

Due Process in a Search of Electronic System By Patrol Officer

Fridolin Nawa (a), Shierren Veronica (b), Anton Hendrik Samudra (c)(d)*, Peter Jeremiah Setiawan (e)

(a) Universitas Surabaya, fridolinnawa99@gmail.com

(b) Universitas Surabaya, shierrenvero@gmail.com

(c) School of Law, University of Leeds, UK, lwahs@leeds.ac.uk

(d) Universitas Surabaya, antonhendrik@staff.ubaya.ac.id
Universitas Surabaya, peterjeremiahsetiawan@staff.ubaya.ac.id

Halaman | 80

Abstract

The criminal justice system provides the legal framework for a fair and justifiable search. A search is justifiable when there is a search warrant or strong suspicion of crime by the police. However, instances of coercion and arbitrary acts by law enforcement officers still occur in practice, as seen in the case portrayed in East Jakarta. While this case does not represent the behaviour of all law enforcement officers, the standard for a fair search must be enforced. This article discusses the legal procedures for conducting a justifiable search of electronic systems suspected to be a tool of crime and evaluates whether such a search would violate the right to privacy. The article provides an academic discussion and evaluation of criminal law procedures in practice, using doctrinal research to scrutinize the provisions within the Electronic Information and Transaction Law (EITL), Criminal Procedure Law (CPL), and Personal Data Protection Law (PDPL) to determine the parameters of a justifiable search of an electronic system that conforms to the due process of law. Additionally, a comparison between the PDPL and the UK GDPR, as well as the 2018 Data Protection Act, was conducted to evaluate the privacy provisions in a search activity by law enforcement officers. The research finds that not every patrol officer has the justified measures to conduct a search on an alleged person, unless there is enough probable cause as stipulated in the CPL. Searches of civilian cell phones that are not in accordance with CPL, EITL, and PDPL should be considered illegal, and the officer who conducts them should be held accountable, both legally and ethically.

Keywords: Criminal justice; Search; Law enforcement; Privacy; Legal procedures.

1. Introduction

One of the [Law No. 11 of 2008 on Electronic Information and Transaction Law \(EITL\)](#) enactment purposes is to respond to technology development, which allows legal actions in cyberspace, including the detrimental ones.¹ There were new criminal provisions and criminal law procedures introduced in the EITL. The criminal law procedure was intended to complement the criminal law procedure which was stipulated in the [Law No. 8 of 1981 on Criminal Procedure](#) (1981 Criminal Procedure Law)(CPL).

The judicial process in Indonesia is based on the principle of due process of law. This is an implementation of the criminal justice system that emphasizes protection, guarantees, and upholding human rights (Tahir, 2010). This principle is universally recognized successively among them in Magna Charta 1215, Bill Of Rights, Miranda Rules to the United Nations Declaration and resolutions, which are then concretely also regulated in [Judicial Power Law \(JPL\)](#), the CPL and EITL. This principle is based on the understanding that every process in the criminal justice system must be based on certain standards according to laws and regulations and based on the protection of individual citizens rights (Hiariej, 2012). Every criminal justice

¹ See Section c, Consideration of the Law No. 11 of 2008 on Electronic Information and Transaction Law.

* Corresponding author

Halaman | 81
**Due Process in a
Search of Electronic
System By Patrol
Officer**

Fridolin Nawa
Shierren Veronica
Anton Hendrik Samudra
Peter Jeremiah Setiawan

procedure with a due process of law, is based on 2 tests, whether the state in the process has eliminated the life, freedom or property rights of the suspect without a procedure and if using a procedure whether the procedure is in accordance with the due process (Wasserman, 2004, p. 1). This principle is aimed at avoiding arbitrary trial proceedings or only based on the power of the apparatus, which can lead to violations of human rights (Reksodiputro, 1994). The implementation of this principle is not only aimed at the right to life and individual freedom, but also includes the right to property (Harahap, 2008). Statutory provisions limit every action of law enforcement officials to ensure compliance with existing provisions and procedures and prevent violations of human rights (Husin K & Husin B, 2016). The Indonesian criminal justice system recognizes several processes including arrest, detention, search, and confiscation. In accordance with the due process of law, Article 7 of [Judicial Power Law](#) and the CPL regulates the implementation of arrest, detention, search and confiscation procedures, that the main thing is that the those legal process cannot be carried out without an official who has authority based on law and only in matters and in a manner regulated by law.

