International Jurnal Islamic Education, Research and Multiclturalism
(IJIERM)
Available online https://journal.yaspim.org/index.php/IJIERM/index

LAW ENFORCEMENT OF CYBERCRIME: TRACKING DIGITAL FOOTPRINTS OF CROSS-BORDER HACKERS

Idham Qrida Nusa[1], Bambang Sugiri[2], Yuliati[3], Faizin Sulistio[4]
[1,2,3,4] Brawijaya University, Indonesia
Email: [1]Idhaman63@gmail.com, [2]bambang.sugiri@ub.ac.id, [3]yuliaticholil@ub.ac.id, [4]faizin@ub.ac.id

Abstrak

Penelitian ini menganalisis penerapan hukum acara pidana (KUHAP) dalam menghadapi kejahatan dunia maya dari perspektif hukum formil. Fokus utama analisis adalah penggunaan cloud storage sebagai media penyimpanan data hasil kejahatan, yang menyulitkan proses penyitaan dan penggeledahan. Penelitian ini mengungkapkan bahwa meskipun penyidik menghadapi tantangan dalam melakukan penyitaan terhadap barang bukti digital, data hasil kejahatan yang tersimpan di cloud tetap dapat diakses dan dimanfaatkan kembali oleh pelaku untuk kejahatan berikutnya. Hal ini memunculkan masalah hukum terkait dengan kurangnya perangkat hukum yang memadai dalam menangani barang bukti digital yang tidak berwujud. Oleh karena itu, penelitian ini mengusulkan amandemen terhadap Undang-Undang Nomor 8 Tahun 1981 tentang KUHAP dengan merujuk pada Konvensi Budapest, guna memperbaiki regulasi yang ada dan mengatur penyitaan barang elektronik yang tersimpan di dunia maya. Metode penelitian yang digunakan adalah pendekatan yuridis normatif, perundang-undangan, pendekatan kasus, dan metode hukum perbandingan yang dipadukan dengan analisis kualitatif. Penelitian ini menyimpulkan perlunya sistem hukum acara formal yang mengatur secara jelas penyitaan barang elektronik yang tidak berwujud agar dapat memenuhi prinsip kepastian hukum dalam penegakan hukum terhadap kejahatan dunia maya.

Kata Kunci: *KUHAP, Peretas, Jejak Digital, Penegakan Hukum, Kejahatan Dunia Maya*

Abstract

This research analyzes the application of criminal procedural law (KUHAP) in addressing cybercrimes from the perspective of formal law. The main focus of the analysis is the use of cloud storage as a medium for storing

Corresponding Author	Idham Qrida Nusa		
Article History	Submitted: 25 March 2025	Accepted: 04 June 2025	Published: 7 June 2025

criminal data, which complicates the process of seizure and search. This study reveals that although investigators face challenges in seizing digital evidence, data from crimes stored in the cloud remains accessible and can be reused by perpetrators for future crimes. This raises legal issues due to the lack of adequate legal mechanisms to handle intangible digital evidence. Therefore, this paper proposes an amendment to Law No. 8 of 1981 on KUHAP, referencing the Budapest Convention, to improve existing regulations and address the seizure of electronic evidence stored in cyberspace. The research employs a juridical-normative, legislative, case-based approach, and comparative legal method, combined with a qualitative analysis approach. The study concludes the necessity of a formal procedural law system that clearly governs the seizure of intangible electronic items to ensure legal certainty in enforcing laws against cybercrimes.

Keywords: KUHAP, Hacker, Digital Traces, Law Enforcement, Cybercrime

INTRODUCTION

Indonesia, as a country governed by the rule of law, faces significant challenges in enforcing legal procedures when it comes to cybercrime, particularly involving breaches of personal data. With the rise of cybercrimes such as the case of the hacker "Bjorka," the country has been confronted with the reality that law enforcement is struggling to access and seize electronic evidence that is stored in cloud systems outside Indonesia's jurisdiction. This is an increasingly crucial issue, as cybercriminals exploit the digital age's vulnerabilities, often hiding their tracks across national borders (Alfiyahsari et al., 2023; Saputra et al., 2023). The inability of law enforcement agencies to effectively access and seize digital evidence from cloud storage raises concerns about the future of Indonesia's digital security and sovereignty, especially in the face of the global nature of cybercrime. As a result, there is an urgent need for legal reforms that would enable more effective enforcement, as this issue is both academically and practically vital to the protection of citizens' rights and national security (Rizaldi et al. , 2023).

Previous research on cybercrime law enforcement in Indonesia has highlighted various aspects of international legal cooperation, such as the use of Mutual Legal Assistance (MLA) systems, and the challenges related to accessing digital evidence across borders. However, these studies often fall short in addressing the inadequacies in Indonesia's current criminal procedure laws regarding the seizure of electronic evidence stored in cloud systems. While research by Hartono & Hapsari (Hartono & Hapsari, 2019) and Sitompul (Sitompul, 2024). explored mechanisms for cooperation with foreign governments and legal frameworks for accessing digital evidence, they failed to provide comprehensive solutions for the challenges posed by the cross-border nature of cybercrime. Furthermore, the existing studies have not sufficiently tackled the specific procedural amendments needed to align Indonesia's laws with international standards on cybercrime.

This research aims to bridge the gap in existing literature by addressing the shortcomings in Indonesia's current criminal procedure code, particularly in the context of cloud storage and cross-border digital evidence. The study focuses on analyzing how the Criminal Procedure Code (KUHAP) can be amended to allow for effective search and seizure of electronic evidence, even when stored in foreign jurisdictions. Specifically, the research intends to offer solutions that would enable Indonesian law enforcement to overcome the barriers imposed by international borders in investigating cybercrimes, and to enhance the country's legal framework in line with global standards (Imtihani & Nasser, 2024; Mutiarawati et al., 2024).

The central argument of this research is that Indonesia's current criminal procedure laws are insufficient for addressing the unique challenges posed by cybercrimes involving cloud storage and cross-border data access. The hypothesis tested in this study is that amending the existing KUHAP to incorporate provisions that specifically address the seizure of intangible electronic evidence, and developing international legal frameworks for cooperation, will significantly improve law enforcement's ability to address cybercrimes effectively. This reform would not only help track cybercriminals like Bjorka, but also strengthen Indonesia's position in the global fight against cybercrime.

