Indonesia Law Review (2017) 3: 201 - 221
ISSN: 2088-8430 | e-ISSN: 2356-2129

DEVELOPING A LEGAL FRAMEWORK OF PERSONAL DATA PROTECTION IN THE INDONESIAN CRIMINAL PROCEDURE LAW

Josua Sitompul*

* PhD candidate at the Department of Criminal Law and Criminology, Faculty of Law, Maastricht University,

Article Info

Received : 25 November 2019 | **Received in revised form :** 13 December 2019 | **Accepted :** 18 December 2019
Corresponding author's e-mail : josua.sitompul@maastrichtuniversity.nl

Abstract

Searching and seizing voluminous data is a challenge that Indonesian law enforcement authorities should resolve. Indonesia does not have a comprehensive regime on personal data protection. The absence of a coherent legal framework on personal data protection does not negate the obligation of Indonesian law enforcement authorities to protect personal data of Indonesian subjects. However, the absence of the framework may lead to uncertainties or ambiguities on how the authorities should protect personal data. Against the uncertainties and ambiguities, Indonesian law enforcement authorities should resolve issues of voluminous data in obtaining e-information with the prevailing legislation. This article attempts to answer the question: how may Indonesian law enforcement authorities interpret the current law to establish a coherent legal framework to protect personal data in searching or seizing voluminous data? The interpretation is instrumental in supporting the development of the Indonesian regime on personal data protection. It proposes that the Indonesian criminal procedure law should emphasise the active role of the chief judges of competent district courts and should incorporate particularity and proportionality as conditions and safeguards in the execution of search and seizure.

Keywords*: cybercrime, search, seizure, voluminous data, personal data protection, KUHAP, Budapest Convention*

Abstrak

Penggeledahan dan penyitaan terhadap data yang banyak (voluminous data) merupakan satu tantangan yang aparat penegak hukum Indonesia harus selesaikan. Indonesia belum memiliki rezim yang komprehensif mengenai perlindungan data pribadi. Ketiadaan kerangka hukum yang koheren dalam perlindungan data pribadi tidak menghilangkan kewajiban aparat penegak hukum Indonesia untuk melindungi data pribadi dari warga negara Indonesia. Akan tetapi, ketiadaan kerangka hukum tersebut dapat mengakibatkan ketidak pastian dalam melindungi data pribadi. Terhadap ketidakpastian tersebut, aparat penegak hukum Indonesia harus menyelesaikan permasalahan perlindungan terhadap data pribadi dengan menggunakan hukum yang telah ada. Artikel ini berusaha untuk menjawab pertanyaan: bagaimana aparat penegak hukum Indonesia dapat menginterpretasikan hukum yang ada dalam membangun suatu kerangka hukum yang koheren untuk memberikan perlindungan data pribadi dalam penggeledahan dan penyitaan. Interpretasi ini instrumental dalam mendukung pengembangan rezim perlindungan data pribadi di Indonesia. Artikel ini merekomendasikan agar hukum acara pidana Indonesia menekankan pada peran aktif ketua pengadilan negeri dalam memberikan perlindungan data pribadi dan memasukkan spesifisitas dan proporsionalitas sebagai ketentuan dalam penggeledahan dan penyitaan.

Kata kunci*: cybercrime, penggeledahan, penyitaan, voluminous data, perlindungan data pribadi, KUHAP, Konvensi Budapest*

DOI : http://dx.doi.org/10.15742/ilrev.v9n3.582

I. INTRODUCTION

Searching and seizing voluminous data is a problem that Indonesian law enforcement authorities should resolve. In daily practice, investigators execute their search and seizure powers to obtain evidence stored in email accounts, social media accounts, laptops, and smartphones[1] that may contain irrelevant voluminous personal data to an investigation. The chief judges of competent district courts issue warrants for searching and seizing voluminous data. They also approve urgent searches and seizures of copious electronic information. A smartphone can have a storage capacity of 64 or 128 gigabytes, and a laptop of 256 or 500 gigabytes. One gigabyte of NSF file format can have 9,000 emails and 3,000 attachments.[2] One gigabyte of a USB stick can store 357 photos of eight-megapixel size. In this respect, Indonesian law enforcement authorities should strike a balance between enforcing the law (obtaining e-evidence and divulging a suspect's identity and location) and protecting the personal data of Indonesian subjects regardless of their status (a suspect, a defendant, a victim, or a witness).

Indonesia lacks a comprehensive regime of personal data protection. The Indonesian government has prepared the Bill on Personal Data Protection.[3] It took into consideration legislation and case law from the European Union (EU) and the United States (US) as references for drafting the Bill. However, the Bill does not cover specifically the criminal justice areas (pre-investigation (*penyelidikan*), investigation (*penyidikan*), and criminal proceedings). The absence of a clear legal framework on personal data protection does not negate the obligation of Indonesian law enforcement authorities to protect the personal data of Indonesian subjects. However, the absence of the framework may lead to uncertainties or ambiguities on how the authorities should protect personal data.[4] Against the uncertainties and ambiguities, Indonesian law enforcement authorities should resolve issues of voluminous data in obtaining e-information with the prevailing legislation.

This article attempts to answer the question: "How may Indonesian law enforcement authorities interpret the current law to establish a coherent legal framework to protect personal data in searching or seizing voluminous data?" The interpretation is instrumental in supporting the development of the Indonesian regime on personal data protection. This article employs a doctrinal method to answer the question. It not only analyses the related provisions prescribed in the Constitution of Indonesia 1945, the Indonesian criminal procedure law, and other legislation that governs personal data protection but also examines relevant decisions of the Constitutional Court of Indonesia and cybercrime cases.

The article is structured as follows. After the introduction in part I, parts II and III re-construe the constitutional foundation for protecting personal data within

[1] Josua Sitompul, "Indonesian Cybercrime Verdicts Collected 2016-2018," Dans.knaw.nl, https://doi.org/10.17026/dans-zrh-cfub. The data set contains 123 decisions of district courts in Indonesia.

[2] Data Volume Estimates and Conversions, https://www.sdsdiscovery.com/resources/data-conversions/, accessed 13 November 2019.

[3] Indonesia, *Rancangan Undang-Undang tentang Perlindungan Data Pribadi* (Data Protection Bill), Draft 29 April 2019 (RUU Perlindungan Data Pribadi)

[4] Sitompul, "Indonesian Cybercrime Verdicts Collected 2016-2018". Indonesian courts have tried many cybercrime cases in which voluminous data is a core issue. However, it is unclear how the courts strike a balance between protecting personal data and accommodating the law enforcement interest to obtain e-evidence. It is also unclear how investigators protect personal data in investigation or pre-investigation phase.

the Indonesian criminal justice areas. Part II argues that enforcing law and justice as prescribed in Article 24(1) of the Constitution of Indonesia 1945 should serve as the constitutional objective of the Indonesian inquisitorial system. Ascertaining the material truth (*kebenaran materil*) is to serve the enforcement of law and justice. Part III discusses the personal data protection framework in the Constitution and legislation of Indonesia. Part IV identifies the gaps and uncertainties in protecting personal data under the criminal procedure law. It explains the principles and provisions of search and seizure prescribed in the Indonesian criminal procedure law, and it examines the limitations in employing the search and seizure provisions in protecting personal data. Part V attempts to re-construe the conditions and safeguards in the execution of search and seizure. It emphasises the active role of the chief judges of competent district courts in determining the reasonableness of searching and seizing voluminous data. Part V also explains the importance of incorporating particularity and proportionality as conditions and safeguards in a search and seizure. It gives an overview of particularity and proportionality in the US and EU member states. Part VI explains the further implications of the right to personal data protection as a constitutional right. Part VII concludes the article.