A search is one of the forms of an investigator's authority which is justified by law should a crime be suspected. There was a broadcast on December 17th, 2019 in one of the local television stations, which demonstrated a night patrol carried out by East Jakarta Resort Police Patrol Team. The patrol team stopped a civilian who was crossing around Cipinang, East Jakarta. After the civilian was stopped, the patrol team proceeded to search the civilian and one of the patrol officers (R) asked the civilian to hand over his mobile phone. The civilian refused but R insisted by saying that he had the authority to check the contents of the mobile phone. Witnessing the commotion, patrol officer MPA as the leader of the patrol team approached the civilian and explained the situation with some coercion, however, there was not any clear base stated. Eventually, MPA did the search with baseless accusations, yet the search did not find any indication of any crime as alleged before. It cannot be said that this case represents the whole picture of law enforcement, however, a case like this should have been addressed accordingly.

In carrying out their duties, police officers are allowed to use coercion if necessary, in terms of force for a search, for instance; moreover, force third parties to follow the procedures. Coercion raises the potential of human rights violations, thus it is necessary to have a set of rules that gives limitations for the police to exercise their authority. These rules must also determine the conditions that should be fulfilled by police officers when they coerce someone (Utomo, 2005). Unconsented search effort must, of course, be carried out responsibly according to the provisions of law and applicable law (due process of law), if it is not, the search should be considered as illegal.

Based on the statute limitations in Article 33 [CPL](#), a search could carried out by investigators when:

- a. they have a search warrant signed by the Chair of Local District Court,
- b. they have official assignment to do so signed by the investigators' commander in chief,
- c. it is witnessed by two witnesses if the search is consented by the property owner, however, if the property owner does not consent nor attend, the search must be witnessed by the chair of the neighborhood,

After the search is conducted, within two days, the investigators are required to make an official search report, and the copy should be provided for the owner or occupant of the house or premise concerned.

When investigators need to search in very necessary and urgent situations, Article 34 of the CPL regulated the following:

- a. The search can be carried out immediately without a search warrant signed by the Chair of Local District Court,
- b. Within a maximum of two days after a search is carried out, the investigator must make an official search report,
- c. A search is only carried out on objects related to the crime in question, and it is an obligation of the investigator to immediately report the search to the Chair of Local District Court for it had been carried out in very necessary and urgent situations.

Besides the statute limitations in the CPL, Indonesia had just recently passed the Personal Data Protection Bill into [Law No. 27 of 2022 on Personal Data Protection](#) (Personal Data Protection Law)(PDPL). The recently inaugurated law prioritized and regulated how one's personal data should be protected and can only be accessed by certain parties. These parties include the data subject and also the processor of the data. Searches in this case would be considered as one of the ways to obtain data and is considered to be part of data processing as stated in Article 16 of PDPL, processing data includes actions of obtaining and collecting data, processing and analysis of data, data storage, data correction and update, appearance; announcement; transfer; distribution; or disclosure of data; and/or erasure or destruction of data. Data processing, in this case a search, must obey the provisions of PDPL which stated that to process data, they must obtain consent from the data subject first.

The search of electronic systems further regulated in EITL, as regulated in Article 43 EITL, concerns investigation against specific criminal acts in fields of information, technology, and electronic transactions, which are stipulated within EITL. Investigators from The Police of Republic of Indonesia and investigators from Civil Servants within the scope within tasks related to information, technology, and electronic transactions are given the authority to conduct the investigation. Investigations are carried out by paying attention to privacy protection, data confidentiality, public service availability, and evidence integrity. Search, according to EITL, is regulated in Article 43(3) which regulates that searches and/or confiscation of electronics systems related to alleged criminal acts in the field of information, technology, and electronics are carried out in accordance with the provision of the CPL.

Based on the elaboration above, the problem question in this article is: What are the legal procedures for a justifiable search of electronic systems in accordance with the due process of law based on the Criminal Law Procedure Law (CPL), Electronic Information and Transaction Law (EITL), and Personal Data Protection Law (PDPL)?

2. Discussion

2.1. Due process based search according to CPL and EITL

Due process of law is a crucial aspect of implementing the rule of law and safeguarding citizens against arbitrary treatment by the judiciary and other officials. It involves regulating legal procedures, setting limitations on actions such as search and seizure, and providing various procedural protections to prevent unfair application of the law or deprivation of life, liberty, and property (Sullivan and Massaro, 2011).

The implementation of due process laws focuses on ensuring procedural rights and brings legal consequences to the exercise of authority by law enforcement officials (Hieariej, 2012, p.

