Uti Possidetis: Journal of International Law
ISSN 2721-8333 (online); 2721-8031 (print)
Vol. 5 No. 1 (2024): 106-139

Application of The Principles of Extraterritorial Jurisdiction Towards Personal Data Breach Committed Cross-Country Borders

Mohammad F.R Ba'abud, Dodik Setiawan Nur Heriyanto
Faculty of Law Universitas Islam Indonesia
**Corresponding author* : dodiksetiawan@uii.ac.id

Submission : 16 September 2023
Revision : 05 Oktober 2023
Publication : 19 Februari 2024

Abstract
The era of digitalization nowadays has resulted huge impact to the society daily life. However, at the same time it also has negative effecy by emerging a very complex cybercrime. One of the most commonly occurring cybercrimes is personal data breach. In light of Law No. 27 of 2022 regarding the Protection of Personal Data, which has extraterritorial application, it is essential to critically assess the jurisdiction applied to offenders involved in transnational personal data breach. The writer conducted normative research for this study, utilizing statutory, conceptual, and comparative analysis. This research uses Law No. 27 of 2022 as the analytical tool for domestic regulation towards the existing multilateral frameworks within international law pertaining to the enforcement of personal data breach. The research leads to the conclusion that a domestic regulation with extraterritorial traits alone is not the ultimate solution for successfully applying extraterritorial jurisdiction for transnational offenders. In summary, an international framework that promotes and sustains intensive international cooperation is necessary to effectively enforce extraterritorial jurisdiction against offenders involved in transnationally committed personal data breach.

Keywords: *cybercrime, extraterritorial jurisdiction, personal data protection, transnational crime.*

Abstrak
Era digitalisasi saat ini telah membawa dampak yang sangat besar terhadap kehidupan masyarakat sehari-hari. Namun, pada saat yang sama juga memberikan dampak negatif dengan munculnya kejahatan siber (cybercrime) yang sangat kompleks. Salah satu kejahatan dunia maya yang paling umum terjadi adalah pelanggaran data pribadi. Mengingat Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mempunyai penerapan ekstrateritorial, maka penting untuk menilai secara kritis yurisdiksi yang diterapkan terhadap pelanggar yang terlibat dalam pelanggaran data pribadi transnasional. Penulis melakukan penelitian normatif untuk penelitian ini, menggunakan analisis undang-undang, konseptual, dan komparatif. Penelitian ini menggunakan Undang-Undang Nomor 27 Tahun 2022 sebagai alat analisis regulasi dalam negeri terhadap kerangka multilateral yang ada dalam hukum internasional terkait penegakan pelanggaran data pribadi. Penelitian ini mengarah pada kesimpulan bahwa peraturan sifat domestik dengan ekstrateritorialitas saja bukanlah solusi akhir untuk berhasil menerapkan yurisdiksi ekstrateritorial bagi pelanggar transnasional. Singkatnya, kerangka kerja internasional yang mendorong dan mempertahankan kerja sama internasional yang intensif diperlukan untuk menegakkan yurisdiksi ekstrateritorial secara efektif terhadap pelanggar yang terlibat dalam pelanggaran data pribadi yang dilakukan secara transnasional.

***Kata kunci**: kejahatan dunia maya; yurisdiksi ekstrateritorial; perlindungan data pribadi; kejahatan transnasional.*

A. Introduction

Technological developments have developed rapidly, starting with the change in human civilization which does everything manually to the digitalization and "internetization" of human activities with the concept of the

Internet of Things (IoT). IoT is a concept that expands the function of continuously connected internet connectivity.[1] In digitalized and "internetized" life, data/information has become a vital object in the continuity of a system. In fact, in modern society many people do not realize that the practical nature resulting from this concept is electronic transactions between developers and data/information, as an extension of the function of internet connectivity. This development also has implications for digital globalization, where borders between countries are increasingly fading and resulting in increasingly cross-border data flows.[2]

One of the negative realities of the convergence between the physical and virtual worlds was when the Republic of Indonesia was shocked by news regarding the leak of 1,304,401,300 SIM (Subscriber Identity Module) Card registration data or contained in a file of 87 GB (GigaByte) containing the Population Identification Number (NIK/*Nomer Induk Kependudukan*), telephone number, mobile operator used and also date of use.[3] This data is then bought and sold by an account called "Bjorka" on the site/forum "breached.co".

[1] Yoyon Efendi, "Internet of Things (IoT) "Sistem Pengendalian Lampu Menggunakan Raspberry PI Berbasis Mobile"," *Jurnal Ilmiah Ilmu Komputer* 4, no. 1 (2018): 19.

[2] Susan Lund, James Manyika, and James Bughin, "Globalization Is Becoming More About Data and Less About Stuff," Harvard Business Review, 2016, https://hbr.org/2016/03/globalization-is-becoming-more-about-data-and-less-about-stuff.