II. PROPOSING THE CONSTITUTIONAL FUNCTION OF THE INDONESIAN INQUISITORIAL SYSTEM

It is widely recognised that the objective of the Indonesian inquisitorial system is to ascertain–or at least as closely as possible–the material truth.[5] Ascertaining the truth is the responsibility of every law enforcement institution in investigation, prosecution, and adjudication. Defendants may challenge the facts or evidence presented by the law enforcement authorities. However, Act 8/1981 on Criminal Procedure Code (KUHAP)[6] does not prescribe the rights of defendants to gather and present evidence explicitly. At the normative level, the method of ascertaining the truth–prescribed in the KUHAP – is a manifestation of due process of law. The objective of due process is to protect Indonesian subjects' constitutional rights in administering justice. Ideally, neither of these two objectives (pursuing the material truth and due process) is higher than the other.

The objective of ascertaining the material truth is not a constitutional requirement. It is an axiom that is manifested in Article 183 KUHAP. According to the provision, a judge may not impose a penalty upon a defendant unless he concludes using at least two admissible (*yang sah*) legal means of evidence (*alat bukti*) that a crime was factually (*benar-benar*) committed and the defendant is guilty of committing it. The ascertained facts (the crime was committed, and the perpetrator committed it) were regarded as the material truth. The Constitutional Court of Indonesia reinforced the axiom. It considered that ideally, the material truth is 'the truth where there is no doubt.'[7] In practice, the material truth is understood as the legal construction of legal facts (*fakta hukum*) of a crime as postulated by the judicial panel in its decision. The legal construction is the ascertainment of whether a crime occurred and if the

[5] Other legal system may use 'objective truth' or 'ontological truth' (Elisabetta Grande, "Rumba Justice and the Spanish Jury Trial," in Comparative Criminal Procedure, ed. Jacqueline E. Ross and Stephen C. Thaman (Massachusetts: Edward Elgar Publishing Limited, 2018), p. 366.)

[6] Indonesia, *Undang-Undang tentang Hukum Acara Pidana (Law regarding Criminal Procedure Law), UU No. 8 Tahun 1981, NL No. 76 Tahun 1982 (Law Number 8 Year 1981, SG No. 1981).*

[7] The Constitutional Court of the Republic of Indonesia, "Decision 34/PUU-XI/2013", p. 83, consideration [3.15].

defendant's acts fulfilled every element of the crime. The ascertainment is based on legal means of evidence and evidentiary objects (*barang bukti*) presented at court.[8]

Arguably, Article 24(1) of the Constitution of Indonesia 1945 could serve as the source of the constitutional function of the Indonesian criminal justice system. The Article prescribes that the judicial powers are an independent power to enable the judiciary to enforce (*menegakkan*) law and justice. The adjudication institution is the last gate in the enforcement process under the criminal justice system. In this respect, the judiciary actualises its constitutional function of enforcing law and justice within the checks-and-balances mechanisms to the investigation and prosecution institution. It means that the obligation and responsibility to enforce law and justice are devolved on those institutions. Thus, both the investigation and prosecution institutions also bear the constitutional obligation and responsibility to enforce law and justice.

In this regard, ascertaining the material truth has a higher purpose. It is a means not only to determine the guilt of a defendant but also to satisfy the constitutional responsibility of law enforcement institutions: to enforce criminal law and justice. As the Constitutional Court underlined, criminal justice emphasises not only legal certainty but also justice.[9] Therefore, ascertaining the material truth is not the primary objective of the Indonesian inquisitorial system. To enforce criminal law and justice is its primary objective. Within this constitutional frame, ascertaining the material truth is subject to the rule of law as a fundamental principle of the legal system of Indonesia.[10]

Asshiddiqie[11] pointed out two main issues that have arisen in the development of the rule of law in Indonesia. They are the limitation of law enforcement authorities' powers[12] and the protection of constitutional rights. The Constitutional Court emphasised that the criminal procedure serves as a means of actualising due process of law,[13] as a fundamental element of the Indonesian rule of law. In this respect, contextualising the objective to ascertain the material truth within the constitutional framework has several implications. First, the objective is to protect human rights.[14] For a victim, the purpose of the ascertainment of the truth is to elucidate his loss and rights. For the perpetrator, it is to ascertain his guilt and impose a just penalty. Second, the Constitution would not prohibit competent authorities from having and executing coercive power to actualise their function in protecting constitutional rights. Third, however, to protect constitutional rights, competent authorities are not to exercise the investigative powers arbitrarily.[15] It means that the State's powers should be limited

[8] Indonesia, *Keputusan Menteri Kehakiman tentang Tambahan Pedoman Pelaksanaan Kitab Undang-undang Hukum Acara Pidana* (*the Decree of Minister of Justice regarding Additional Guidelines for the Implementation of the Criminal Procedure Law*), Keputusan No. M.14-PW.07.03 Tahun 1983 (Decree No. M.14-PW.07.03 Year 1983), General Part, Chapter I, Introduction. See also the District Court of Banda Aceh, "Decision 03/Pid.B/2015/PN Bna," p. 21.

[9] The Constitutional Court of the Republic of Indonesia, "Decision 34/PUU-XI/2013", p. 85, consideration [3.15].

[10] Article 3 Indonesia, *Undang-Undang Dasar Negara Republik Indonesia Tahun* 1945 (*the Constitution of the Republic of Indonesia Year 1945*). See also Article 28I (5) of the Constitution of Indonesia 1945.

[11] Jimly Asshiddiqie, Menuju Negara Hukum yang Demokratis, (Jakarta: Bhuana Ilmu Populer, 2009), p. 81.

[12] See also the Constitutional Court of the Republic of Indonesia, "Decision 65/PUU-VIII/2010", p.87, consideration [3.11].

[13] *Ibid*., p. 87, consideration [3.12].

[14] The Constitutional Court of the Republic of Indonesia, "Decision 21/PUU-XII/2014", p. 97, consideration [3.14].

[15] The Constitutional Court of the Republic of Indonesia, "Decision 20/PUU-XIV/2016", p.96, con-

and prescribed clearly under a particular Act.[16] The criminal procedure must have adequate constitutional conditions and safeguards to protect constitutional rights.

III. PERSONAL DATA PROTECTION FRAMEWORK IN THE CONSTITUTION AND LEGISLATION OF INDONESIA

This section discusses the right to personal data protection under Indonesian law. It starts by explaining the relationship between the right to privacy and the right to personal data protection under the Constitution of Indonesia 1945. Then, it discusses the provisions relating to personal data protection regulated in the Act 11/2008 as amended by Act 19/2016 on Electronic Information and Transaction (EITA),[17] the Government Regulation 71/2019 on Electronic System and Transaction (GR 71/2019), and the Regulation of the Minister of Communication and Information Technology 20/2016 on the Protection of Personal Data in the Processing of the Data in an Electronic System (Regulation of the MCIT 20/2016).