30). This includes their use of coercion (*dwang middelen*), such as in the context of arrest, detention, search, or seizure during the investigation of alleged criminal cases.

The essence of due process of law lies in protecting individuals from arbitrary actions by the government. It is a constitutional guarantee that prevents individuals from being deprived of their life, liberty, or property without just cause. Essential elements of due process include the right to a fair hearing, legal counsel, defense, presentation of evidence, and a fair and impartial court (Tahir, 2010).

The principle of due process of law is fundamental and must be upheld in all aspects of law enforcement. In Indonesia, the current criminal procedural law, which is based on the Code of Criminal Procedure (CPL), applies the principle of due process. Additionally, special laws contain provisions related to criminal procedure. The purpose of criminal procedure law is generally seen as limiting the power of the state when it comes to dealing with citizens involved in the criminal justice process (Reksodiputro, 2020).

For the effective and universal protection of human rights, it is essential to regulate the principle of human rights protection in applicable provisions, ensuring that law enforcement authorities abide by and respect human rights. Both law and human rights are binding on everyone, striking a balance between individual rights, freedom, and the obligation to respect the human rights of others within their social order (Zubairy et al., 2021).

Due process of law must be considered in the whole process of the criminal justice system, including in the pre-investigation (*penyelidikan*) and investigation (*penyidikan*) process; where the police, among others, are given the authority to carry out coercive measures. The coercive measures regulated in CPL can be exercised in arrest, detention, search, and confiscation. There are complaints about the existence of various investigative procedures that deviate from provisions of the criminal law procedure, or the discretion exercised by investigators which is contrary to human rights in the investigation process. Referring to research by KontraS, during July 2021 until June 2022 there were 647 cases of violence involving police officers which consisted of 456 shooting, 83 persecution, 47 arbitrary arrest, and 43 violent dispersal of demonstration cases (Dzulfaroh, 2022). If it is not carried within the prescribed criminal law procedure, the investigation that uses coercive measures could be considered unlawful. Although Indonesia is a non-stare decisis country, there was a pre-trial hearing decision No. 38/Pid.Pra/2022/PN JKT.SEL, which stated that investigation, search, and confiscation carried out by the investigators against Titan Infra Energy Company as unlawful; it could be set out as a precedent which could be cited by the next judges for the similar cases.

A search is a necessary force to be carried out in investigations by the police, even though it is a deprivation of a person's freedom and rights of property. In principle, no one should be forced to undergo arbitrary and unlawful interference to their privacy, family, home or correspondence. Everyone has the right to be protected by law against harassments or even assaults against them. The justification for the law enforcement to exercise coercive effort is prescribed by law, however it has its limitations to prevent human rights violation. There was a problem during its application, when the law enforcement exercised improper use of authority, took the effort beyond or deviated from the procedure that was given by the law.

To prevent arbitrary acts of interfering in private rights, CPL stipulates the basic principles of carrying out searches in detail. For human rights consideration, every search must be carried out with great care and within the limits and methods specified in CPL and other special laws related to criminal procedure law.

There are two forms of searches based on the CPL: house searches and body searches. The legal basis for a search is provided by Article 32 and 33(1) and 33(2) of the CPL. The objects of a search are houses and closed spaces related to the crime, and the suspect's body and clothes. A house search can only be conducted by investigators, while a clothes search can be ordered by detectives when arresting a suspect, and there is strong evidence and sufficient reason to believe that the suspect is carrying objects that can be confiscated as evidence. However, due to technological advancements, the EITL has prescribed norms for electronic device searches in Article 43(3), which refers to the provisions of the CPL because the EITL is not a procedural law.

There was a search attempt in 2019 toward civilians, and was broadcasted in one of national televisions, by patrol officers that coerced the civilians to hand over their mobile phones to be searched. The patrol officers said that they have a strong suspicion of the civilians. As prescribed in the CPL and EITL, a search should be carried out considering the rules as follow:

1. Article 32 CPL stated that a search can only be carried out if there is a suspected crime found during the investigation or any examination by the investigators including limitative forced measures as stipulated within,
2. Article 33(1) CPL, a police officer who is on duty cannot arbitrarily search mobile phones which belong to a civilian without a search warrant from the Chair of a Local District Court. The warrant should explain that there is a strong suspicion of a crime which could be proven with the mobile phone content as the evidence. The investigators need to be very careful before requesting a warrant, should it be proven otherwise, the search can be considered illegal and violates the CPL provisions.
3. Article 33(2) CPL stipulated that in the case of conducting a search, a police officer must be accompanied with a written order from his superintendent, or in this case an investigator, whether it is a letter of assignment or a search warrant. This is essential because a search is a violation of human rights. A written order from an authorized official is required as a justification in an attempted forced search.
4. Article 34 CPL regulated that for urgent and necessary circumstances, a search can be immediately carried out towards someone suspected of committing a crime. In the event of being caught red-handed, it is not possible to wait for a warrant from the Chair of the local district court beforehand. However, investigators are still required to report to the Chair of the local district court afterward to obtain the following warrant and make an official report and its copies to the person of interest. The discernment of necessary and urgent situations is emphasized on the relatively subjective assessment of the investigator (Harahap, 2003). But, there is an ethics committee to evaluate the investigators decision.
5. A body search is carried out based on Article 37 of CPL, which includes the status of the person being searched as a suspect. It can be carried out by investigators when making an arrest. However, investigators are only authorized to search clothes including objects carried and in the possession of the person of interest in cases of strong suspicion and sufficient reasons.
6. A mobile phone search must be carried out in accordance with the provisions in EITL. Article 43(3) of EITL regulates searches of electronic systems, related to alleged criminal

acts in the field of information technology and electronic transactions carried out according to the CPL provisions.

Looking at the statute limitations, the search in the case *a quo* was not in accordance with the procedures specified in CPL and EITL, as the search did not meet the statutory provisions.

Article 16(1)d of [Law No. 2 of 2002 on State Police of the Republic of Indonesia](#) regulates the legal basis of police officers authority to order a suspected person to stop, ask, and examine personal identification, stated that it must be carried out with due observance of the procedures for exercising authority as stipulated in the [Indonesia Police Chief Regulation \(IPCR\) No. 8 of 2009](#). In the regulation, there are provisions that must be followed by the police officers before they are able to conduct a forced search. In Article 32(1) IPCR No. 8 of 2009, police officers must identify themselves, show a letter of assignment, and clearly explain the purpose of the search. In addition, the officers must ask for a consent from the person being searched, and apologize for the disruption of their rights of privacy because of the search. The search must be conducted thoroughly, politely, ethically, sympathetically and taking the rights of the person being searched into account. At the end of the search, police officers are obliged to thank the person for being searched. But even then, if the implementation is not carried out in accordance with the criminal law procedures, then the search is considered unlawful.

Restrictions on conducting a search are further stipulated in Article 32(2) IPCR No. 8 of 2009. Article 32(2)b stipulates that “police officers are prohibited from carrying out excessive searches that might result in deprivation of the privacy rights of those being searched”. Relating to the development of technology, digital devices play an important role in the investigation of a crime. Frequently, data contained in the digital device could be a lead or indication of a time when a crime occurs or occurred. It is common for investigators to search electronic systems of the person of interest to collect evidence related to a suspected crime. However, practically, the data in the digital devices could relate to other persons or parties which is considered as personal data, for instance, someone’s personal information that is not related to the crime being investigated. This raises concerns about the potential breach of privacy caused by the search.

Police officers, such as MPA and R, must have a compelling basis, including a search warrant from the Chair of the Local District Court that explains that there is a strong suspicion of a crime, which could be revealed with digital evidence in the person of interest’s digital device. If there is a strong suspicion that the evidence in the mobile phone is part of a crime committed, then police officers have the authority to inspect the mobile phone. However, in that particular search conducted by MPA and R, there was no compelling basis for the search as for reading private conversations, personal information, and everything in the digital device. As it turned out, the suspected crime was not there. When the officers of the law cannot explain the urgency of the search from its starting point, and the civilian did not give his consent, then the officers do not have the basis of authority to search his digital device. Additionally, Article 30 EITL states that any individual who intentionally and unlawfully accesses a computer or electronic system in any manner for the purpose of obtaining electronic information or documents can be subject to punishment.

2.2. Privacy issues in search according to PDPL

In Indonesia, personal data protection is regulated by [the PDPL](#), which was finally passed last year. It is a set of regulations that aim to protect the privacy of individuals by regulating

how personal data is obtained, used, and stored. It also provides individuals with certain rights regarding their personal information. The law requires organizations to obtain consent from individuals before collecting, processing and using their personal data, and to ensure that the personal data is protected against unauthorized access, alteration and loss. Organizations must also take appropriate measures to ensure the accuracy and security of the personal data they hold, and to delete the personal data when it is no longer necessary. Organizations must appoint a data protection officer, who is responsible for ensuring compliance with the PDPL. The law also gives individuals the right to access, correct and delete their personal data, and to file a complaint if their personal data is mishandled.