LITERATURE REVIEW

The existing literature on cybercrime law enforcement has emphasized the challenges of managing cross-border data access and the limitations of domestic legal frameworks in dealing with international cybercrime. Three key trends emerge from previous studies: 1) the complexity of investigating cybercrimes in a globalized digital space, 2) the role of international legal cooperation frameworks, and 3) the need for technological adaptation in the enforcement of digital evidence laws. Research by Curtis & Oxburgh (Curtis & Oxburgh, 2023) and Jerman-Blažič & Klobučar (Jerman-Blažič & Klobučar, 2019) explores the implementation of international treaties like the CLOUD Act and GDPR, respectively, to address these challenges. Furthermore, the studies indicate that while countries such as the United States and members of the European Union have made significant strides in adapting their laws, Indonesia's legal system remains lagging in this regard.

The first trend involves studies that focus on international cooperation frameworks, specifically Mutual Legal Assistance (MLA). Research by Hartono & Hapsari (Hartono & Hapsari, 2019) highlights how Indonesia has engaged in MLA systems to facilitate cross-border legal assistance in cybercrime cases. However, this research largely focuses on formal agreements and protocols, without addressing the procedural gaps in Indonesia's domestic law that hinder effective access to cloud storage evidence. This pattern of research emphasizes cooperation but overlooks the need for national legal reforms to enable law enforcement to act autonomously in retrieving cross-border data.

The second trend concerns the need for technological advancement in handling digital evidence. Apau & Koranteng and Alastal & Shaqfa (Apau & Koranteng, 2020; Alastal & Shaqfa, 2023). discuss the evolution of digital forensics technologies and specialized training for law enforcement, aiming to overcome the technical complexities of investigating cybercrimes. This body of research highlights the importance of forensic technology in analyzing digital evidence but does not sufficiently address the legal and procedural obstacles that limit investigators' ability to access and seize evidence stored in cloud systems. The focus here is more on technological

solutions than on the integration of these solutions into national legal frameworks.

The third trend focuses on national legal reforms and the adaptation of criminal procedure laws. (Budiman et al. , 2021) stress the importance of updating Indonesia's legal framework, particularly the KUHAP, to incorporate specific provisions for handling digital and intangible evidence. This research calls for procedural amendments to ensure that electronic evidence, especially in the form of cloud storage, is subject to seizure and can be used in legal proceedings. However, this literature often overlooks the global dimension of cybercrime and the need for international collaboration in enforcing these reforms across jurisdictions.

While the previous studies effectively address various aspects of international cooperation and technological solutions, they fail to fully explore the procedural limitations of Indonesia's criminal justice system, especially in terms of cloud storage and cross-border data access. The literature often overlooks the legal challenges posed by intangible electronic evidence and fails to suggest concrete legal reforms to address these challenges. This gap in the literature presents an opportunity for this research to propose a legal framework that would address both domestic and international issues surrounding cybercrime.

This study aims to fill the gap by focusing on reforming Indonesia's criminal procedure laws to accommodate the complexities of cloud storage and cross-border data access. By analyzing the legal systems of the United States and the European Union, this research will propose a more adaptive legal framework for Indonesia that aligns with international standards, addresses the procedural issues in handling digital evidence, and fosters better international cooperation. This novel approach will strengthen Indonesia's legal capacity to tackle transnational cybercrime and improve law enforcement's ability to protect citizens' digital rights.

RESEARCH METHODS

This research uses a qualitative approach with a case study method and a comparative approach to analyze Indonesia's criminal procedure law provisions in facing the challenges of cybercrime investigations, specifically related to the search and seizure of electronic evidence stored in cloud storage. This study compares Indonesia's criminal policy system with the

criminal justice systems in the United States and the European Union to formulate recommendations for reforms to the Criminal Procedure Code (KUHAP). The selection of these three legal systems is based on the characteristics of their approach in handling digital evidence across jurisdictions: The United States through the CLOUD Act, the European Union with the European Investigation Order (EIO), and Indonesia which is still limited to the Mutual Legal Assistance (MLA) framework. These differences provide a strong comparative basis for evaluating the readiness of national laws to face global challenges.

The data used in this research is secondary data obtained through a literature study of national laws and regulations, court decisions, Constitutional Court decisions, as well as relevant regional and international legal instruments. Data collection was conducted systematically through searching legal databases, academic journals, and official documents of judicial institutions and international organizations. To analyze the data, this research uses doctrinal legal methods to examine the coherence of legal norms in KUHAP, as well as a sociological approach to understand the social dynamics and practical challenges faced by law enforcement officials in the electronic evidence process. The analysis was conducted using content analysis techniques, which identified recurring legal themes, interpreted the structure of the argumentation in the decision, and compared it with international norms. Through this framework, the research aims not only to evaluate the weaknesses of the national criminal procedure law in responding to developments in information technology, but also to develop recommendations for reformulation of the Criminal Procedure Code that is more adaptive to the complexities of modern electronic evidence.

RESULTS AND DISCUSSION

1. The act of Hacking, without the right to enter a computer system.

Other terms for this computer crime are "unauthorized use of computer system", "illegal access", or "unlawful entry". The popular term is "hacking". The act of unlawfully entering someone else's computer system does not directly harm the owner, because the perpetrator usually only wants to know what is contained in the computer data. However, this can indirectly cause harm, because the

activities in the computer system can be monitored proving that the existing "security measures" can be bypassed. Hackers only want to show that the institution's security system has been successfully breached with the intention of showing weaknesses in the owner's computer security system. In the case of the hacker's account named Bjorka, he has openly intended to obtain and freely sell confidential data on the privacy of the wider community that needs protection, including the NIK (residential identification number), even the name of the biological mother, which is usually related to the security password for bank account ownership. It has been proven that the NIK data can be misused, such as when someone whose NIK is used to own a luxury car, the actual NIK owner is not economically capable of owning a car, let alone a luxury car. This action is intended to ensure that the real owner avoids the progressive motor vehicle tax imposed very expensive because of the luxury car tax and the real owner already owns more than one car, thus benefiting from the difference in the progressive tax on motor vehicles over many years which is not a small amount.