A. The Rights to Privacy and Personal Data Protection as Constitutional Rights

The protection of privacy and personal data in Indonesia has been regulated on a sector-by-sector basis.[18] The recognition of privacy protection in the areas of criminal justice, as part of constitutional rights, has gradually developed. The recognition of the right to personal data protection has emerged due to the EITA's enactment in 2008. However, the two rights have been regarded as emanating from the Constitution of Indonesia 1945. The following paragraphs discuss first the recognition of the right to privacy and, then, the right to the protection of personal data.

The original Constitution of 1945 contained no provision on the right to privacy.[19] The Constitutions of 1949 and 1950 recognised some manifestations of privacy

sideration [3.10]; the Constitutional Court of the Republic of Indonesia, "Decision 21/PUU-XII/2014", pp. 96, 100, considerations [3.14], [3.16]; the Constitutional Court of the Republic of Indonesia, "Decision 34/PUU-XI/2013", p. 84, consideration [3.15].

[16] Decision 20/PUU-XIV/2016, p. 93, consideration [3.9]. The case is of interception. See also the Constitutional Court of the Republic of Indonesia, "Decision 69/PUU-X/2012", p. 138, consideration [3.10.1]. The case is of interception.

[17] Indonesia, *Undang-Undang tentang Informasi dan Transaksi Elektronik (Law regarding Electronic Information and Transaction), UU No. 11 Tahun 2008, LN. No. 58 Tahun 2008 (Law Number 11 Year 2008, SG. No. 58 Year 2008), as amended by Undang-undang tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Law regarding the Amendment of Law Number 11 Year 2008 regarding Electronic Information and Transaction), UU No. 19 Tahun 2016, LN. No. 251 Tahun 2016 (Law Number 19 Year 2016, SG No. 251 Year 2008).*

[18] For example, in banking sector, bank secrecy is regulated under Indonesia, *Undang-Undang tentang Perbankan (Law regarding Banking), UU No. 7 Tahun 1992, LN. No. 31 Tahun 1992 (Law Number 7 Year 1992, SG. No. 31 Year 1992) as amended by Indonesia, Undang-Undang tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan (Law regarding the Amendment of Law regarding Banking), UU No. 10 Tahun 1998, LN. No. 182 Tahun 1998 (Law Number 10 Year 1998, SG. No. 182 Year 1998.* In health industry, secrecy of medical records is regulated under Indonesia, *Undang-Undang tentang Kesehatan (Law regarding Health), UU No. 36 Tahun 2009, LN. No. 144 Tahun 2009 (Law Number 36 Year 2009, SG. No. 144 Year 2009).*

[19] Josua Sitompul, "Perlindungan Privasi dan Data Pribadi: Suatu Telaahan Awal," Buletin Hukum Perbankan dan Kebanksentralan, 2013; Mahkamah Konstitusi, Buku I: Latar Belakang, Proses, dan Hasil Pembahasan UUD 1945, Revised ed., Naskah Komprehensif Perubahan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945: Latar Belakang, Proses, dan Hasil Pembahasan 1999-2002, (Jakarta: Sekretariat Jenderal dan Kepaniteraan Mahkamah Konstitusi, 2010).

protection.[20] The two Constitutions stipulated protection of non-interference with a residence and the secrecy of correspondence.[21] In 1959, Indonesia returned to the Constitution of 1945. During the Reformation era, there had been a series of amendments to the 1945 Constitution between 1999 and 2002 (to distinguish it from the original constitution, the term Constitution of Indonesia 1945 is used). However, in the Constitution of Indonesia 1945, the term "*privasi*" (privacy) as an umbrella term remains absent. Many publications have associated privacy with Article 28G(1) of the Constitution of Indonesia 1945,[22] but they have not substantively explained how this Article is associated with *privacy*.

Since 2003, the Indonesian Constitutional Court has authoritatively recognised privacy as a constitutional right in the areas of criminal justice. The Court has developed this recognition gradually from at least three decisions concerning interception and wiretapping in electronic communications. The applicants in the cases posited that interception or wiretapping was a human right infringement based on Article 28G(1) of the Constitution of Indonesia 1945.

Table-1: The Constitutional Court's Decisions on Privacy in Interception and Wiretapping

Decision	Provision of Act contested	Provisions of Constitution contested
006/PUU-I/2003	Article 12 (1)a. Act 30/2002 on the Corruption Eradication Commission: In a pre-investigation, formal investigation, and prosecution, the Corruption Eradication Commission has the authority to wiretap and record communication.	Article 28G (1): "Anyone has the right of protection for his or her self (diri pribadi), family, respectability (kehormatan), dignity (martabat), and property in his possession, and has the right to security and for protection from a threat to exercise or not exercise his human rights."
012-016-019/PUU-IV/2006		
5/PUU-VIII/2010	Article 31(4) Act 11/2008 on Electronic Information and Transaction: The procedures of lawful interception shall be regulated in government regulations.	

In Decisions 006/PUU-I/2003 and 012-016-019/PUU-IV/2006, the Court was silent on the link between the term 'privacy' and Article 28G(1). In Decision 006, it recognised that rights emanating from that Article are derogable human rights. The restriction of the rights, the Court ruled, should only be exercised in accordance

[20] Privacy protection is prescribed in Article 12 Universal Declarations of Human Rights.

[21] Articles 16 and 17 of the Federal Constitution 1949 and the Provisional Constitution 1950. See Kuntjoro Purbopranoto, Hak-Hak Asasi Manusia dan Pancasila, 4th ed. (Jakarta: Pradnya Paramita, 1969). See appendix.

[22] Sinta D. Rosadi, "Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia," Brawijaya Law Journal 5, no. 1 (2018): 145; Sinta Dewi, "Privacy: An Overview of Indonesia Statutes Governing Lawful Interception," Central European Journal of International and Security Studies 12, no. 4 (2018). See also Indonesia, "Naskah Akademis RUU Perlindungan Data Pribadi," (Jakarta: Badan Pembinaan Hukum Nasional, 2016), p. 192. The academic paper stated that the bill 'is a mandate from' (*merupakan amanat dari*) Article 28G(1) of the Constitution of Indonesia 1945.

with an Act.[23] In Decision 012-016-019, the Court linked the freedom and secrecy of correspondence in electronic communications to Act 39/1999 on Human Rights, but not to Article 28G(1).[24] The Court also emphasised that the wiretapping procedure must be regulated in a particular Act.[25]

The issue in Decision 5/PUU-VIII/2010 concerned a mandate from the EITA to the government to regulate the interception procedure further in a government regulation. The applicants considered the mandate to be unconstitutional because restrictions on constitutional rights have to be based on an Act, not a government regulation. The legislative, as the representative of the people, plays a role in the enactment of an Act.

Furthermore, the applicants stated that due to the development of automatic processing technology, the State has the responsibility to ensure the adequate protection of personal data. The responsibility arose because, according to the applicants, both the State and private entities that process personal data have the power to exploit personal data, and such exploitation threatens individuals' privacy.[26] In the decision, the Court explicitly established the link between privacy and the Constitution with regard to interception:[27]

"*Interception is essentially an infringement of rights of privacy that is against the Constitution of Indonesia 1945. The right to privacy is part of derogable human rights; restrictions toward the right, however, shall only be exercised based on [a particular] Act*."