[3] Arrijal Rachman, "3 Miliar Data Sim Card Bocor, Kominfo: Baru 15-20 Persen Yang Cocok," Tempo.co, accessed September 5,

Until now, the government has still not been able to catch the perpetrator alias Bjorka, and one of the factors that makes it difficult to enforce crimes in the cyber sector is the difficulty of tracking down the perpetrators of these cyber crimes, especially considering the anonymity that is the nature of technological advances and information coupled with qualified expertise in this field will certainly increase the level of difficulty of prosecuting cyber crimes. Apart from Bjorka, we can also mention a series of cases such as the BPJS (Health Insurance) data leak, BSI (Indonesian Sharia Bank) data hacking, and the sale of E-HAC (Health Tracing) data.

The difficulty in prosecuting cyber crimes will of course also be related to problems related to the erosion of regional classification and territorial jurisdiction. In accordance with Debra L. Shinder's, "cybercrime cases, more than most others, often involve complex jurisdictional issues that can present both legal and practical obstacles to prosecution.[4] The difficulty in prosecuting cybercrime in the realm of jurisdiction is greatly influenced by the model of cybercrime itself, namely borderless (without borders) and anonymous

2023, https://bisnis.tempo.co/read/1630609/13-miliar-data-sim-card-bocor-kominfo-baru-15-20-persen-yang-cocok#:~:text=Senin%2C 5 September 2022 14%3A48 WIB&text=Dari hasil penelusuran sementara dengan,data SIM Card yang bocor.

[4] Sigid Suseno, "Pengaturan Dan Penegakan Hukumnya Di Indonesia Dan Amerika Serikat," *Jurnal Ilmu Hukum Padjajaran* 33 (2009): 41–42.

(unknown). The potential for cybercriminals to be anywhere as long as there is an internet network makes the world globally a place for cybercriminals, and the anonymity of the perpetrators themselves where the perpetrators usually cannot be recognized or traced using conventional methods for finding traces of cybercrime.

As a consequence, this makes the principle of conventional jurisdiction where the state only has absolute authority to apply its laws in a limited way within its own territory, outdated and irrelevant, as Gercke that "it is difficult to base cooperation in cybercrime based on traditional principles of mutual legal assistance. The formal requirements and the time needed to collaborate with foreign law-enforcement agencies often hinder investigations".[5]Formal requirements and the time required to cooperate with foreign law enforcement agencies often hinder the progress of the investigation process. For example, data that is vital for tracking criminals is often deleted or hidden not long after the incident is committed, causing coordination between state

[5] Gercke, "The Slow Wake of a Global Approach Against Cybercrime," *Computer Law Review International*, 2006, 142. Mutual Legal Assistance is a form of agreement between countries that provides a legal basis for countries to request and/or provide assistance related to transnational criminal matters in matters relating to the process of investigation, prosecution and examination so that perpetrators can be subject to the national laws of the country requesting the assistance. For further explanation, see "Law no. 1 of 2006 concerning Mutual Assistance in Criminal Matters", Art. 2 and 3.

law enforcement institutions as a procedural requirement to provide additional time for perpetrators to hide their tracks.[6].

Law No. 27 of 2022 concerning Personal Data Protection takes the European Union's General Data Protection Regulation (GDPR) as one of the basic references for privacy law from the standards for establishing personal data protection regulations[7]. We can compare the implementation of this from the scope of the subject to which this law applies, where the Indonesian government has boldly emphasized in Law No. 27 of 2022 on Personal Data Protection which enforces national regulations regarding personal data by applying the principle of passive nationality as stated in article 2 paragraph (1) point b which states that this Personal Data Protection Law applies to every person, legal entity or organization internationally, both within and outside the jurisdiction of Indonesia as long as the action has legal consequences in the jurisdiction of the Republic of Indonesia or impacts personal data subjects of Indonesian citizens who are outside the jurisdiction of the Republic of Indonesia. However, enforcement regarding this matter is

[6] Marco Gercke, "Understanding Cybercrime: Phenomena, Challenges, and Legal Response," *International Telecommunications Union*, 2012, 77.

[7] Edmon Makarim, "Penelitian Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT) Dalam RDPU RUU PDP," n.d., https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200701-114522-4891.pdf.

certainly difficult if it is realized only by national law without correlating it with international law.

Formal requirements and the time required to cooperate with foreign law enforcement agencies often hinder the progress of the investigation process. For example, data that is vital for tracking criminals is often deleted or hidden not long after the incident is committed, causing coordination between state law enforcement institutions as a procedural requirement to provide additional time for perpetrators to hide their tracks.[8] Considering the various problems above, the author intends to write this research which focuses on both the regulation of cyber criminal acts of personal data breach carried out across national and international borders, as well as the application of the principle of extraterritorial jurisdiction as an answer to the enforcement of perpetrators of cyber crimes. related to personal data breaches across national borders.