The British Parliament approved and enacted the Computer Misuse Act 1990 which came into effect on 29 August 1990. This law prohibits the act of entering another person's computer system without authorization, whether for mere curiosity or for certain malicious purposes (hacking for a further purpose). The penalty is a sentence of 6 (six) months in prison or a fine for the crime of "unauthorized entry into a computer". The penalty increases to 5 (five) years in prison or a fine, for the crime of " unauthorized access to a computer with the intent to commit or facilitate the commission of a serious crime. ' And the crime of "unauthorized modification of computer data". In Indonesia, a similar case occured with the hacking of the KPU (General Election Commission) where images of party participants were changed.

2. Comparison of provisions in the Criminal Code

Article 21 of the Swedish Data Protection Act of 2 April 1973, amended on 1 July 1982, criminalizes 'any person who enters a computer system without authorization'. Article 167 of the Indonesian Criminal Code only regulates the act of entering a house, room or yard unlawfully, and in accordance with the legal experts' opinion, in general

it cannot be extended to the definition of unauthorized entry into a computer system. The article states: "Anyone who unlawfully enters by force into or unlawfully is in a house or a closed place or a closed yard, which is used by another person and does not immediately leave that place, at the request of the person entitled or a request on behalf of the rightful person, shall be punished with imprisonment for a maximum of nine months or a fine." The Canadian Department of Justice drafted amendments to the law prohibiting these acts, which later became the Criminal Law Amendment Act, 1985. Article 301. 2(1)(b) states it as a criminal offense:

> "…anyone who dishonestly and without right…using electromagnetic, acoustic, mechanical or other means intercepts or causes to be intercepted, either directly or indirectly, any function of a computer system (31).

Several other countries have created new provisions prohibiting the act of 'unauthorized entry into a computer system', as stipulated in articles 1,2,3 of the UK's Computer Misuse Act 1990 Article 502(d)(2) of the California Penal Code which came into effect on January 1 1985, makes it a violation (misdemeanor) an act that only takes the form of 'mere access', namely 'Anyone who intentionally enters a computer system, computer network, computer program, or data, knowing that entering the system is prohibited by the owner or lessee.

The new federal law, The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, effective from October 12, 1984, criminalizes anyone who unauthorized accesses a computer with the intent to obtain confidential information that could harm the United States government, or benefit other countries, to obtain information from financial institutions or 'consumer reporting agencies', or intentionally uses, changes, destroys or publishes information, or prevents the use of certain computers by authorized persons. It seems that these provisions are not yet complete, so several changes have been made to Chapter 33 concerning Computer Crimes.

The new provisions of article 263(2) of the Danish Penal Code regarding 'Datacriminalitet' criminilize the act of "Accessing another person's information system or program intended for use during data

processing. ". Apart from that, article 263 (3) threatens with a more serious punishment if the act is carried out 'with the intention of knowing or obtaining trade secret information of a company'.

3. The criminal offence of disclosing secrets

The provisions applied in some countries regarding disclosure state secrets can be applied to the act of disclosing secrets contained in computer data by anyone. However, protection against disclosure of company secrets that may be contained in the computer data can only be applied to acts committed by employees assigned to keep the secret or by former employees. and cannot be extended to outsiders other than employees/former employees.

Considering the value of company's secrets, in practice, the provisions of Civil Law are used to claim compensation, for example in the provisions regarding unfair competition or unlawful acts. Since company secrets are often stored in computer data, the possibility of them being 'stolen' by outsiders quickly and unnoticed becomes easier. In order for this criminal act to apply to outsiders, several countries have refined criminal provisions regarding the disclosure of company secrets, , such as article 202a of the West German Penal Code (formerly) which was included in the amendment to the "Second Law for the Prevention of Economic Crimes 1986 which contains:

Section 202a. Spionage Data: (a) Whosoever unlawfully obtains data for himself or others that are not intended for him and are especially protected against unauthorised access, shall be liable to imprisonment for up to three years or a fine. (b) The data referred to in subsection (1) are data those stored or transmitted electronically or magnetically or by other ways that are not directly visible.

Article 17 of the criminal provisions regarding West German 'Unfair Competition' was revised by the 'Second Law for the Prevention of Economic Crime 1986', by adding several words in point 1 and new provisions. As a guideline, a case is considered serious if the perpetrator knows at the time of disclosing (communicating) that the secret will be used abroad or that he himself will use it abroad. By proposing improvements regarding the criminal act of "disclosing secrets" almost the same as article 112 and so on. Criminal Code, namely by adding ". .

. . data or information, and objects from which the data or information comes", to eliminate misunderstandings related to the use of the words data or information in articles 98, 98a, 98b, 98c, above.

4. The principle of the Rule of Law or Rechstaat in its implementation

The United Nations, particularly the International Commission of Jurists (ICJ), has assessed that the 1945 Constitution of Indonesia (UUD 1945) has not fully provided independent power to the Judiciary. In fact, it has been criticized for giving too much power to the executive, especially during the Old Order and New Order governments. One of the indications of this criticism is the argument that the Criminal Procedure Code (KUHAP) does not sufficiently guarantee human rights protection according to international standards, particularly regarding There is no law regulating the procedures for the use of forced or unlawful evidence. Regarding the searches and seizures, the ICJ has pointed out that the provisions of the Criminal Procedure Code (KUHAP) give exessive authority to investigators and public prosecutors; which is inconsistent with Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). In its recommendations, the ICJ stated that searches and seizures must be conducted with the judge's permission and after a preliminary examination first if there is probable cause, including taking an oath of the complainant and witnesses. (Hatta book, pp. 17-18, several law enforcement issues).

5. Cross-Border Cyber Crime

Some cybercrime cases have jurisdictional issues, such as confiscating Facebook accounts or searching Gmail accounts. However, none of these cases have raised and discussed the issue of cross-border access to electronic evidence stored in cloud storage, as is suspected to have been done by hackers including Bjorka's account! It is important to examine further the aspects or situations that obstruct discussion of cross-border access issues.

There are two principles of law enforcement jurisdiction that must be applied in cybercrimes. The first principle is that a sovereign state has authority within its own territory and can enforce its laws

within that territory. The second principle is that one no state may enforce its laws in any form within the jurisdiction of another state without the consent of that state. (Joshua p. 23. 35). The problem of cross-border access to electronic evidence remains unresolved in the regulation of cybercrime.