The Court did not explicitly rule from which Article in the Constitution the privacy of electronic communication emanates. Neither did the Court explain the relationship between the right to privacy and the right to the protection of personal data. However, as an inference, the Court seemed to agree with the applicants in the three cases that it emanates from Article 28G(1).

Furthermore, in Decision 20/PUU-XIV/2016, the Constitutional Court stated:[28]

"*Interception is prohibited because [it] violates the constitutional rights of citizens particularly the privacy of every person to communicate as guaranteed in Article 28F Constitution of Indonesia 1945*.

However, in a plain reading, Article 28F does not substantially concern privacy. The Article emphasises the right to communicate and acquire information to develop oneself and social environment, and the right to seek, obtain, possess, store, process and disseminate information through all kinds of channels available. Still, from the Constitutional Court's decisions discussed above, it could be concluded sufficiently that the right to privacy as a constitutional right emanates from the Constitution of Indonesia 1945.

How about the right to personal data protection? The recognition of the right to

[23] The Constitutional Court of the Republic of Indonesia, "Decision 006/PUU-I/2003," pp. 103-04.

[24] The Constitutional Court of the Republic of Indonesia, "Decision 012-016-019/PUU-IV/2006", p. 275.

[25] *Ibid*., pp. 275-76.

[26] The Constitutional Court of the Republic of Indonesia, "Decision 5/PUU-VIII/2010," p. 28.

[27] *Ibid*., pp. 68-69, consideration [3.21]; [3.20]; and [3.24]. Constitutional Judge Suhartoyo reiterated para. [3.21] in his dissenting opinion in the Constitutional Court of the Republic of Indonesia, "Decision 20/PUU-XIV/2016," p. 102.

[28] The Constitutional Court of the Republic of Indonesia, "Decision 20/PUU-XIV/2016", p. 93, consideration [3.9].

the protection of personal data has emerged since the EITA's enactment. The EITA determines that personal data protection is a part of the right to privacy.[29] The Bill on Personal Data Protection also declares that personal data protection is a human right that is part of the protection of self (*diri pribadi*).[30] The Bill further states that the regulation related to the right to privacy upon personal data "is a manifestation of the recognition and protection toward human rights," particularly Article 28G(1) of the Constitution of Indonesia 1945.[31] In other words, the right to the protection of personal data is a derivative right that emanates from the Constitution of Indonesia 1945.

EU data protection law is a reference that the Indonesian government used to prepare the Bill on Personal Data Protection.[32] Thus, it is important to note here that under the EU data protection law, the rights to privacy and personal data "strive to protect ... the autonomy and human dignity of individuals."[33] The right to privacy emphasises "a general prohibition on interference".[34] On the other hand, the right to personal data protection underscores the protection of personal data "wherever personal data are processed" ... irrespective of the relationship and impact on privacy".[35] This understanding of the relationship between the two rights can be useful in establishing the Indonesian regime of personal data protection.

Since it has been regarded as a constitutional right, the right to personal data protection has applied in relationships between the government and Indonesian subjects and between corporations and Indonesian people. The recognition that the right to personal data protection is a constitutional right has implications in the Indonesian criminal procedure law. This constitutional recognition means that the right is to have constitutional conditions and safeguards that the criminal procedure law should incorporate. The recognition of personal data protection as a constitutional right also applies to all phases of criminal proceedings, including the pre-investigation (*penyelidikan*). This recognition mandates the establishment of the regulatory framework for data protection in the criminal justice system. Limitations of the rights are constitutionally possible according to Article 28J of the Constitution of Indonesia 1945. However, any limitation of constitutional rights is to be scrutinised and prescribed under strict due process of law in primary legislation, and not in secondary one. Furthermore, powers for law enforcement authorities to derogate from privacy are to be scrutinised and guarded by a checks-and-balances mechanism.

However, gaps exist between the recognition of the right to personal data protection and its implementation in the criminal procedure law. The gaps create uncertainties and ambiguities on how Indonesian law enforcement authorities should protect personal data in the law enforcement process, such as in cybercrime investigation. The following section explains the gaps and uncertainties.

---

[29] Explanatory Report Article 26(1) of the EITA.

[30] Consideration a, Data Protection Bill.

[31] Explanatory Report, I. General, paras 2-3, RUU Perlindungan Data Pribadi. (My translation of "*... pengaturan menyangkut hak privasi atas data pribadi merupakan manifestasi pengakuan dan perlindungan atas hak-hak dasar manusia*.")

[32] Depkominfo, "Naskah Akademis RUU tentang Informasi dan Transaksi Elektronik," (Jakarta: Depkominfo).

[33] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law (Luxembourg: Publications Office of the EU, 2018), p.19.

[34] *Ibid*.

[35] *Ibid*., 20.

B. Personal Data Protection in the Indonesian Criminal Procedure Law

The KUHAP and the EITA are the primary legislation used in cybercrime investigation. The KUHAP does not prescribe, at least explicitly, provisions on personal data protection. The EITA requires investigators 'to be mindful of' (*memperhatikan*) the protection of users' privacy, secrecy, continuity of public service, data integrity, and data entirety under the prevailing law.[36] However, the term 'to be mindful' signifies a weak obligation in protecting the right to personal data protection actively. More fundamentally, the provision does not reflect clear constitutional conditions and safeguards as a manifestation of the acknowledgement that the right emanates from the Indonesian Constitution.

Article 14 of the GR 71/2019 prescribes principles in processing personal data. The main principle is that personal data shall be collected limitedly, specifically, legally, and justly, with the knowledge and consent of the data subjects. Another principle is that the processing of personal data shall be carried out accurately, completely, and accountably. Furthermore, the processing shall also ensure the protection of personal data from, among other things, illegal access and unauthorised disclosure, alteration or deterioration. The Regulation of the MCIT 20/2016 stipulates the obligation and rights of both a controller and a data subject in the processing of personal data in an electronic system. However, the two secondary legislations do not explain how those provisions are applicable in the criminal justice areas (such as in pre-investigation and investigation).

It is expected that the Bill on Personal Data Protection will harmonise the existing legislation and create a comprehensive legal framework.[37] The Bill stipulates the principles that the GR 71/2019 prescribes. The Bill requires a controller to obtain the consent of data subjects before the controller collects their personal data. Unfortunately, it regulates the protection of personal data in the criminal justice areas superficially.[38] For example, it rules that serving the interest of justice is a valid reason for excluding the obligation to obtain data subjects' consent.[39] Even more, for the interest of justice, personal data protection prescribed in the Bill can be ruled out to enforce provisions prescribed in another Act.[40] However, the Bill does not provide further explanation of how law enforcement authorities will protect personal data for the interest of justice.

Establishing the general principles of personal data protection is one thing. Implementing them in the criminal justice areas is another. The government should have concrete direction in developing a coherent legal framework of personal data protection in these areas. In searching the direction, the government may start by confronting the principles in processing personal data with provisions and principles of the criminal procedure law. Hence, the government can have an accurate understanding of the limitations and uncertainties in using the prevailing criminal procedure law to protect personal data. Then, the government and law enforcement authorities can develop a coherent framework of personal data protection in the

[36] Article 43(2) of the EITA.

