators are often located in countries with different regulations, giving rise to jurisdictional conflicts and difficulties in law enforcement. Second, disparities in regulations between countries and weak international cooperation hamper investigations, especially when the perpetrators are nationals without diplomatic relations with Indonesia or are in areas without extradition treaties. Technical obstacles such as the rapid removal of digital traces also complicate the collection of evidence. The journal concludes that although the extraterritorial principle in the Personal Data Protection Law is a progressive step, its optimization requires strengthening international cooperation and harmonization of global regulations to address the complexity of cross-border cybercrime.

REFERENCES

A. Buku

Budhijanto, D. (2023). Hukum Perlindungan Data Pribadi di Indonesia. Bandung: PT. Refika Aditama.

Jawahir Thontowi, P. I. (2016). Hukum Internasional Kontemporer. Bandung: PT. Refika Aditama.

M. Arief Mansur, E. G. (2005). Cyber Law Aspek Hukum dan Teknologi Informasi. Bandung.

Mamuji, S. (2013). Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta: Raja Grafindo Persada.

Nugroho, C. (2020). Cyber Society. Jakarta: Kencana.

Shaw, M. (1986). International Law. London: Butterworths.

Zainal Arifin, E. P. (2023). Cybercrime. Yogyakarta: Deepublish.

B. Jurnal

Brownlie, I. (1990). Principles of Public International Law. Clarendon Press, 227.

Erlina Maria, M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0. Jurnal RechtsVinding.

Gianpero Greco, N. M. (2021). The Phenomenon of Cybercrime: From the Transnational Connotation to the Need of Globalization of Justice. European Journal of Social Sciences Studies, 2.

Harlod J.Berman, C. K. (1978). The Law of Intenational Commercial Transaction. Lex Mercatoria, 221.

Mann. (1964). The Doctrine of Jurisdiction in International Law. Recueil des Cours de l'Académie de Droit International (RCADI), 36-37.

Prasetiyo, M. Z. (2020). Penegakan Hukum oleh Aparat Penyidik Cybercrime dalam Kejahatan Dunia Maya (cybercrime) di wilayah Hukum Polda DIY. Jurnal IJCLC.

Rawat, M. (2021). Transnational Cybercrime: Issue of Jurisdiction. International Journal of Law Management & Humanities, 254.

Raymond T. Nimmer, P. A. (1992). Informasi as a Commodity: New Imperatives of Commercial Law. Law and Contemporary Problems, 103.

Reidenberg, J. R. (1998). The Formulation of Information Policy Rules Thouh Technology. Lex Informatica, 533.

Stahl, W. M. (2011). The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. 40 GA. Journal of. INT'L & COMP. Law , 252.

C. Website

Prinsip Ekstrateritorial dalam UU PDP: Tantangan dan Implikasinya Diakses Pada Minggu, 15 Juni 2025, Pukul 16.00 WIB

Yuridiksi Ekstrateritorial sebagai Upaya Pelindungan Data Pribadi Lintas Negara di Era Internet of Things (IoT) | HeyLaw Diakses Pada Minggu 15 Juni 2015, Pukul 16.34 WIB

https://diskumal.tnial.mil.id/fileartikel/artikel-20180511-152350 Diakses pada Minggu 15 Juni 2025, Pukul 16.00 WIB