B. Discussion

The phenomenon of internetization results in global network interconnection where even if one node/connection point is destroyed the network will continue to operate with other nodes, which makes this structure the main force for

[8] Gercke, "Understanding Cybercrime: Phenomena, Challenges, and Legal Response," 10–11.

perpetrators of cyber crimes committed transnationally.[9] This is also the fulcrum for regulations regarding cybercrime personal data breach, which can be carried out across national borders. In terms of enforcement, this phenomenon creates difficulties for the state in creating regulations that are suitable as preventive or repressive measures against perpetrators of cyber crimes across national borders.

This interconnection results in several weaknesses in terms of prevention and enforcement, namely:[10] First, the potential targets/targets globally as long as they are connected to the internet network and second, the disparity in the regulation of cyber crimes both domestically and the weak international cooperation regarding the enforcement and prevention of this type of crime results in one of the factors causing difficulties in the enforcement of cyber crimes. As one of the critics regarding the enforcement of cybercrime states that the transnational nature of cybercrime represents a major challenge for world government, because the movement from material and physical environments into the

[9] William M. Stahl, "The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. 40 GA.," *Journal of International and COMP. Law*, 2012, 252.

[10] Meetali Rawat, "Transnational Cybercrime: Issue of Jurisdiction," *International Journal of Law Management & Humanities* 4, no. 2 (2021): 254.

immaterial/intangible makes classical/traditional legal dogmas unsuitable for application.[11]

In 2005, four American citizens experienced theft of sensitive financial data resulting in a loss of $3,50,000, carried out by 3 employees of Citibank's BPO (Business Process Outsourcing) company in India.[12] Luckily, the Indian government was able to identify and follow up on this crime, even though the process of recovering losses between the two states was difficult. However, this illustrates the transnational nature of cyber criminal acts of personal data breach. We also have to imagine how enforcement will be for other crimes that are not followed up/identified and are not even known by the country where the perpetrator resides.

The intensive application of extraterritorial jurisdiction and international cooperation is generally carried out to investigate and enforce cyber crimes in the form of personal data breach. One example of the success of the formation of effective international cooperation is the disclosure of a cybercrime syndicate that attacked the technological infrastructure of several companies in France, Germany and Romania with a ransomware type attack, namely taking

[11] Gianpero Greco and Nicola Montinaro, "The Phenomenon of Cybercrime: From the Transnational Connotation to the Need of Globalization of Justice," *European Journal of Social Sciences Studies* 2, no. 1 (2021): 2.

[12] Vinita Bali, "Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?," *Temple International and Comparative Law Journal* 21, no. 103 (2007): 1.

company data hostage until a certain amount of money was paid, which resulted in losses of a certain amount. millions of euros. Investigation and enforcement were ultimately carried out by a joint team from Europol, the police of France, Germany, Romania and Switzerland with judicial assistance from the Eurojust institution. Although this investigation was fruitful, it is known that the two perpetrators who were caught were only part of a larger organizational scheme, facilitating software tools to carry out cyber attacks in other cybercrime cases.[13] Another case example is a financially motivated cyber attack on 1800 victims spread across 71 countries, with the method of stealing confidential data through malware or dangerous programs.[14]

Departing from this, we will examine the regulations related to cyber crimes of personal data breach both internationally and nationally to better understand the status quo of eradicating cyber crimes of personal data breach committed transnationally/across national borders.

[13] "European Union Agency for Criminal Justice Cooperation," Ransomware Gang Dismantled with Eurojust Support, 2021, https://www.eurojust.europa.eu/news/ransomware-gang-dismantled-eurojust-support.

[14] Henry Pope, "Organized Crime and Corruption Reporting Project," 2021, https://www.occrp.org/en/daily/15419-ukraine-switzerland-arrest-12-suspects-of-international-cybercrime.

1. Legal Instruments for Protecting Personal Data against Cyber Crime

In regulating cybercrime/cybercrime related to the theft of personal data, it will be easier to study international instruments initiated at the global and regional levels and their comparison with regulations at the national level, followed by an analysis of the harmony of these regulations in the context of prevention and/or enforcement of cyber criminal acts of theft of personal data.

A. International Instrument

There are several international instruments or basic guidelines that regulate the rights to protection of privacy, such as:

1) Universal Declaration of Human Rights

   This recognition is confirmed in article 12 of the Universal Declaration of Human Rights, which states that "No one shall be subjected to arbitrary interference in his personal, family and household affairs or correspondence, nor shall attacks be made against his honor and reputation." Everyone has the right to legal protection against such harassment or attacks."

2) International Covenant on Civil and Political Rights

   Protection of personal data is found in Article 17 which reads "(1) No one may be arbitrarily or unlawfully interfered with in his personal affairs,

family, home or correspondence, or unlawfully attacked on his honor and his good name. (2) Everyone has the right to legal protection against the interference or attacks mentioned above." Regarding this article, it is explained further in General Comment No. 16: Article 17 (Rights to Privacy) which explains that the collection and storage of personal information on computers, data banks and other devices, whether by public authorities or private individuals/entities, must be regulated by law.