[37] Agus T. Haryanto, "Draft RUU Perlindungan Data Pribadi Dibahas Bulan Depan (Bill on Personal Data Protection will be Discussed Next Month)," https://inet.detik.com/law-and-policy/d-4426709/draft-ruu-perlindungan-data-pribadi-dibahas-bulan-depan, accessed 30 April 2019.

[38] Indonesia, "Naskah Akademis RUU Perlindungan Data Pribadi, Draft 2016." The Bill was downloaded from the website of the National Law Development Agency (BPHN).

[39] Article 23(4)c of the Bill on Personal Data Protection.

[40] Article 58(1) of the Bill on Personal Data Protection.

criminal justice areas.

IV. LIMITATIONS AND UNCERTAINTIES IN PROTECTING PERSONAL DATA UNDER THE INDONESIAN CRIMINAL PROCEDURE LAW

A. The General Principles of Search and Seizure

Search and seizure are the investigative powers that Indonesian investigators use most frequently to obtain evidentiary objects, include e-information. The KUHAP defines a search of a house and other closed premises (*tempat-tempat tertutup*),[41] and a suspect's body or clothing.[42] However, the definitions do not limit the scope of a search. According to Article 33(1) KUHAP, investigators have the authority to search any place where they may discover, locate or indicate the presence of a suspect. They may search for a place where they may discover any trace of a crime or where the crime was committed.[43] Furthermore, examining letters, books or other papers is a form of a search.[44] Investigators also have the authority to search virtual space, such as email accounts and computer systems.[45] In short, a search is an examination of any premises or matter to collect evidentiary objects and legal means of evidence, to find and arrest a suspect, or to ascertain facts and the constitutive elements of a crime.

Principally, a search is to be carried out in accordance with a warrant from the chief judge of a competent district court.[46] However, in *very* necessary and urgent circumstances, investigators may execute a search according to an order from their superintendent (urgent search).[47] The KUHAP determines conditions of 'very necessary and urgent circumstances.'[48] First, the suspect would immediately escape or re-commit the crime. Second, a person would immediately destroy or remove evidentiary objects. Third, the investigators could not obtain the warrant using reasonable means and promptly. After they have carried out an urgent search, the investigators must report it promptly to the chief judge of the competent district court to obtain his approval. In this respect, investigators' discretion plays a vital role in determining the need for an urgent search.[49] Being caught in the act is a practical situation where a third party[50] could assess the necessity of an urgent search equitably. However, other practical situations are more difficult for the party to assess equitably.

On the other hand, the essence of seizure is to expropriate or retain an object (*benda*), either moveable or immoveable, under the investigator's control for

[41] Article 1.17 of the KUHAP.

[42] Article 1.18 of the KUHAP jo. Article 37 of the KUHAP.

[43] Article 34(1) of the KUHAP.

[44] Article 34(2) of the KUHAP. See the Constitutional Court of the Republic of Indonesia, "Decision 21/PUU-XII/2014", p. 107, consideration [3.16].

[45] See Article 43(3) of the EITA. See also the District Court of Masohi, "Decision 45/Pid.B/2012/PN.MSH", p. 23; the District Court of Buol, "Decision 50/Pid.Sus/2015/PN Bul", p. 22; the District Court of Gorontalo, "Decision 188/Pid.Sus/2017/PN Gto"; the District Court of Ciamis, "Decision 267/Pid.Sus/2015/PN Cms", p. 20; the District Court of Gorontalo, "Decision 269/Pid.Sus/2016/PN Gto", p. 15.

[46] Article 33 of the KUHAP.

[47] Indonesia, *Peraturan Kapolri tentang Manajemen Penyidikan Tindak Pidana* (*Regulation of the National Police Chief on the Administration of Criminal Investigation*), Peraturan No. 14 Tahun 2012 (Regulation No. 14 Year 2012).

[48] Explanatory Report to Article 34 of the KUHAP.

[49] M. Yahya Harahap, Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan, (Jakarta: Sinar Grafika, 2016), p. 255.

[50] Such as a defendant or his legal counsel or a person who is subjected to an urgent search.

evidentiary purposes.[51] The principles in seizing electronic evidence are no different from those of physical evidence. All evidentiary objects that are relevant to a criminal case have to be put under a seizure and obtained lawfully. The seized objects are to have a direct or substantial connection (*hubungan langsung*) to the investigated crime.[52] Therefore, *a contrario*, a seizure of a person's property that is irrelevant (it has no correlation or insubstantial connection) to the case is an excessive seizure that could be regarded as unlawful. Nevertheless, in seizing e-information, investigators could not always determine at a glance which e-information that is relevant to the case they are investigating.

Principally, investigators can only seize objects according to a warrant from the chief judge of the competent district court. The exception to that rule is when they face a very necessary and urgent circumstance. In such circumstance, investigators may seize the objects first and then apply for approval from the judge. Although the KUHAP does not provide an explicit explanation concerning 'a very necessary and urgent circumstance,' its scope follows the legal construction of an urgent search.[53]

B. Limitations in Using the Search and Seizure Provisions in Protecting Personal Data

The conditions and safeguards in carrying out a search and seizure prescribed in the KUHAP, the EITA and the secondary legislation mentioned above are general ones. Thus, law enforcement authorities should apply them in as many concrete scenarios as possible to identify their limitations in dealing with voluminous data issues. The following practical questions may assist law enforcement authorities in examining the extent to which the existing provisions can be used to strike a balance between the right to personal data protection and the interests of law enforcement.

Investigators have the authority to search e-system and seize e-information. The GR 71/2019 stipulates that the collection of personal data must be specified and the data controller must collect the data justly. In this respect, how should investigators minimise the exposure of irrelevant personal data in a search or seizure? Next, data minimisation is a principle prescribed in the GR 71/2019 that law enforcement authorities have to take into consideration. Then, to what extent may investigators use the copy of voluminous data they seized in one case for another case? Are investigators authorised to deploy malware in pre-investigation phase to reveal suspects' identity and location or to collect evidence? If they are permitted to use malware, what are the conditions and safeguards, both *ex ante* and *ex post*? Furthermore, transparency is an essential principle in processing personal data. In this respect, must investigators submit to the competent court all copies of e-information that they copied from a user's device? Last but not least, how long must investigators retain e-information that is irrelevant to the investigated case?

The chief judges of competent district courts have the authority to issue search and seizure warrants. The judges also have the power to approve urgent searches or seizures. In this respect, to what extent do the chief judges have to examine the methods that investigators will execute in searching and seizing voluminous data

[51] Article 1.16 of the KUHAP.

[52] Article 39 of the KUHAP.

[53] Ratna N. Afiah, Barang Bukti dalam Proses Pidana (Jakarta: Sinar Grafika, 1989), p. 75; Harahap, Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan, p. 269.

before they issue a warrant? In a similar vein, do the chief judges have to examine the methods that investigators took in searching or seizing voluminous e-information before they approve an urgent search or seizure? Such an examination at the substantive level is instrumental as a check-and-balance mechanism in ensuring the protection of personal data.