6. State jurisdiction in international law

Jurisdiction is the actualization of a country's sovereignty. In this case, jurisdiction refers to the legal authority of a state, as manifested in its organs, to exclusively regulate (prescribe) certain actions, events, people and legal interests, enforce (enforce) its laws through various mechanisms; and adjudicating cases according to the country's laws. On the other hand, jurisdiction also refers to restrictions, particularly concerning boundaries, or limits between countries in enforcing its power or authority to control various matters. In the Indonesian Criminal Justice System. the historical relationship between Indonesia and the Netherlands during the colonial era has strongly embedded a civil law legal system and its inquisitorial characteristics which are clearly visible in Law No. 8 of 1981 concerning the Criminal Procedure Code. Many issues in the application of KUHAP arise because the KUHAP regulations are unspecific, have multiple interpretations and are unclear (vague) [Josoa p. 212. 5]. The Indonesian inquisitorial system applies functional role differentiation, which is also known as the compartmentalization paradigm. Based on this paradigm, institutions in charge of investigation, prosecution and adjudication have autonomous functions which must not be interfered with by other law enforcement agencies (Sitompul, 2024). The aim of the Indonesian inquisitorial system is to find or at least get approximate material truth (Grande, 2016). In practice, material truth is understood as a legal construction of the legal facts concerning a criminal act as determined by the panel of judges in their decision. This legal construction ensures whether a criminal act has occurred and whether the defendant fulfills all the elements of the crime. This certainty is based on the evidence and the evidence presented in court which constitutes formal procedural law.

7. Budapest Convention On Cybercrime

The Budapest Convention was drafted with a clear understanding that the countries' criminal laws must be able to keep up with technological developments. Technological developments have created uncertainties in law and cooperation in investigating cross-border cybercrimes. Therefore, the members of the Budapest Convention believe that countries require "a concerted international effort" and "only a binding international instrument can ensure the necessary efficiency in the fight" against cybercrime. Through ratification and accession, parties can expect to build "a community of trust" (Budapest Convention, n. d.). Therefore, the community mentioned can provide mutual legal assistance to the 'widest extent possible'.

To keep up with evolving threats of cybercrime, the cloud computing environment, and the need for productive cooperation, the Cybercrime Convention Committee (T-CY) has produced eleven Budapest Convention guidance notes since 2012 (Sitompul, 2024). Law enforcement authorities from the Budapest Convention parties need not only sophisticated equipment to combat new threats of cybercrime but also flexibility in obtaining electronic evidence stored abroad. However, the sections below show that the parties of the Budapest Convention have faced problems in applying the 'Lotus prohibitive rule' strictly.

The material criminal provisions of the Budapest Convention are the most widely adopted legal framework globally for defining and criminalizing cybercrimes. These provisions serve as a reference point for many countries in formulating their cybercrime laws. Prior studies, such as those by Bechara & Schuch, (2021) and Frosio & Geiger (2023), emphasize that the Convention provides a structured approach to addressing cyber threats while allowing flexibility for national legal systems. The provisions categorize cybercrimes into two main groups: first, offenses against the confidentiality, integrity, and availability of data and computer systems, including illegal access, illegal interception, data interference, system interference, and misuse of devices; and second, computer-related crimes, such as computer-related forgery and computer-related fraud. By establishing these categories, the

Convention aims to harmonize legal standards across jurisdictions while ensuring an effective response to the evolving nature of cyber threats.

The use of malware, botnets, or DDOS attacks in the commission of cybercrime indicates the intent of criminals to hide their identity and location, including hackers of Bjorka's account. Thus, even if a perpetrator commits the criminal act from the territory of the forum country (Budapest Convention), he can design his action to appear as if the act originated from a computer system located in various foreign jurisdictions. A perpetrator can also use the identity of a foreign national to deceive victims in the same territory where the perpetrator commits the crime. This occurred in the case of the Bjorka account hacker, where previously he had purchased the account of an ice seller in Indonesia. As a result, the police arrested and interrogated the account owner, but finally he was released because he was not the Bjorka they were looking for.

8. Efforts to Track Cross-Border Hacker

To deal with the threats of Cross-Border hacking, law enforcement agencies need appropriate law enforcement authority, accompanied by coercive measures, advanced equipment capable of tracking the origin of hackers. Multilateral conventions, such as the Budapest Convention, accommodate the idea of having law enforcement authority, coercive measures, and International cooperation among countries. A member state of the convention will consider the legal systems and practices of other convention members before allowing those other parties to request and seize electronic evidence stored within its territory without prior consent. The application of due process of law, the availability and completeness of required legislation, ease of access to justice, accountability of law enforcement agencies, and implementation of personal data protection practices are some of the key consideration. To overcome gaps and uncertainties that arise from differences in legal systems and legal practices among the parties, it is necessary to establish conditions and safeguards.

The Budapest Convention does not determine restrictions on the types of conditions and safeguards established by members, as mentioned in the Explanatory Report to the Budapest Convention, paragraph 147. The conditions and safeguards are discussed based on European standards. Indonesia must face differences in standards regarding conditions and safeguards to strengthen cooperation in criminal matters with European countries or access the Budapest Convention. Specificity or particularity is a fundamental element of the conditions and safeguards in the Budapest Convention. For example, law enforcement authorities must mention specifically the electronic evidence (Budapest Convention, n. d.) they ordered so that someone keep or communicate as law enforcement officials intercepted. (Budapest Convention, n. d.) Law enforcement authorities are prohibited from intercepting communications to uncover criminal acts other than those directly related to the legal basis for the interception. These specific elements emphasize the obligations of law enforcement officials to protect the personal data and the privacy of internet users.