3) Organization for Economic Co-Operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data.

It is a guideline created by the OECD Organization in 1980 and revised in 2013.[15] This instrument is vital because its non-binding nature and in the form of guidelines makes it easier for countries, especially developing countries at that time, to form regulations regarding the protection and transfer of data, including cross-border transfers. This guideline is divided into four parts, such as general rules, basic

[15] OECD, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD Publishing, 2002, https://doi.org/https://doi.org/10.1787/9789264196391-en.

principles for national use, basic principles for international use: free flow and legitimate restrictions, national implementation, and international cooperation.

4) Council of Europe Convention on Cybercrime

It is a convention initiated by the European Assembly but inviting non-member countries to participate in ratifying the convention. The European Convention on Cybercrime provides a draft of regulations specifically for cybercrime, one of which is personal data breach. This convention is also the only binding convention among many other international instruments regarding data protection and cybercrime. This convention has four chapters consisting of the use of terms (operational definitions), measures to be taken at the national level, international cooperation, and final provisions. The Chapter 2 of this Convention contains "offenses" for acts that are declared as cyber criminal acts, personal data breach can be annotated in the majority of the articles contained therein. In Chapter 2, in general, the relevance of data protection against cybercrime consists of offenses against the confidentiality, integrity, and availability of computer data and systems, and computer-related crimes.

5) Regional Instruments

Apart from the instruments above which are global, there are also instruments that are regional, with the example of Asia and Southeast Asia, namely the Asia-Pacific Economic Cooperation (APEC) Privacy Framework which was created in 2004 and revised in 2015, as well as the ASEAN Declaration to Prevent and Combat Cybercrime, a regional declaration that agrees on the need of countries in Southeast Asia for a legal instrument that accommodates cross-border law enforcement and enforcement of electronic evidence to combat cybercrime.[16]

B. National Instrument

Indonesia has Law No. 27 of 2022 on Personal Data Protection as the main legal umbrella in regulations related to data protection and also related to personal data breach, and this law will be our main analysis in discussing legal regulations related to personal data breach, especially in a transnational context. Law No. 27 of 2022 on Personal Data Protection, has a total of 76 articles in 15 chapters which refer to the following discussion:

[16] Asean Summit, "ASEAN Declaration to Prevent and Combat Cybercrime," Asean Summit, 2017, https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf.

1) Definition and types of personal data;
2) Rights of the data owner;
3) Processing of personal data;
4) Obligations of personal data controllers and personal data processors when processing personal data;
5) Transfer of personal data;
6) Administrative sanctions;
7) Prohibition of some uses of personal data;
8) Settlement of disputes regarding personal data;
9) International Cooperation;
10) Criminal provisions, and;
11) The role of government and the public.[17]

Getting to the heart of the problem, the regulations regarding the personal data breach has regulated specifically in chapter 13 concerning prohibitions on the use of personal data which reads:

1) Every person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him with the intention of benefiting himself or another person which could result in loss to the personal data subject.

[17] Muhammad Firdaus, "A Review of Personal Data Protection Law in Indonesia," Interdisciplinary Program of Information Security. Graduate School PKNU, 2022, https://osf.io/tmnwg/download.

2) Every person is prohibited from unlawfully disclosing personal data that does not belong to him.
3) Everyone is prohibited from unlawfully using personal data that does not belong to them.

As well as article 65 in the Law No. 27 of 2022 also reads: "Everyone is prohibited from creating false Personal Data or falsifying Personal Data with the intention of benefiting themselves or others which could result in harm to others."

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

The definition related to failure to protect Personal Data is explained as 'failure to protect a person's Personal Data in terms of confidentiality, integrity, and availability of Personal Data, including security breaches, whether intentional or unintentional, which leads to destruction, loss, alteration, disclosure, or access. unauthorized use of Personal Data that is sent, stored, or processed.[18] Then in certain cases it is 'if failure to protect personal data

[18] "Law No 27 of 2022 on Personal Data Protection" (n.d.), Art. 46 par. 1.

disrupts public services and/or has a serious impact on the interests of society. We can conclude that this obligation is binding not only on the private sector but also on government institutions that use personal data in their activities. This can be seen in article 2 (1) which states that:

1) This Law applies to every person, public body and international organization that carries out legal actions as regulated in this law:
    a) which is in the jurisdiction of the Republic of Indonesia; and
    b) outside the legal territory of the Republic of Indonesia, which has legal consequences:
        i. in the jurisdiction of the Republic of Indonesia; and/or
        ii. for Personal Data Subjects who are Indonesian citizens outside the jurisdiction of the Republic of Indonesia.