Furthermore, the judicial panel determines the final status of the seized evidentiary objects. The panel may require that an email or web service account related to the criminal case be deprived (*rampas*) and deleted permanently (*musnahkan*),[54] deleted (*hapus*),[55] or suspended (*blokir*).[56] However, irrelevant e-information that a digital forensic examiner copied may not part of the evidentiary objects an investigator must *formally* seize and present to a court. Thus, the court may not know that the examiner has already copied voluminous irrelevant e-information. If a defendant raises this issue at trial, will the court order the prosecutor to return the residual information to the defendant? Will the seizure of voluminous irrelevant e-information serve as a sufficient legal basis for affected parties to file a complaint at pre-trial (*praperadilan*)? Does a suspect, a defendant or an affected party have the right to ask for unnecessary e-information to be deleted?

The judicial panel can also determine that a defendant's email accounts are returned to him.[57] Suppose at the investigation phase, the defendant informed the passwords of his accounts to the investigator who examined his case. The investigator used the passwords to copy evidence. Then, the investigator changed the passwords to prevent the defendant from obstructing or tempering evidence stored in the accounts. In this context, let's assume the following two scenarios. First, the investigator did not record the passwords and forgot them. Second, the investigator recorded the password. However, since the criminal proceedings took months, the service provider automatically inactivated the accounts. The defendant could not activate the account. In these two scenarios, the defendant cannot use his accounts. In that respect, what are effective remedies that the criminal procedure law can provide against those circumstances? Is the defendant entitled to such a right?

V. RE-CONSTRUING CONDITIONS AND SAFEGUARDS IN THE EXECUTION OF SEARCH AND SEIZURE

Indonesian law enforcement authorities may answer the practical questions mentioned above on a case-by-case basis. They may resolve issues of searching and seizing voluminous data differently and inconsistently, as a comprehensive personal data protection framework is yet to be established. The following paragraphs offer a reinterpretation of the existing conditions and safeguards in search and seizure. This reinterpretation revitalises the conditions and safeguards so that they are applicable in encountering the issues of voluminous data. First, the revitalisation is centred in the active role of the chief judges of competent district courts in enforcing law and justice. Second, the revitalisation incorporates specificity or particularity and proportionality

[54] The District Court of Pangkal Pinang, "Decision 267/Pid.B/2015/PN.Pgp." See also verdict 767/Pid.Sus/2014/PN Srg (Serang) in the District Court of Banten, "Decision 55/PID/2015/PT.BTN."

[55] The District Court of Yogyakarta, "Decision 257/Pid.Sus/2015/PN.Yyk."

[56] The District Court of Medan, "Decision 1960/Pid.Sus/2018/PN Mdn."

[57] The District Court of Surabaya, "Decision 847/Pid.B/2014/PN.SBY"; the District Court of Bogor, "Decision 222/Pid.Sus/2014/PN.Bgr," p. 31; the District Court of Amuntai, "Decision 276/Pid.Sus/2017/PN Amt."

explicitly into the conditions and safeguards in searching or seizing voluminous data. The incorporation of particularity and proportionality are instrumental in determining the reasonableness of searching and seizing voluminous data.

A. The active role of the chief judges of competent district courts

A warrant is a manifestation of the checks-and-balances mechanisms between the investigation and adjudication institutions. A warrant manifests the involvement of an impartial institution to ensure the protection of constitutional rights. The chief judges of competent district courts play an active role in safeguarding the right to personal data protection in searching and seizing voluminous data. The issuance of a warrant signifies the confidence of the chief judge of a competent district that the execution of a search and seizure is reasonable. Of equal importance, the investigator who executes the warrant has adequate methods to protect the affected persons' data. In a similar vein, the chief judges' approval for an urgent search and seizure signifies two things. First, the chief judges have concluded that the execution of those investigative powers was reasonable. Second, the investigator who executed the powers observed the criminal procedure law and protected the personal data of the affected persons. Thus, investigators should not regard the requirement to obtain a warrant or approval for as a mere formality. Neither should the chief judges of competent district courts view the responsibility to issue a warrant or an approval for search and seizure as an administrative matter. The chief judges should not regard that a search or a seizure as a mere responsibility of investigators. Furthermore, the responsibility of the investigators and chief judges to ascertain the material truth should not diminish the main function of a warrant or an approval for search or seizure.

Before the chief judges issue a warrant, they have the responsibility to examine the warrant application that investigators submit to the court. In a similar vein, before they issue an approval for an urgent search or seizure, the chief judges have the responsibility to examine the approval application they receive from investigators. Recognising the main function of the warrant and the approval, recognising that the chief judges' main obligation is to enforce law and justice, recognising that they hold the impartial authority to strike a balance between protecting constitutional rights and accommodating the interests of law enforcement, the chief judges should examine the application at the substantive level, and not at the administrative one.

B. Particularity and Proportionality in the Indonesian Criminal Procedure Law

The incorporation of specificity or particularity and proportionality into the Indonesian criminal procedure law is in harmony with principles of personal data protection in GR 71/2019 and Regulation of the MCIT 20/2016. Regarding a search, the specificity element can be found in Article 34 KUHAP. An investigator has to ascertain that a suspect lives at a certain house or apartment in which premises the investigator is about to search. An investigator has to determine that a criminal offence is committed in a specific location. The investigator has to ensure that they can find traces of the investigated crime in particular premises which they about to search. Regarding a seizure, Article 39 of the KUHAP contains the particularity element. Before the investigators can seize an object in a very necessary and urgent circumstance, they have to ascertain that an object has a direct and substantial connection to the investigated criminal offence.

The following paragraphs explain some implementations of the particularity element in the context of cybercrime investigation. On the one hand, investigators should describe in their warrant application the electronic systems they will search or the e-information they will seize unambiguously. They should not apply for a carte-blanche warrant for ascertaining the material truth. For example, they should describe clearly a suspect's email account that they have to search (e.g. johndoe@yahoo.com) and the files stored therein that they intend to seize (e.g. communications between the suspect and the user of johnsmith@yahoo.com). In cases where investigators obtain a search and seizure warrant, they cannot search the suspect's social media accounts or seize USB sticks that they can find in the suspect's residence, except in a very urgent and necessary condition.

On the other hand, the chief judges of competent district courts should not issue a warrant where the application describes an e-system that investigators will search or e-information they will seize over-broadly or ambiguously. The judges should not issue a warrant where the application describes the rationale for executing the search or seizure insufficiently. A mere statement that an email account has a direct and substantial connection to the investigated crime without a clear description of the connection between the account and the crime does not meet the specificity requirement.

Proportionality is another safeguard in searching or seizing personal data. This safeguard deals with the methods that investigators will carry out in searching or seizing voluminous data. Every technique has limitations in both protecting the rights of a data subject and preserving the interests of law enforcement. Investigators should assess and determine the most appropriate method that can minimise the exposure of personal data and maximise the interests of law enforcement. The nature of a criminal offence (serious or misdemeanour) is a relevant aspect that investigators should take into consideration in striking a balance between the two competing interests. Furthermore, maintaining transparency about the methods investigators will use in searching or seizing voluminous data strengthens the right to personal data protection.