The PDPL, unfortunately, does not set out statutory limitations on how search activities can be conducted in order to protect the privacy of individuals. In addition, it does not outline the responsibilities of those conducting searches and provides guidance on how to ensure that searches are conducted in accordance with the law. There is no provision Indonesia's PDPL states anything regarding search activities. It was enacted specifically to address personal data and privacy as fundamental rights of men, and to give a standard of general personal data protection.² However, it does not anticipate specifically in search and seizure measures of electronic systems which inevitably encounter personal data. Article 15 PDPL provides an overview of what rights of personal data that would be derogated for specific occasions, including law enforcement. Therefore, the accused could not dwell on his personal data protection under the PDPL, should the law enforcement engage a search to his electronic system. However, the law enforcement has the statute of limitations to obtain enough evidence before a search warrant could be asked to the Chair of the Local District Court as mentioned in the previous discussion.

Various countries have enacted laws that regulate personal data protection with the rise of concerns of personal data breaches in the world, one of which is the United Kingdom. The personal data protection law made by the United Kingdom is known as the [United Kingdom's General Data Protection Regulation](#) (UK GDPR) which was made from the awareness to prevent personal data from becoming the new 'currency' in the digital world. ([Hoofnagle, Sloot, Borgesius, 2019](#)). After the UK GDPR was made, the United Kingdom implemented these rules in [the 2018 Data Protection Act](#) (2018 DPA). With the 2018 DPA, laws regarding data protection that are certain and binding were created. The 2018 DPA regulates the rights of the data subject to get protection of their personal data. As stated in Chapter 1, Article 2(1) about protection of personal data, it is stated that the GDPR protect individuals with regard to the processing of personal data, in particular by: a) requiring personal data to be processed lawfully and fairly, on the basis of the data subject's consent or another specified basis, b) conferring rights on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and c) conferring functions on the Commissioner, giving the holder of that office responsibility for monitoring and enforcing their provisions. Other than that, data subjects also have the right to access, information, rectification, erasure or restriction of processing, right not to be subjected to automated decision making, to intervene in automated decision making, to information about decision making, and object to processing. This means that the rights given to the data subjects are proof that the principle due process of law is in action. With the 2018 DPA, which has been developed since the 90s, many countries

² See General Elucidation of PDPL

decide to implement data protection law with one of them being Indonesia. Therefore, 2018 DPA can be used as comparison for the newly made data protection law of Indonesia.

Based on Article 1 PDPL, personal data is data related to an individual who is identified or can be identified separately or combined with other information, either directly or indirectly through electronic or non-electronic systems. Personal data can only be accessed by the data subject (owner) and data controller. Based on the UK GDPR, controller means a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In accessing personal data, a controller must have consent from the data subject. This is also mentioned in Chapter 2 Article 35(2)a 2018 DPA, that the data subject must give consent to controllers (law enforcers) if the controllers want to process the data. Personal data processing based on the UK GDPR is a broad range of operations including collection, structuring, dissemination and erasure of data. During the data processing, legitimate interest becomes the base for both the data controllers and data subject. The UK GDPR imposes a balancing test, in which the legitimate interest of the data controller must be balanced against the interests of data subjects, and to have a lawful, legitimate interest, the latter should not outweigh the former (Mazzi et al, 2022). The UK GDPR also offers personal protection from self-incrimination. Article 20(1) 2018 DPA stated that a person need not comply with the listed GDPR provisions to the extent that compliance would, by revealing evidence of the commission of an offence, expose the person to proceedings for that offence. Indonesia has not yet made this kind of rule which led to some cases that let people self incriminate themselves. Regarding personal data, there are restrictions or forbidden actions stated in Article 65 and 66 PDPL. Article 65 stipulates three forbidden actions which includes obtaining or collecting personal data that does not belong to them with the intention of benefiting themselves or others which can result in loss for personal data subjects, disclosing, and using personal data that does not belong to themselves. While Article 66 PDPL specifies on prohibiting anyone from making false or falsifying personal data with the intent to benefit themselves or others which can cause harm to others. If someone violates these two articles, then they will be subjected to criminal provisions regarding data protection, which includes Article 67 until Article 73 PDPL.