Privacy rights are part of personal data protection, which is a human right protected under the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe. The right to privacy and the right to personal data protection are two fundamental rights regulated in the Charter of Fundamental Rights of the EU (Charter of Fundamental Rights of the European Union, n. d.). EU Directive 95/46/EC on the personal data protection sets out fundamental principles in the processing of personal data. Personal data must be collected for specific, explicit and legitimate purposes and shall not be further processed in a manner incompatible with those purposes (Perlindungan Individu Sehubungan Dengan Pemrosesan, n. d.). EU Regulation 2016/679 on personal data protection replaced the directive. This regulation still maintains these fundamental principles. Furthermore, the Explanatory Report to the Budapest Convention notes that some parties consider "the collection of traffic data as being equivalent to the collection of content data in terms of privacy and intrusiveness (*Laporan Penjelasan Konvensi Budapest*, n. d.). However, ensuring the fulfillment of particularity can be difficult when law

enforcement officials faces large volumes of data and various encryption technologies. In cases where the electronic information sought contains personal data, mutual legal assistance may become more complicated.

Another manifestation of having adequate conditions and safeguards is the presence of judicial and independent institutions in investigating of cybecrimes. Independent institutions are very important in balancing the interests of the parties and resolving adverse impacts that may arise from the implementation of a coercive measure. Prior research, such as that by De Bellis, (2021) and Jabban et al. , (2024), highlights that judicial oversight is essential in ensuring that investigative measures do not disproportionately infringe upon fundamental rights. Furthermore, proportionality serves as a key safeguard that must be incorporated into national laws in alignment with the Budapest Convention (Mantelero, 2024). In the context of European countries, proportionality requires that authorities and procedures correspond to the nature, severity, and specific circumstances of the offense, ensuring that investigative powers are exercised within reasonable and justified limits (Sitompul, 2024).

9. Coercive Measures in Cybercrimes

The Budapest Convention stipulates four types of coercive measures to combat cybercrime, first; expedited preservation of both stored data and traffic data, secondly; production order to produce data, third; search and seizure, fourth; and real-time data collection (both traffic data and content data). Law enforcers can combine these four coercive measures according to the specific needs and conditions of cases occurring in the field. The Budapest Convention strictly enforces the collaboration of these coercive measures called the Lotus prohibitive: a state may execute coercive measures within its own territory but it is prohibited from applying it in another state's jurisdiction. For example, the convention requires that important elements in the implementation of coercive measures must be present within the territory of the enforcing party. Such as a person ordered by the law enforcement to produce data (Article 18. 1. a); service providers ordered by law enforcement to produce electronic information (Article 18. 1. b): computer systems searched by law enforcement officials to

collect real-time traffic data and content data (Articles 20 and 21). This regulation is intended as a reminder to prevent violations of the sovereignty of other parties.

If these elements (person/thing, service provider/PSE (Electronic System Provider), computer system, and technical equipment) are located outside the territory of the member party of the Budapest Convention, is the implementation of coercive measures in these conditions an extraterritorial investigation? In other words, does the Budapest Convention permit the unilateral execution of coercive measures that cause extraterritorial effects? Article 32 of the Budapest Convention provides an affirmative response to this question. It stipulates that a party may, without the consent of the other party, access electronic information stored in the territory of the other party under two conditions. First, electronic information is available to the public. Second, electronic information can be accessed from the territory of the enforcing party, and the authority of that party obtains legal and voluntary consent from the person who has the right or authority to provide such consent. However, apart from the conditions specified in Article 32, it is not clearly regulated in the Budapest Convention, to what extent the convention permits its parties to use other coercive measures that cause extraterritorial effects.

The difficulties of ensuring a violation of sovereignty in the implementation of coercive measures for obtaining electronic information have been recognized since the drafting of the Budapest Convention. In 1990, the European Committee on Crime Problems pointed out these difficulties by illustrating several conditions regarding "pure direct penetration" (CoE, n. d.). This terminology is defined as accessing computer data stored abroad using a computer located in the enforcing party's territory. As an illustrative example, a police officer searches a room and finds a computer; the officer proceeds the search without knowing that the data on the computer is stored abroad (CoE, n. d.). The Committee observed that some parties might view that the police actions (accessing computer data stored abroad) as a violation of international law (CoE, n. d.). This assumption aligns with the strict interpretation of the Lotus prohibitive rule. Whether the police officer

knew that the data was stored overseas is irrelevant. According to a strict interpretation of the rule, what matters is that the officer accessed electronic information stored in another country's territory. However, the European Committee on Crime Problems also argued that other countries might consider the police officer's actions as not a violation of international law if the officer acted in good faith when accessing the data (Sitompul, 2024).

10. Search and Seizure

The formulation of Article 19 of the Budapest Convention aims to establish authority that equivalent to search and seizure. Search refers to the use of coercive measures to access a computer system where the required electronic evidence is stored (Budapest Convention, n. d.). The Budapest Convention does not limit the methods or technology used to carry out searches. However, the convention mandates its members to authorize law enforcement officials to extend the scope of searches as soon as possible to other computer systems (Budapest Convention, n. d.). This extension is rationalized by the presumption of interconnectivity between various computer systems in cyberspace (*Laporan Penjelasan Konvensi Budapest*, n. d.). The Budapest Convention explicitly regulates that Article 19 does not cover cross-border searches (*Laporan Penjelasan Konvensi Budapest*, n. d.). This provision emphasizes that search and seizure are coercive measures that are territorial in nature. Search is accessing a system to retrieve electronic evidence, while seizure is securing a computer system or storage media, including cloud storage. It also includes rendering electronic evidence within the system inaccessible (Budapest Convention, n. d.). Similar to search, the Budapest Convention does not limit the methods or approaches of seizure.

Compared to a production order, search and seizure are more intrusive on privacy but more productive in collecting electronic evidence. The level of control in examining and searching for electronic evidence through searches and seizures is higher than with production orders. Prior research, such as that by Nuzzo (2022) and (Bernardini & Sanvitale, (2023), has emphasized that search and seizure provide greater access to digital evidence, particularly when authorities face vast

amounts of data that cannot be easily specified beforehand. However, these studies also highlight concerns about the potential overreach of law enforcement and the need for strict safeguards to balance investigative efficiency with privacy rights. In situations where authorities can specify electronic evidence and protect data privacy, production orders remain a viable option. However, when data volume is overwhelming and service providers lack the expertise or willingness to allocate resources to locate relevant evidence, search and seizure become a prioritized coercive measure, allowing investigators to clarify and determine significant or relevant information for an investigation.