Apart from applying to every organ, both private and government, from this regulation we can also conclude that the government is trying to make this regulation extraterritorial in nature, provided that during the legal event, it has an impact on Indonesian citizens or other subjects under its auspices. This of course requires cooperation with other countries, especially in terms of

enforcement. The article 62 regulates 'international cooperation' which is stated that:

1) International cooperation is carried out by the Government with governments of other countries or International Organizations regarding the Protection of Personal Data.
2) International cooperation in the framework of implementing this Law is carried out in accordance with the provisions of statutory regulations and international legal principles.

This law applies in addition to forty-nine other sectoral regulations regarding the regulation of Personal Data Protection in Indonesia, where these regulations will become *lex specialis*, acting as the main reference when touching on data-related regulations in Indonesia.

C. Analysis of Personal Data Protection Arrangements in Indonesia in the Case of Personal data breach

There are several problems contained in Personal Data Protection regulations, especially Law No. 27 of 2022. The first problem is the correlation between Law No. 27 of 2022 on Personal Data Protection with the other sectoral laws in efforts to prevent and enforce personal data breach. Harmonization between these laws is vital considering that personal data correlations arise in these regulations, for example in the case of personal data

breach Law No. 27 of 2022 has four variables in Articles 65 and 66 which are considered personal data breach in the Article concerning the prohibition on the use of personal data, namely obtaining/collecting, disclosing, using and falsifying personal data that does not belong to them unlawfully.

Technical guidance is needed regarding various forms of obtaining/collecting, disclosing, using and falsifying personal data which are against the law, bearing in mind that Law No. 27 of 2022 is intended not only for conventional or non-electronic documents, but is intended for electronic documents so technical guidance is needed, where the absence of this guidance can result in confusion, definition errors, and enforcement errors by law enforcement officials. The absence of this guide will result in errors in the use of Law No. 27 of 2022, as happened to Law no. 11 of 2008 on Electronic and Information Transactions. In the Law No. 11 of 2008, which is actually intended as a regulation regarding electronic transactions and internet use, is used as an article on defamation.[19] This is caused by the unclear definition of privacy in legal substance, legal structure,

[19] Jihyun Park and Dodik Setiawan Nur Heriyanto, "In Favor of an Immigration Data Protection Law in Indonesia and Its Utilization for Contact Tracing," *Prophetic Law Review* 4, no. 1 (2022): 15.

and legal culture which determine the effectiveness of law enforcement.

The second problem is that the international cooperation launched by the government does not yet have a strong juridical basis. If making a reciprocal legal agreement becomes a solution, you can imagine how long it will take for law enforcement regarding data theft to be realized. Apart from that, these agreements have nothing in common with each other and have high variability because they have to adapt to the domestic laws of each country. An example is Law No. 5 of 2020 on the Ratification of Bilateral Treaty between Indonesia and Switzerland on Mutual Legal Assistance on Criminal Matters. Not to mention the main variable that in the case of cybercrime, it is very likely that the perpetrator is not in just one country, as is the mode of operation of cybercrime syndicates in general. As a result, it can be said that it is inappropriate to base cooperation specifically in enforcing data theft on this type of agreement.

The third problem is the absence of an independent data authority institution. As an example, the data authority institution model regulated in the European Union's General Data Protection Regulation, in Article 51 concerning Supervisory Authority, where each member country is obliged to create an independent public

authority responsible for supervising the implementation of the GDPR. If we compare it to the institution of the data supervisory authority designed in Law No. 27 of 2022, in Chapter IX on Institutional especially in Articles 58, 59, and 60 which explain the institutions responsible for data authority. It regulates that "(3) Institutions as intended in paragraph 2 are determined by the president", and "(4) Institutions as intended in paragraph 2 is responsible to the president." Furthermore, other provisions will be regulated in a Presidential Regulation according to paragraph 5 of the same article. In article 60, which explains the implementation of the authority of this institution with material in the form of formulating and establishing policies in the field of personal data, the imposition of administrative sanctions by the institution, models of cooperation with other countries' data protection institutions in enforcing cross-border data violations, and other materials. those listed in Article 60 will be regulated in Government Regulations.

If we compare it with the independence possessed by the GDPR data authority institution, by regulating both the duties and authority of this institution in this regulation, it will guarantee the strength and authority of the institution even when taking action against violations committed by state/public bodies. This will also determine the strength or adequacy of Law No. 27 of

2022, one example is when the United States in its report expressed concern over the use of data in the *Peduli Lindungi* application, which was used to collect people's personal data which allegedly did not have strong security in terms of storage and use.

In this case, if the data monitoring institution does not have legal independence, then the level of trust and legitimacy of supervision of public institutions is also vulnerable to legal bias. Another case that represents negligence on the part of the government in protecting personal data is the leak of E-HAC application data in August 2021 with a total of 1.3 million E-HAC user data being bought and sold on the dark web called raidforum. This proves weak supervision of data use by the government, which also requires independent supervision and control from a commission/data monitoring agency.