The UK GDPR is a long-standing law that has established specific provisions concerning issues such as investigations or searches that may pose a risk to privacy. However, these specific provisions are not yet available in Indonesia since the law is relatively new, and there have not been any real implementations yet. Therefore, Indonesia's PDPL can be considered flawed in certain areas, particularly regarding searches and investigations. In the UK GDPR, specifically in Part 3, Article 34(1) regulates the six principles of controllers during data processing. These principles include ensuring that processing is lawful, fair, and for explicit and legitimate purposes. They also include making sure that personal data is accurate, relevant, not excessive, and is kept secure. Article 35(2)(a) UK GDPR also states that the processing of personal data for law enforcement purposes is lawful only if it is based on law and the data subject has given their consent for that purpose. However, Indonesia has not developed similar provisions, which has resulted in cases like MPA and R. While the CPL have provisions regarding searches, they lack any explanations regarding privacy issues, making the privacy of data subjects vulnerable to disclosure during searches or data processing. Although it is not in the PDPL, Indonesia could enforce punishments for a person who illegally process data as in the EITL criminal provisions should any violations occur; whereas in the UK GDPR, when a

data controller who violates any of the six principles can be fined up to 20,000,000 Euros or 4% of the global annual turnover, whichever is greater (Baker, 2020).

A search can be categorized as one of the ways to collect or obtain personal data which means that it can be deemed as one of the ways to process data. This is specified in Article 16(1) PDPL which states that processing data includes actions of obtaining and collecting data, processing and analysis of data, data storage, data correction and update, appearance; announcement; transfer; distribution; or disclosure of data; and/or erasure or destruction of data. Data controllers may conduct data processing, a search in this case, as long as it obeys the provisions stated in Article 16(2) PDPL. However, it does not explicitly stipulate that police investigators are within its scope. As it is a way to obtain someone's data, a search supposedly be conducted according to the provisions, and yet, the PDPL does not provide this because it is considered as one of the administrative laws.

An investigator is justified to collect or obtain someone's data if the person is suspected to possess evidence or unlawful material(s). For example, there was a case where a civilian by the name of Peirson was searched by a police officer with consent and found drug related messages inside his phone. To conduct a lawful search, then police must be able to show a search warrant or can prove that the processing can be accounted for, as stated in Article 16(2) PDPL. If the police cannot provide a search warrant or prove anything, then the police must ask consent from the data subject to conduct the search. This is specified in Article 20(2)a PDPL which requires consent from the data subject for one or several specific purposes. Article 21(1) PDPL also regulated that data controllers are obliged to deliver information to the data subject about the legality and purpose of data processing, the type and relevance of the personal data, the retention periods for documents containing personal data, details regarding the information collected, period of data processing, and rights of the data subject. The police may conduct a warrantless search when there is a strong allegation that the data subject has or keeps evidence of committing a crime. If the subject does not give consent then the police may seize the item as evidence and can only examine the phone after they have an authorized warrant. (Raj & Marshall, 2019). However, if the search conducted does not follow the provisions of PDPL then the search would be considered as illegal and a breach to one's personal data. 2018 DPA stipulated that a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. Therefore, an illegal search could be subjected to personal data breach as it is a way to obtain data by accessing through them. If an illegal search was indeed conducted then they will be subjected to Article 67(1) PDPL which states that every person who intentionally or unlawfully obtains or collects personal data that does not belong to him with the intention of benefiting himself or another person which can result in loss of personal data as referred to in Article 65 (1) shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah).

MPA and R were unable to show any warrant to search the mobile phone, and did not inform the civilian of the purpose and legal grounds of the search and did not ask for consent from the civilian being searched, instead abusing their authority to conduct the search. MPA and R do not have any evidence that the civilian withheld crime evidence on their mobile phone resulting in the search becoming a personal data breach for the civilian. But if there is indeed evidence on the mobile phone which proves that the civilian committed a crime or the search was carried out in accordance with the CPL provisions, then this cannot be categorized as a

personal data breach because as stated in Article 15(1) PDPL, the rights of data subject are exempt in the interests of national defense and security, law enforcement process, public interest in the framework of administering the state, supervising the financial services sector; monetary; payment systems; and financial system stability carried out in the framework of administering the state; or statistical interests and scientific research.