11. Real-Time Collection of Electronic Evidence

In the Budapest Convention, law enforcement officials are given the authority to collect electronic evidence (either traffic data or communications content) in real time. Law enforcement officials can carry out these coercive measures themselves or through electronic system administrators. Again, the Budapest Convention does not expressly permit the implementation of such coercive measures which have extraterritorial range. If law enforcement officials from an enforcing party intercepts a citizen of its country communicating with a foreign national in the territory of that foreign country, then, it cannot be avoided, communication data from the foreign citizen is part of the data that is intercepted. Even though law enforcement officials conduct interceptions in their jurisdiction, these actions have extraterritorial range in the territory of other countries. Regarding this unavoidable extraterritorial range, the Budapest Convention delegates this problem to the legislation of its member states.

Considering the impact of privacy violations resulting from the implementation of this coercive measure (Budapest Convention, n. d.) members of the Budapest Convention are required to implement it with strict conditions and safeguards (*Laporan Penjelasan Konvensi Budapest*, n. d.). Because communication content data reveals more private or personal information than traffic data, the conditions and safeguards for interception can be stricter than those applied to the collection of traffic data. However, the conditions and safeguards must not fall below the standard required for the collection of traffic data.

12. Cross-border access

Budapest Convention Article 32b strictly regulates cross-border access. At first glance, this provision is an exception to the requirement for mutual legal assistance in retrieving electronic evidence and is an exception to the Lotus Prohibitive rule. These provisions grants the enforcing party the authority to access or receive, through a computer system within its jurisdiction, electronic information located in the territory of another party to the Budapest Convention. Law enforcement officials of the Enforcing party may do so if they obtain voluntary valid consent from persons who have the legal right to disclose the electronic information to law enforcement officials.

In 2014, T-CY issued Guidance Note #3 regarding Transborder Access to Data. This note confirmed and included irrefutable conditions that comply with the Lotus prohibitive rule. First, Article 32b can be applied between two members of the Budapest Convention. This provision does not cover situations where the data is stored in another member, or where the enforcing state is not sure where the data is stored. Understandably, the Budapest Convention does not regulate the actions of countries that are not members of the Budapest Convention. However, in a cloud computing environment, the requirement to have prior knowledge that electronic information is stored in the territory of another party may be difficult to fulfill.

Second, in efforts to obtain cross-border access, a party is encouraged to fully utilize all international cooperation mechanisms regulated in the Budapest Convention. In other words, this convention suggests that the enforcing party should not use Article 32b as the initial option to obtain electronic information, especially if the party does not know where the electronic information sought is stored. Previous studies, such as those by Mariam, (2024) and Abraha, (2020), have highlighted the challenges of cross-border data access, emphasizing that reliance on mutual legal assistance treaties (MLATs) remains the preferred approach despite their procedural complexities. These studies also argue that Article 32b should be interpreted narrowly to prevent potential conflicts with national sovereignty and data protection laws.

Third, the person providing access is physically located within the teritory of the enforcing party. Therefore, the person can give consent and disclose electronic information from the territory of the enforcing party. T-CY raises several other possibilities by considering the location where the person gives their consent and accesses the electronic information. The place where the consent is given or where the electronic information is accessed may be in the territory of another party or within the jurisdiction of a third country. However, T-CY reminds us that beyond the explicitly regulated (default) conditions, namely that a person gives consent in the enforcing party's territory and accesses electronic information from within that territory:

"many parties would object-and some even consider it a criminal offence-if a person who is physically in their territory is directly approached by foreign enforcement authorities who seek his or her cooperation" (Sitompul, 2024).

Therefore, Article 32(b) can be safely applied under the following ideal conditions. First, an individual with the legal right to disclose the sought information is present within the jurisdiction of the enforcing party. Second, the individual provides consent to the authority of the enforcing party. Third, the enforcing party ensures that the electronic information is stored within the territory of another party to the Budapest Convention.

Fourth, the other party does not prohibit the disclosure of the sought electronic information. Fifth, the individual accesses the electronic information from a computer system located within the territory of the enforcing party. Under these ideal conditions, the allegation that Article 32(b) "might damage the sovereignty and security of member countries and their citizens right" (Computer Crime Research Center, 2008) may be refuted. Nevertheless, Law enforcement authorities may question to what extent Article 32b is practical if they are required to meet all the intended ideal conditions. "

13. Use of Malware in Cybercrime Investigations

The Budapest Convention neither permits nor explicitly prohibits the use of malware in criminal investigations. Guidance Note #7 defines malware as "a piece of software inserted into an information system to

cause harm to that system or other system, or to subvert them for use other than intended by their owners (Cybercrime Convention Committee, 2013). On one hand, the use of malware disrupts users' privacy. Malware can take control of computer systems. Therefore, malware can reveal highly private information about users without their consent. On the other hand, despite the intrusive nature of malware towards users' privacy and the potential harm it may cause to computer systems, malware can be a tool for investigating cyber crimes. Malware can help investigators reveal the identity and location of perpetrators as well as uncovering criminal acts hidden within the darknet. Bjorka's account also utilized several darknet sites. Furthermore, malware can also collect electronic evidence from jurisdictions whose location are uncertain. By emphasizing their authority, law enforcement officials can use malware as a form of coercive measure as regulated in the Budapest Convention. First, malware can act as a tool to access a computer system or as a means to confiscate electronic information. In Article 19, the drafters of the Budapest Convention deliberately chose the phrases 'search or similarly access' and 'seize or similarly secure computer data'

Search and seizure are inherently coercive measures. An investigator who has court permission can conduct searches and seizures without the consent of the person who has the authority to control the computer system. The Budapest Convention does not limit methods for searching or confiscating information. Any method that provides the functionality to access and secure computer data should be permitted. What is emphasized by the Budapest Convention in implementing every coercive measure regulated in the convention is the fulfillment of conditions and safeguards. Particularly the protection of privacy and personal data. The United States uses malware as a tool to conduct search and seizure (Kolochenko, 2022).

Second, in Article 20 and Article 21, malware can function as an interception tool to collect or record traffic data and communication content in real-time. The Budapest Convention does not regulate interception methods in detail and states that "no obligations in technical terms are defined" (*Laporan Penjelasan Konvensi Budapest*, n. d.