2. Implementation of the Principle of Extraterritorial Jurisdiction against Cyber Crime Perpetrators of Personal data breach Across National Borders

Law No. 27 of 2022 concerning Personal Data Protection is indeed extraterritorial. Likewise Law No. 19 of 2019 on the Amendment of the Law No. 11 of 2008 has already regulated

the extraterritorial scope of the law.[20] This arrangement also did not produce effective results in the enforcement of personal data breaches where both of them did not have any power in enforcing Indonesian jurisdiction outside Indonesian jurisdiction, with the absence of international legal instruments to determine Indonesian jurisdiction.

This can lead to impunity for perpetrators of cyber crimes committed transnationally, as in the case of the United States and the Philippines in 2000, namely the "I Love You" virus. This case began when a student in the Philippines, Onel de Guzman, designed a program to steal internet account passwords, scan computers for log-in passwords, destroy image and sound data, and spread a virus program automatically to all contacts in the email. As a result, this virus caused losses of 10 billion dollars, infiltrating the computer systems of at least 14 federal agencies in the United States, as well as the parliamentary systems of Britain, Belgium, and international organizations.[21] When de Guzman was tracked down, the Philippine government which initially prosecuted

[20] "Law No. 19 of 2019 Concerning Amendments to Law No. 11 of 2008 Concerning Information and Electronic Transactions" (n.d.). This Law applies to every person who commits legal acts as regulated in this Law, whether within the jurisdiction of Indonesia or outside the jurisdiction of Indonesia, which have legal consequences in the jurisdiction of Indonesia and/or outside the jurisdiction of Indonesia and detrimental to Indonesia's interests.

[21] Tech. of the H. Comm. on Sci, *The Love Bug Virus: Protecting Lovesick Computers from Malicious Attack: Hearing Before the Subcomm* (United State of America, 2000).

de Guzman had to withdraw its lawsuit because the Philippines did not have a law on computer hacking, while the United States government itself could not extradite de Guzman because the dual criminality/dual criminality requirements were not met. In the end, de Guzman received impunity for his actions.[22]

If we analyze it, the absence of an American legal basis to determine its jurisdiction is an obstacle to enforcing this case. From this reason, the author believes that the existence of a globally recognized legal instrument is one of the factors for the successful application of extraterritorial jurisdiction, especially in the field of cyber crime. In the Budapest Convention Article 27 concerning Procedures for the implementation of mutual legal assistance in the absence of international agreements/instruments,[23] where a legal basis is determined that can be used in the conditions of the United States and the Philippines, such as the absence of an international legal basis to use.

Issues related to jurisdiction are vital problems encountered in enforcement related to cyber crimes, due to geographical location, scale of the act, and other elements that

[22] Alexandra Perloff and Girles, "Transnational Cyber Offenses: Overcoming Jurisdictional Challenges," *Yale Journal of International Law* 43, no. 191

[23] "Convention on Cybercrime Procedure Pertaining to Mutual Assistance Request in the Absence of Applicable International Agreement,"

make cyber crimes different from other conventional crimes, making the implementation of jurisdictional principles difficult to apply. The difficulties in enforcing transnational crimes can be classified into three factors, namely difficulties in using evidence, difficulties in investigating, and difficulties in carrying out trials against transnational perpetrators.[24] As an answer to this difficulty, the Budapest Convention is a solution that can be used as a forum for implementing jurisdiction over cross-border cyber crimes. In this convention there are regulations related to jurisdiction which can be used as a benchmark for use and conflict in determination. Besides that. CoE is also a method of harmonization for regulations related to the enforcement of cyber crimes with specifications for determining the laws used, and accommodating international cooperation, extradition and other legal assistance.[25]

Meanwhile, in its enforcement function, Interpol has become a means of coordinating the enforcement of legal efforts related to cyber crimes, as well as training for member countries in handling cyber crimes. One example of the implementation of cooperation based on collaborative

[24] Ermanto Fahamsyah et al., "Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention," *Jurnal Hukum Dan Syariah De Jure* 14, no. 1 (2022): 150.

[25] "Budapest Convention on Cybercrime" (n.d.), Chapter III (International Cooperation).

enforcement is Operation Avalanche, a collaborative operation between Interpol and 30 other countries in uncovering and bringing down cyber criminal infrastructure which has resulted in losses worth 6 million Euros,[26] and operation Goznym, named after a piece of malware that was distributed to financial institutions and resulted in losses of over one hundred million USD, which succeeded in bringing down the cyber syndicate's network.[27] We can do this on the basis of having binding legal instruments that will accommodate international cooperation in enforcing cyber crimes, especially in the form of personal data breach, namely the Budapest Convention or Convention on Cybercrime.

The application of extraterritorial jurisdiction to foreign nationals who commit cyber crimes that have a transnational impact is also carried out by the United States against a cybercriminal group/organization that engages in carding, identity theft and theft of financial data which is then sold on a dark web site.[28] The arrest and closure of this organization

[26] "'Avalanche' Network Dismantled in International Cyber Operation," INTERPOL, n.d., https://www.interpol.int/ar/1/1/2016/Avalanche-network-dismantled-in-international-cyber-operation.