The search conducted by MPA and R were not in accordance with CPL provisions then they violated Article 24(2) PDPL about proof of consent - because they did not have a search warrant, from data subject during the data processing, as well as being subjected to Article 13 PDPL which regulates that the data subject has the right to demand and receive compensation for violations of their personal data in accordance with the law and Article 50 PDPL in which they will receive sanctions in the form of compensation and/or administrative fines. In criminal provisions, they will be subjected to Article 67(1) PDPL which states that every person who deliberately and unlawfully obtains or collects personal data that does not belong to them with the intention of benefiting themselves or others which can result in loss for the data subjects as referred to in Article 65(1) shall be subjected to imprisonment for a maximum of 5 (five) years and/or a maximum fine Rp5.000,000,000,00 (five billion rupiahs).

3. Conclusion

Based on the description and discussion above, conducting a justifiable search of electronic systems in accordance with due process requires compliance with the CPL, EITL and PDPL. These laws establish the legal procedures that must be followed when conducting searches of electronic systems to ensure that human rights are protected and respected. The police must uphold the rights of civilians, and conduct searches in accordance with the provisions of CPL, EITL and PDPL, including obtaining a search warrant and permit from the Chair of the District Court. Therefore, it is essential to follow these legal procedures to ensure that the search of electronic systems is justifiable and in accordance with due process. It can be inferred that the search carried out by the police officers in the case presented as an example was not compliant with the CPL, EITL and PDPL, and that the patrol officers do not have the justified measures to conduct a search on the alleged person. Searches of civilian cell phones that are not in accordance with CPL, EITL, and PDPL regulations may result in legal action being taken against the police officers who carry out illegal searches may face disciplinary or criminal charges. Furthermore, police officers must adhere to the instructions for carrying out police duties, including explaining the purpose of the search, obtaining consent, and conducting the search politely, ethically, and sympathetically while respecting the rights of the person being searched.

The suggestions given include ensuring that police officers implement their duties and powers in accordance with applicable regulations and codes of ethics, and that civilians have the right to ask for a warrant or permit during a search. Any civilian who is subjected to an arbitrary search by a police officer can report to the Occupation and Security Division at the local police station. If the search is considered as illegal, civilians can report it as a crime.

BIBLIOGRAPHY

Books:

- Atmasasmita, R. (2021). *Hukum Dan Penegakan Hukum: Seri Pemikiran Romli Atmasasmita* (1st ed.). KENCANA.
- Effendi, T. (2013). *Sistem Peradilan Pidana Perbandingan Komponen dan Proses Sistem Peradilan Pidana di Beberapa Negara*. Penerbit Pustaka Yustisia.
- Hamzah, A. (2016). *Hukum Acara Pidana Indonesia*. (Tarmizi, Ed.; Edisi Kedua). Sinar Grafika.
- Harahap, M. Y. (1985). *Pembahasan Permasalahan Dan Penerapan Kuhap (Jilid I)*. Pustaka Kartini.
- Harahap, M. Y. (2008). *Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan Dan Penuntutan* (2nd ed.). Sinar Grafika.
- Hart, & Nusantara, A. H. G. (1986). *Hukum Acara Pidana Dalam Perspektif Hak Asasi Manusia* (Sarwoko, Ed.; 1st ed.). Yayasan Lembaga Bantuan Hukum Indonesia.
- Hartono. (2010). *Penyidikan & Penegakan Hukum Pidana Melalui Pendekatan Hukum Progresif* (1st ed.). Sinar Grafika.
- Hasibuan, E. S. (2021). *Hukum Kepolisian dan Criminal Policy dalam Penegakan Hukum* (Y. S. Hayati, Ed.; 1st ed.). Rajawali Pers.
- Huda, N. (2012). *Hukum Tata Negara* (6th ed.). Rajawali Pers.
- Husin, K., & Husin, B. R. (2016). *Sistem Peradilan Pidana Di Indonesia* (D. M. Listianingsih, Ed.; 1st ed.). Sinar Grafika.
- Makarim, E. (2005). *Pengantar Hukum Telematika Suatu Kompilasi Kajian*. PT Raja Grafindo Persada.
- Marzuki, P. M. (2005). *Penelitian Hukum* (Edisi Revisi). Kencana.
- Muis, A., Anwar, H., & Rosidawati, I. (2021). *Hukum Kepolisian Dan Kriminalistik* (A. Budiman, Ed.). Pustaka Reka Cipta.
- Nusantara, A. H. G., Pangaribuan, L. M. P., & Santosa, M. A. (1996). *Kitab Undang-Undang Hukum Acara Pidana dan Peraturan-Peraturan Pelaksana*. Djambatan.
- Ranoemihardja, R. A. (1981). *Hukum Acara Pidana*. Tarsito, Bandung.
- Reksodiputro, M. (2020). *Sistem Peradilan Pidana* (Y. S. Hayati, Ed.; 1st ed.). Rajawali Pers.
- Sadjijono. (2008). *Polri dalam Perkembangan Hukum di Indonesia: Vol. I* (M. Khoidin, Ed.). LaksBang PRESSindo Yogyakarta.
- Sasangka, H., Rosita, L., & Hadiwijono, A. (1996). *Penyidikan, Penahanan, Penuntutan dan Praperadilan* (Pertama). Dharma Surya Belian Surabaya.
- Suteki. (2021). *Hukum dan Masyarakat*. Thafa Media.
- Tahir, H. (2010). *Proses Hukum Yang Adil Dalam Sistem Peradilan Pidana Di Indonesia* (T. Sabriantina, Ed.; 1st ed.). LaksBang PRESSindo.
- Tri wibowo, K. (2020). *Hukum acara pidana: menggugat kelemahan kitab undang-undang hukum acara pidana di Indonesia* (B. Pasaribu & A. Harris, Eds.). Papas Sinar Sinanti.
- Utomo, W. H. (2005). *Hukum Kepolisian Di Indonesia*. Prestasi Pustaka.