). As mentioned previously, the convention applies stricter conditions and safeguards to the interception of data content compared to traffic data. The Budapest Convention limits the use of interception tools to record data content for only investigations of serious cybercrime. An investigator must determine specifically the communications he or she will intercept. Conditions and safeguards regarding the implementation of this coercive measure are strictly regulated in the convention. France, Germany, Italy, and Australia are members of the Budapest Convention that use this construction.

Although the Budapest Convention has designed the coercive measures (search and seizure and interception of electronic information) for territorial use, its parties have used such coercive measures extraterritorially. It seems the debate over the use of malware is not about whether law enforcement officials are permitted to apply it. But instead, the debate emphasizes whether the use of malware has a sufficient legal basis and what requirements of ex ante and ex post that should be applied in the use of malware (Mayer, 2018). However, law enforcement officials who use malware to deal with loss of jurisdiction situations must be able to anticipate the technical risks and legal consequences that may arise in the territory of other countries where the electronic evidence sought is stored or where the perpetrator is hiding.

14. Indonesian Practices in Resolving Cyber Crime

Initially, the government's main objective in enacting the criminal provisions in the ITE Law was to criminalize unlawful activities in cyberspace and strengthen international cooperation in combating cybercrime (Depkominfo, 2008). With the aim of strengthening this cooperation, the Indonesian government has shown a strong intention to accede to the Budapest Convention. After the ITE Law was promulgated in 2008, in the same year, the government prepared two draft laws, namely the Information Technology Crime Bill and the Budapest Convention on Cybercrime Accession Bill. The concept developed through these two drafts is that the purpose of the first draft is to harmonize the Indonesian criminal law with the provisions of the Budapest Convention (Sasongko, 2010). After that, the government officially acceded to the convention mentioned based on the second

draft law. The Indonesian government stated this intention at the 2010 Octopus Conference, an international conference under the Council of Europe which was formed as a platform to exchange information and practices in combating cybercrime. However, the government did not continue with the accession plan. Some of the considerations that motivate this are the Indonesian Ministry of Foreign Affairs (Kemenlu) providing diplomatic considerations. The Ministry of Foreign Affairs sees aspects of the nature of the convention as a regional instrument and the fact that Indonesia is not a country involved in formulating the convention (Sitompul, 2017). Therefore, Indonesia does not have room for negotiation to accommodate the interests of its law enforcement officials, including in tracking and arresting the account hacker named Bjorka. The Ministry of Foreign Affairs' view seems to be the determining factor in terminating the action plan. In the Open Ende Intergovernmental Expert Group organized by UNODC in 2013, the Indonesian delegation, together with several other countries, voiced the importance for countries to consider establishing an international instrument to combat cyber crime.

A more substantive view is that the accession plan is not based on mature considerations (Kabag Hukum Ditjen Aptika, n. d.). The government prepared a country profile report regarding Indonesian law in line with the Budapest Convention (Indonesia, 2008). However, the government has not yet implemented the implications of canceling accession to the convention. Furthermore, the termination of the accession plan may also be influenced by the fact that the Indonesian government must prioritize the preparation of the implementation of the ITE Law. Terminating plans for accession to the Budapest Convention was the right policy at that time, where the losses from cybercrime were not considered worrying before there was a breach of privacy data due to hacking, especially an account hacker named Bjorka. Accessioning the Budapest Convention is a complex project that requires substantial financial resources but results in substantial legal implications. However, It is still much more important and far smaller compared to the finances spent for the unclear IKN project and fulfilling promises of free lunches made during

the previous presidential election campaign. Which of these priorities is truly more important?

CONCLUSION

This study highlights the importance of aligning Indonesian criminal procedure law with international standards, particularly in the areas of search and seizure of electronic evidence and building effective international cooperation. The key lesson drawn from this research is that Indonesia's current legal system is not yet fully responsive to the challenges posed by advancements in information technology, especially concerning digital evidence stored in cloud storage outside Indonesia's jurisdiction. Therefore, reform of Indonesia's criminal procedure law is necessary to address future cybercrimes more effectively.

The strength of this research lies in the use of a comparative approach and multidimensional analysis covering both normative and sociological aspects, which results in reformative recommendations for strengthening Indonesia's criminal justice system. This research contributes to the academic field by identifying gaps in Indonesia's legal system related to the enforcement of laws against cybercrime, particularly those involving cross-border electronic evidence. By comparing Indonesia's legal system with those of the United States and the European Union, the study provides new insights on how Indonesia can enhance international cooperation and adapt its legal framework to global advancements in information technology.

The main limitation of this research is that it did not involve primary data collection or interviews with relevant stakeholders, meaning that the interpretation of the law's implementation relies solely on secondary sources and documented decisions. As a result, while this research provides a comprehensive overview of the need for reform in Indonesia's criminal procedure law, it does not fully capture the perspectives of law enforcement officials or assess the technical implementation of the existing legal framework. Future research is expected to include interviews with law enforcement officers to gain a deeper understanding of the challenges in implementing and assessing the effectiveness of the current laws in addressing cybercrime.