[27] EUROPOL, "Goznym Malware: Cybercriminal Network Dismantled in International Operation," European Union Agency for Law Enforcement Cooperation, n.d., https://www.europol.europa.eu/media-press/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation.

[28] United States District Court, Nevada: United States of America v Svyastoslav Bondarenko (2019).

was carried out in a joint operation called Operation Shadow Web, consisting of the United States, European countries, Australia and Asian countries. Perpetrators of crimes were arrested in several countries such as Australia, UK, France, Italy, Kosovo, Serbia and the United States in 2018.[29] One of the perpetrators, namely Syvastoslav Bondarkeno, who is a Ukrainian citizen, was charged and tried in the Nevada district court, United States based on his crimes using the extraterritorial application of the RICO statute (Racketeer Influenced and Corrupt Organizations Act). It is worth remembering that the United States is also a member of the Budapest convention, which facilitates coordination and use of enforcement instruments such as Interpol as mentioned in the press release from the United States ministry of justice.[30] Apart from Bondarkeno, the United States also prosecuted more than 30 other perpetrators from various countries, for example Macedonia, Egypt, Pakistan, UK, Ivory Coast, Australia, and others.

[29] "Thirty-Six Defendants for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrime," The United States Departemen of Justice (DoJ) Press Release, 2018, https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible.

[30] Budapest Convention on Cybercrime, Art. 27 par. 9 (b). Interpol is a transnational-based law enforcement coordination and communication instrument for member countries. "Any request or communication under this paragraph may be made through the International Criminal Police Organization (Interpol).

Enforcement of Article 2 of Law No. 27 of 2022 to apply extraterritorial jurisdiction to protect personal data for Indonesian citizens is just a dream without a legal instrument that accommodates this. Jurisdiction will remain a key issue in enforcing personal data breaches of transnational scope. This study then highlighted its importance as mentioned under the Budapest Convention in its preambule which stated: "Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation … Believing that an effective fight against cybercrime requires increased, rapid, and well functioning international co-operation in criminal matters"[31].

Which states on the basis of the necessity to pursue a similar criminal policy to protect society, where one way is to adopt adequate regulations and develop international cooperation, also that the fight against cyber crime requires increased, continuous and well-functioning international cooperation. As in practical, Indonesia needs specific regulation or guideline to enable this international cooperation or most importantly ratifying relevant international instruments.

[31] Budapest Convention on Cybercrime, Preambule.

C. Conclusion

Regulations regarding cyber criminal acts of personal data breach in Indonesia are covered by Law No. 27 of 2022 on Personal Data Protection, in addition to international provisions regarding data protection and cyber regulations such as the Budapest Convention. Contents in Law No. 27 of 2022 has regulations starting from the rights of data subjects, obligations of data subject processors and controllers, as well as regulations regarding data transfer traffic, institutional structure of data supervisors, prohibitions on data use, administrative and criminal sanctions, as well as provisions regarding international cooperation. As a result, this law is the right step for Indonesia, but it is not an end goal but rather a beginning for the protection of personal data. However, there are several critical notes for this law, especially in terms of preventing and enforcing personal data breach.

The first is the need to draft technical regulations regarding forms of violation of personal data so that they can serve as guidelines for law enforcement and the public in realizing the existence of cyber crimes. This aims to ensure that the authorities and the public know what is considered a criminal act, especially in matters of violation of personal data and not to be careless in applying the law. The second is a form of international cooperation designed in Law No. 27 of 2022 needs to be followed up with a good strategy to overcome the problem of personal data breaches both in the domestic and

transnational domains. Until now, Indonesia only has MLA agreements with several countries both in the Southeast Asia region and outside it as an instrument of international cooperation to apply extraterritorial law enforcement, but this method is very time-consuming and cost-inefficient, and its effectiveness of it has not yet been assessed. This agreement has relatively no impact on law enforcement in the cyber sector. The synergy between national and international legal instruments is decisive in making data protection against cyber crimes, especially personal data breaches carried out across national borders, optimal and sustainable.

Meanwhile, in terms of the application of extraterritorial jurisdiction to enforce against perpetrators of criminal acts of personal data breach committed across national borders as intended by Law No. 27 of 2022 in Article 2, this will be difficult to do without strong international instruments that accommodate state mobilization in enforcement, because the elements of cybercrime itself cannot be predicted, both the location and the potential scale of the act. The solution to this is to ratify the only binding convention related to cybercrime, such as the Council of Europe Convention on Cybercrime along with the second additional protocol related to increasing cooperation and disclosing electronic evidence. The Cybercrime Convention and its additional protocols can be a tool that makes it easier for Indonesia to implement

extraterritorial jurisdiction to tackle and enforce laws related to personal data breach in a transnational context.