Wasserman, R (2004). *Procedural Due Process: a Reference Guide to the United States Constitution*. Praeger Publishers

Journal articles:

Raj, Matthew & Marshall, Russ. (2019). *Examining The Legitimacy of Police Powers to Search Portable Electronic Devices in Queensland*. *The University of Queensland Law Journal*. 38(1), 107 - 115. <https://journal.law.uq.edu.au/index.php/uqlj/article/view/1547>

Sullivan, E. Thomas & Massaro, Toni M. (2011). *Due Process Exceptionalism*. *Irish Jurist (N.S.)* Vol. 46 (2011), 117-151. <https://www.jstor.org/stable/44027090>

Hoofnagle, C. J., Sloot, B. v.d., & Borgesius, F. Z. (2019). *The European Union general data protection regulation: what it is and what it means*. *Information & Communications Technology Law*. 28(1), 65 & 72. <https://doi.org/10.1080/13600834.2019.1573501>

Mazzi, Francesca; Adonis, Abid; Cowls, Josh; Tsamados, Andreas; Taddeo, Mariarosaria; Floridi, Luciano. (2022). *The UK reform of data protection: key changes and their ethical, social and legal implications*. *International Journal of Law and Information Technology*. 1(11), 3. <https://doi.org/10.1093/ijlit/eaac024>

Zubairy, A., Brigjen Hasan Basri, J., Banjarmasin, K., Kalimantan Selatan, P., & Brigjen Hasan Basri Komplek Polsek Banjarmasin Utara Jalur, J. H. (2021). *Reka Ulang Sebagai Alat Bukti Surat Oleh Penuntut Umum Dalam Perkara Pidana Berdasarkan Prinsip Due Process Of Law*. 270-188. <https://ojs.bdproject.id/index.php/jphi/article/view/34>

Websites:

Darmawan, R. A. (2021, October 19). *Viral Aipda Ambarita Periksa HP Warga Saat Patroli, Kopolnas: Keliru!* Detiknews. Accessed on March 9th 2022. <https://news.detik.com/berita/d-5773371/viral-aipda-ambarita-periksa-hp-warga-saat-patroli-kopolnas-keliru>

Dzulfaroh, A. N. (2022, Juli 4). *Survey Litbang Kompas: Citra Polisi Terus Menurun, Apa Penyebabnya?*. Accessed on December 5th 2022. <https://www.kompas.com/tren/read/2022/07/04/170000665/survei-litbang-kompas--citra-polisi-terus-menurun-apa-penyebabnya?page=all>

Puspita, R. (2022, January 24). *Kapolri Listyo Klaim Penyimpangan Anggota Polisi Menurun*. REPUBLIKA.CO.ID. Accessed on July 23rd 2022. <https://sindikasi.republika.co.id/berita/r67eb8428/kapolri-listyo-klaim-penyimpangan-anggota-polisi-menurun>

Baker, Alice. (2020, January 28). *A breakdown of the GDPR's six data processing principles*. itgovernance.eu. Accessed on February 26th 2023. <https://www.itgovernance.eu/blog/en/a-breakdown-of-the-gdprs-six-data-processing-principles>