Before issuing a warrant, the chief judges of competent district courts should ascertain that the method that investigators will use is proportional to the investigation's objective. Investigators can use various methods in searching and seizing e-evidence. For example, investigators can order suspects to give their email account password to them. Then, the investigators can use the password to search emails therein and select some of them as evidence. Using the password in front of the suspects signifies transparency, whereas utilising it without the suspects' knowledge impairs transparency. Also, investigators can use malware to search and seize e-evidence. Malware can serve as both a method and a tool to intercept. Investigators can inject the malware into suspects' device to obtain control over the device. Then, they can use the malware to open files stored therein. They can also record activities that the suspects do with the device and then transfer the record to the investigators' computer. The use of malware to reveal suspects' identity and location in investigating an online defamation case may not be proportional. Deploying malware to investigate the dissemination of child pornography materials can be proportional where investigators have tried other methods without success. These examples suggest that the ascertainment regarding proportionality requires an examination at the substantive level. The chief judges should strike a balance between protecting constitutional rights and ascertaining the material truth. If they

cannot find any or sufficient description about the method, the judges may order the investigators to provide it or reject their application.

In a similar vein, investigators should not misuse urgent search and seizure provisions. After executing an urgent search and seizure, investigators have to apply for approval from the competent district court. The judge has an active role in ensuring that the affected persons' constitutional rights are guarded. The role as such aligns with the judiciary's responsibility to enforce law and justice. Thus, the judge should issue an approval decision after examining the execution of an urgent search and seizure at a substantive level. The judge should assess whether the executed search and seizure meet the particularity and proportionality safeguards.

It is important to be reiterated here that the KUHAP does not prescribe particularity and proportionality in the execution of search and seizure explicitly. However, they are conditions and safeguards which are aligned with the Constitution of Indonesia 1945. Their incorporation into the Indonesian law and practice can strengthen the protection of personal data in searching or seizing voluminous data. Particularity and proportionality serve as means of enforcing law and justice. The active role of the chief judges of competent district courts in examining the reasonableness of searching or seizing voluminous data at the substantive level is pivotal in ensuring that affected persons (victims, witnesses, suspects, and defendants) can have their constitutional rights protected.

C. Particularity and Proportionality in Foreign Legal Systems

Particularity and proportionality are conditions and safeguards in searching e-system and seizing e-information that many states have in their criminal procedure law. An impartial institution determines the sufficiency of these conditions and safeguards in the execution of investigative powers, such as search and seizure. In the United States (US), probable cause and particularity are two fundamental elements of the Fourth Amendment. They are constitutional conditions and safeguards, and they determine the reasonableness or constitutionality of a warrant. Probable cause means a reasonable judgement that a search or seizure is necessary to discover more facts, evidence or circumstances regarding the commission of a crime and the perpetrator. On the other hand, particularity is a clear description of objects (or subjects in arrest) a warrant authorises in a search or seizure.[58] Particularity determines the scope of a warrant, whereas the warrant itself must emanate from the probable cause.[59] Therefore, an over-broad warrant means insufficient or no probable cause. It may also mean that a warrant has no particularity regarding the subject or the object of search or seizure.[60]

The European Union, consisting of 28 member states, established data protection law that it claims as "the toughest privacy and security law in the world."[61] It enacted Directive 2016/680 on personal data protection in criminal matters stipulates the

[58] U.S. v. Hill, 459 F.3d 966, 73, 973 (9th Cir. 2006)

[59] *Ibid*.

[60] U.S. v. George, 975 F.2d 72, 78 (2d Cir. 1992). Under the plain view doctrine, an officer is authorised 'to seize evidence without a warrant when it is immediately apparent that the object is connected with criminal activity ... and where such search and seizure do not involve an invasion of privacy.'

[61] GDPR.EU, "What is GDPR, the EU's new data protection law?," https://gdpr.eu/what-is-gdpr/, accessed 19 November 2019.

principles relating to the processing of personal data in the EU.[62] These principles are prescribed to assure the protection of personal data as a fundamental right under the Charter of Fundamental Rights of the EU. EU Member States' competent authorities, acting as the controllers of personal data, must process personal data lawfully and fairly. They must collect the data for specified, explicit and legitimate purposes. The controllers are prohibited from processing personal data in a manner that is incompatible with those purposes. They have to process personal data adequately and not excessively in relation to the purposes for which they are processed. The controllers must also process only relevant personal data and ensure that they are accurate. They are obliged to take every reasonable step to ensure that personal data that are inaccurate, in relation to the purposes for which they are processed, are erased or rectified without delay. Moreover, they must implement appropriate technical and organisational measures to protect personal data from, among other things, unlawful processing, accidental loss, destruction or damage.

The US and EU member states are parties to the Council of Europe's Budapest Convention. This convention has been regarded as 'the only multilateral treaty to address the problems of computer-related crime and electronic evidence gathering.'[63] Several conditions and safeguards are discussed explicitly in the Explanatory Report. Specificity or particularity is a fundamental element of the conditions and safeguards in the Convention. For example, law enforcement authorities are to specify the e-evidence[64] that they are ordering a person to preserve or the communications they intercept.[65] The authorities are prohibited from intercepting communications to discover criminal activities other than those they are authorised to intercept.[66] The specificity element signifies the obligation of law enforcement authorities to protect personal data and the privacy of internet users. Proportionality is another safeguard that a party should incorporate in its national law. For the European states, proportionality refers to power or procedure that should correspond to the nature and circumstances of the offence.[67]

The fact that many states incorporate particularity and proportionality into their criminal procedure law is an important aspect that Indonesia should take into consideration in strengthening cooperation with the US or EU member states on the transfer of personal data. They are conditions and safeguards that those states establish to protect their citizens' right to information privacy or personal data protection. Presumably, the US or EU member states will hesitate to provide their citizens' personal data to Indonesian law enforcement authorities if the level of protection of personal data that Indonesian law and practice have is not equal with those of the states. In other words, if Indonesia has the interest to strengthen the cooperation with the US or EU member states on the transfer of personal data for law enforcement purposes, it should have a compatible regime of personal data protection with those states.

[62] Directive 2016/680 on Personal Data Protection in Criminal Matters.

[63] Richard G. Lugar, "The Report from the Committee on Foreign Relations on Council of Europe Convention on Cybercrime," (Washington: US Senate Committee on Foreign Relations, 2003).

[64] Article 16 and 17 of the Budapest Convention.

[65] Article 20 and 21 of the Budapest Convention.

[66] Explanatory Report to the Budapest Convention, para. 219.

[67] Explanatory Report to the Convention on Cybercrime (ETS 185), para. 146.

VI. CHANGING LEGAL CULTURE IN ENFORCING LAW

The concept of the right to personal data protection as part of constitutional rights may impede the existing practice of collecting, using, and retaining personal data for criminal justice purposes. Law enforcement authorities may find more restrictions and obligations in the processing of personal data that emanate from the implementation of the concept. Incorporating the concept into the Indonesian criminal procedure law requires a paradigm shift. That shift is from pursuing the material truth to enforcing law and justice. That shift requires law enforcement authorities to leave their comfort zones and enter into a new environment in which they have to carry more responsibility to ensure the protection of personal data.