Reference

Asean Summit. "ASEAN Declaration to Prevent and Combat Cybercrime." Asean Summit, 2017. https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf.

Bali, Vinita. "Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?" *Temple International and Comparative Law Journal* 21, no. 103 (2007).

Budapest Convention on Cybercrime (n.d.).

"Convention on Cybercrime Procedure Pertaining to Mutual Assistance Request in the Absence of Applicable International Agreement," n.d.

Efendi, Yoyon. "Internet of Things (IoT) "Sistem Pengendalian Lampu Menggunakan Raspberry PI Berbasis Mobile"." *Jurnal Ilmiah Ilmu Komputer* 4, no. 1 (2018).

EUROPOL. "Goznym Malware: Cybercriminal Network Dismantled in International Operation." European Union Agency for Law Enforcement Cooperation, n.d. https://www.europol.europa.eu/media-press/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation.

Fahamsyah, Ermanto, Vicko Taniady, Kania Venisa Rachim, and Novi Wahyu Riwayanti. "Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention." *Jurnal Hukum Dan Syariah De Jure* 14, no. 1 (2022).

Firdaus, Muhammad. "A Review of Personal Data Protection

Law in Indonesia." Interdisciplinary Program of Information Security. Graduate School PKNU, 2022. https://osf.io/tmnwg/download.

Gercke. "The Slow Wake of a Global Approach Against Cybercrime." *Computer Law Review International*, 2006.

Gercke, Marco. "Understanding Cybercrime: Phenomena, Challenges, and Legal Response." *International Telecommunications Union*, 2012.

Greco, Gianpero, and Nicola Montinaro. "The Phenomenon of Cybercrime: From the Transnational Connotation to the Need of Globalization of Justice." *European Journal of Social Sciences Studies* 2, no. 1 (2021).

INTERPOL. "'Avalanche' Network Dismantled in International Cyber Operation," n.d. https://www.interpol.int/ar/1/1/2016/Avalanche-network-dismantled-in-international-cyber-operation.

Law no. 19 of 2019 concerning Amendments to Law no. 11 of 2008 concerning Information and Electronic Transactions (n.d.).

Law No 27 of 2022 on Personal Data Protection (n.d.).

Lund, Susan, James Manyika, and James Bughin. "Globalization Is Becoming More About Data and Less About Stuff." Harvard Business Review, 2016. https://hbr.org/2016/03/globalization-is-becoming-more-about-data-and-less-about-stuff.

Makarim, Edmon. "Penelitian Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT) Dalam RDPU RUU PDP," n.d. https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200701-114522-4891.pdf.

OECD. "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." OECD Publishing,

2002. https://doi.org/https://doi.org/10.1787/9789264196391-en.

Park, Jihyun, and Dodik Setiawan Nur Heriyanto. "In Favor of an Immigration Data Protection Law in Indonesia and Its Utilization for Contact Tracing." *Prophetic Law Review* 4, no. 1 (2022).

Pembukaan Convention on Cybercrime (n.d.).

Perloff, Alexandra, and Girles. "Transnational Cyber Offenses: Overcoming Jurisdictional Challenges." *Yale Journal of International Law* 43, no. 191 (n.d.).

Pope, Henry. "Organized Crime and Corruption Reporting Project," 2021. https://www.occrp.org/en/daily/15419-ukraine-switzerland-arrest-12-suspects-of-international-cybercrime.

Rachman, Arrijal. "3 Miliar Data Sim Card Bocor, Kominfo: Baru 15-20 Persen Yang Cocok." Tempo.co. Accessed September 5, 2023. https://bisnis.tempo.co/read/1630609/13-miliar-data-sim-card-bocor-kominfo-baru-15-20-persen-yang-cocok#:~:text=Senin%2C 5 September 2022 14%3A48 WIB&text=Dari hasil penelusuran sementara dengan,data SIM Card yang bocor.

Ransomware Gang Dismantled with Eurojust Support. "European Union Agency for Criminal Justice Cooperation," 2021. https://www.eurojust.europa.eu/news/ransomware-gang-dismantled-eurojust-support.

Rawat, Meetali. "Transnational Cybercrime: Issue of Jurisdiction." *International Journal of Law Management & Humanities* 4, no. 2 (2021).

Stahl, William M. "The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to

the Problem of Cybersecurity. 40 GA." *Journal of International and COMP. Law*, 2012.

Suseno, Sigid. "Pengaturan Dan Penegakan Hukumnya Di Indonesia Dan Amerika Serikat." *Jurnal Ilmu Hukum Padjajaran* 33 (2009).

Tech. of the H. Comm. on Sci. *The Love Bug Virus: Protecting Lovesick Computers from Malicious Attack: Hearing Before the Subcomm*. United State of America, 2000.

The United States Departemen of Justice (DoJ) Press Release. "Thirty-Six Defendants for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrime," 2018. https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible.

United States District Court. Nevada: United States of America v Svyastoslav Bondarenko (2019).