BIBLIOGRAPHY

1) Abraha, H. H. (2020). Government access to digital evidence across borders: Some lessons for Africa. In K. M. Yilma (Ed.), *The internet and policy responses in Ethiopia: New beginnings and uncertainties*
2) Alastal, A. I. , & Shaqfa, A. H. (2023). Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool. *Journal of Data Analysis and Information Processing*, *11*(2), 121-143. https://doi. org/10. 4236/jdaip. 2023. 112008
3) Alfiyahsari, R., Taurina, R. C., & Priyanka, G. (2023). Does the use of Digital Marketing Communication Strategy Effectively Affect Conversions? (Case Study on DatascripMall.ID). *International Journal of Islamic Education, Research and Multiculturalism (IJIERM)*, *5*(3), 653–672. https://doi.org/10.47006/ijierm.v5i3.249
4) Apau, R. , & Koranteng, F. N. (2020). An overview of the digital forensic investigation infrastructure of Ghana. *Forensic Science International: Synergy*, *2*, 299-309. https://doi. org/10. 1016/j. fsisyn. 2020. 10. 002
5) Bechara, F. R. , & Schuch, S. B. (2020). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*. https://doi. org/10. 1108/JFC-07-2020-0149
6) Bernardini, L. , & Sanvitale, F. (2023). Searches and seizures of electronic devices in European criminal proceedings: A new pattern for independent review? *Revista Italo-española de Derecho Procesal*, 1, 73–119. https://doi. org/10. 37417/rivitsproc/1475
7) Budapest Convention, Pub. L. No. 16 and 17.
8) Budiman, A. A. , Maya, G. , Rahmawati, M. , & Abidin, Z. (2021). Mengatur Ulang Kebijakan Tindak Pidana di Ruang Siber Studi Tentang Penerapan UU ITE di Indonesia. *Institute for Criminal Justice Reform (ICJR)*.
9) Charter of Fundamental Rights of the European Union. CoE. (n. d.). *Rekomendasi Kejahatan Terkait Komputer No. R (89) 9 tentang Kejahatan Terkait Komputer dan Laporan Akhir Komite Eropa untuk Masalah Kejahatan* (p. 87).
10) Computer Crime Research Center. (2008). *Putin defies Convention on Cybercrime*.
11) Curtis, J. , & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal*, *96*(4), 573–592. https://doi. org/10. 1177/0032258X221107584
12) Cybercrime Convention Committee. (2013). *T-CY Guidance Note #7 on New Forms of Malware*.
13) De Bellis, M. (2021). Multi-level administration, inspections and

fundamental rights: Is judicial protection full and effective? *German Law Journal,* 22(3), 416–440. Depkominfo. (2008). *Naskah Akademis RUU tentang Informasi dan Transaksi Elektronik*. 15. https://doi. org/10. 1017/glj. 2021. 14

14) Ferdiyanto, R. (2017). Barang Bukti di Rupbasan Nyaris jadi Rongsokan. *Fokus. Tempo. Co*.
15) Frosio, G. , & Geiger, C. (2023). Taking fundamental rights seriously in the Digital Services Act's platform liability regime. *European Law Journal.* https://doi. org/10. 1111/eulj. 12475
16) Grande, E. (2016). Rumba justice and the Spanish jury trial. In *Comparative Criminal Procedure* (pp. 365–395). Edward Elgar Publishing.
17) Hartono, B. , & Hapsari, R. A. (2019). Mutual Legal Assistance Pada pemberantasan Cyber Crime Lintas Yurisdiksi di Indonesia. *Sasi*, *25*(1), 59–71. https://doi. org/10. 47268/sasi. v25i1. 136
18) Imtihani, H., & Nasser, M. (2024). THE UNJUSTIFIABLE TARGETING OF HEALTHCARE IN PALESTINE: A VIOLATION OF HUMAN RIGHTS AND INTERNATIONAL LAW. *International Journal of Islamic Education, Research and Multiculturalism (IJIERM)*, *6*(3), 763–783. https://doi.org/10.47006/ijierm.v6i3.367
19) Indonesia. (2008). *Profil Negara Legislasi Kejahatan Siber Indonesia (Draf 25 Maret 2008)*.
20) Jabban, M. , Saber, M. , & Mojab, S. D. (2024). A typology of judicial oversight systems in criminal investigation and prosecution: A comparative study. *Pakistan Journal of Criminology,* 16(1), 93–109. https://doi. org/10. 62271/pjc. 16. 1. 93. 109
21) Jerman-Blažič, B. , & Klobučar, T. (2019). A New Legal Framework for Cross-Border Data Collection in Crime Investigation amongst Selected European Countries. *International Journal of Cyber Criminology*, *13*(2). https://doi. org/10. 5281/zenodo. 3698359
22) Kabag Hukum Ditjen Aptika. (n. d.). *Background of the EITA*.
23) Kolochenko, I. (2022). *Framework Proposal to Regulate Lawful Hacking by Police within Criminal Investigations*. Capitol Technology University.
24) *Laporan Penjelasan Konvensi Budapest*. (n. d.).
25) Mantelero, A. (2024). The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. *Computer Law & Security Review,* 54, 106020. https://doi. org/10. 1016/j. clsr. 2024. 106020
26) Mariam, S. (2024). Legal and ethical challenges in international cybersecurity: Addressing cross-border data breaches. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures,*

8(12). http://polarpublications. com/index. php/JACSTIC/article/view/3
27) Mutiarawati, I., Dewantara, R., & Rachmat, S. N. (2024). The Law Responsibility of E-Commerce Organizers Regarding The Failure of Payment in PayLater System. *International Journal of Islamic Education, Research and Multiculturalism (IJIERM)*, *6*(2), 528–546. https://doi.org/10.47006/ijierm.v6i2.344
28) Mayer, J. (2018). Government Hacking. *YAle Law Journal*, *3*, 659–660.
29) Nuzzo, V. (2022). Search and seizure of digital evidence: Human rights concerns and new safeguards. *In Investigating and preventing crime in the digital era* (pp. 119–149). Springer Nature.
30) Perlindungan Individu sehubungan dengan Pemrosesan, Pub. L. No. Pasal 6. 1(b) Arahan 95/46/EC.
31) Rizaldi, M. Z. , Putra, R. D. , & Hosnah, A. U. (2023). Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data. *JUSTITIA J. Ilmu Huk. Dan Hum*, *6*(2), 619–627. http://jurnal. um-tapsel. ac. id/index. php/justitia
32) Rojszczak, M. (2020). CLOUD act agreements from an EU perspective. *Computer Law & Security Review*, *38*, 105442. https://doi. org/10. 1016/j. clsr. 2020. 105442
33) Sasongko, A. (2010). Cybercrime Legislation of Indonesia. In *Octopus Interface Conference-Cooperation against Cybercrime*.
34) Saputra, R., Setiodjati, J. P., & Barkhuizen, J. (2023). Under-Legislation in Electronic Trials and Renewing Criminal Law Enforcement in Indonesia (Comparison with United States). *Journal of Indonesian Legal Studies*, *8*(1), 243–288. https://doi.org/10.15294/jils.v8i1.67632
35) Sitompul, J. (2017). *Latar Belakang UU ITE*.
36) Sitompul, J. (2024). Akses Bukti Elektronik Lintas Batas Memperkuat Hukum dan Praktik Indonesia dalam Penyelidikan Tindakan Pidana Siber. *Kencana, Jakarta*.