Thus, if there is any complacency about the existing practice that does not sit well with the concept, then such complacency should stop. The impediment and complacency should not be used as a justification for pursuing a lower standard of personal data protection than what Indonesian citizens (regardless their status as victims, witnesses, suspects, or defendants) can possibly enjoy according to the Constitution. Protecting constitutional rights must be above practical difficulties that arise as a result of the incorporation of personal data protection concept into the criminal procedure law. In the end, incorporating the enforcement of law justice as the constitutional objective of the Indonesian criminal justice system and the right to personal data protection as a constitutional right into the Indonesian criminal procedure law will change the law substantially. It will be a reform that should not be regarded as a sprint but as a marathon. It requires strong political will, thorough consideration and perseverance.

VII. CONCLUSION

There should be a coherent regime regarding the protection of personal data in criminal justice areas in Indonesia. The government could either incorporate the matter into the Bill on Personal Data Protection or enact another Act that addresses specifically the implementation of the right to personal data in those areas. In the absence of the regime, this article answered the question of how Indonesian law enforcement authorities may interpret the prevailing law to establish a coherent legal framework to protect personal data in searching or seizing voluminous data. This article has re-construed the prevailing law to develop a coherent interpretation of why Indonesian law enforcement authorities should protect personal data and how they may do it in searching and seizing voluminous data.

First, it is proposed that the constitutional objective of the Indonesian inquisitorial system is to enforce law and justice. In this respect, Indonesian law enforcement institutions have the same objective: to enforce law and justice. Ascertaining the material truth is to serve the constitutional objective.

Second, the Indonesian criminal justice system has gradually recognised the protection of privacy and personal data as constitutional rights. However, such recognition requires a concrete implementation in the Indonesian criminal procedure law. The Bill of Personal Data Protection does not provide a clear legal framework on how law enforcement authorities should protect personal data in executing their investigative powers. The article has unpacked problems in implementing the prevailing law to protect personal data in searching and seizing voluminous data.

Third, this article has re-construed the existing conditions and safeguards of search

and seizure to make them applicable in protecting personal data. The reinterpretation could serve as a guideline for law enforcement authorities in encountering the absence of the Indonesian regime of personal data protection. The article suggests that the chief judges of competent district courts should examine the reasonableness of search and seizure of voluminous data at the substantial level. They should do so before they issue a warrant or an approval for search and seizure. The chief judges serve as an impartial authority that strikes a balance between protecting personal data and accommodating the interests of law enforcement. The Indonesian criminal justice system should incorporate particularity and proportionality explicitly to ensure the protection of personal data and transparency in protecting the constitutional right. Particularity and proportionality are conditions and safeguards that the judges should examine at the substantive level before they issue a warrant or an approval for search and seizure. Inserting these elements into the Indonesian criminal procedure law means changing legal culture and paradigm. It requires persistence from not only lawmakers but also law enforcement authorities on reforming the law. The responsibility of enforcing law and justice and the obligation to protect constitutional rights could serve as the source for having persistence in developing the legal culture.

Finally, the adherence of the Indonesian criminal justice system to the rule of law principle is essential for Indonesia to demonstrate in strengthening cooperation in combating cybercrime with other states. Indonesia should demonstrate that the Indonesian criminal justice system provides sufficient powers for law enforcement authorities to enforce law and justice. Its criminal justice system should demonstrate the adequacy of conditions and safeguards as well as checks-and-balances mechanisms in protecting Indonesian subjects' constitutional rights in every law enforcement phase.

BIBLIOGRAPHY

Legal Documents

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28 January 1981. European Treaty Series, No. 108.

Convention on Cybercrime. Budapest, 23 November 2001. European Treaty Series, No. 185.

Constitutional Court of the Republic of Indonesia. "Decision 006/PUU-I/2003."

---. "Decision 012-016-019/PUU-IV/2006."

---. "Decision 5/PUU-VIII/2010."

---. "Decision 65/PUU-VIII/2010."

---. "Decision 34/PUU-XI/2013."

---." Decision 21/PUU-XII/2014."

---. "Decision 20/PUU-XIV/2016."

District Court of Masohi. "Decision 45/Pid.B/2012/PN.MSH."

District Court of Bogor. "Decision 222/Pid.Sus/2014/PN.Bgr."

District Court of Surabaya. "Decision 847/Pid.B/2014/PN.SBY."

District Court of Banten. "Decision 55/PID/2015/PT.BTN."

District Court of Ciamis. "Decision 267/Pid.Sus/2015/PN Cms."

District Court of Yogyakarta. "Decision 257/Pid.Sus/2015/PN.Yyk."

District Court of Pangkal Pinang. "Decision 267/Pid.B/2015/PN.Pgp."

District Court of Banda Aceh. "Decision 03/Pid.B/2015/PN."

District Court of Buol. "Decision 50/Pid.Sus/2015/PN Bul."

District Court of Gorontalo. "Decision 269/Pid.Sus/2016/PN Gto."

District Court of Amuntai. "Decision 276/Pid.Sus/2017/PN Amt."

District Court of Gorontalo. "Decision 188/Pid.Sus/2017/PN Gto."

District Court of Medan. "Decision 1960/Pid.Sus/2018/PN Mdn."

EU. "Directive 2016/680 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and Repealing Council Framework Decision 2008/977/JHA." 2016.

Indonesia, *Undang-Undang tentang Hukum Acara Pidana* (*Law regarding Criminal Procedure Law*), UU No. 8 Tahun 1981, LN No. 76 Tahun 1981 (Law Number 8 Year 1981, SG No. 1981).

---.*Undang-Undang tentang Perbankan* (*Law regarding Banking*), UU No. 7 Tahun 1992, LN. No. 31 Tahun 1992 (Law Number 7 Year 1992, SG. No. 31 Year 1992).

---. *Undang-Undang tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan* (*Law regarding the Amendment of Law regarding Banking*), UU No. 10 Tahun 1998, LN. No. 182 Tahun 1998 (Law Number 10 Year 1998, SG. No. 182 Year 1998.

---. *Undang-Undang tentang Informasi dan Transaksi Elektronik* (*Law regarding Electronic Information and Transaction*), UU No. 11 Tahun 2008, LN. No. 58 Tahun 2008 (Law Number 11 Year 2008, SG. No. 58 Year 2008)

---. *Undang-Undang tentang Kesehatan* (*Law regarding Health*), UU No. 36 Tahun 2009, LN. No. 144 Tahun 2009 (Law Number 36 Year 2009, SG. No. 144 Year 2009).

---. *Undang-undang tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008*

tentang Informasi dan Transaksi Elektronik (*Law regarding the Amendment of Law Number 11 Year 2008 regarding Electronic Information and Transaction*), UU No. 19 Tahun 2016, LN. No. 251 Tahun 2016 (Law Number 19 Year 2016, SG No. 251 Year 2008).

---. *Rancangan Undang-Undang tentang Perlindungan Data Pribadi* (*Data Protection Bill*), Draft 29 April 2019.

---. *Keputusan Menteri Kehakiman tentang Tambahan Pedoman Pelaksanaan Kitab Undang-undang Hukum Acara Pidana* (*the Decree of Ministry of Justice regarding Additional Guidelines for the Implementation of the Criminal Procedure Law*), Keputusan No. M.14-PW.07.03 Tahun 1983 (Decree No. M.14-PW.07.03 Year 1983).

---. *Peraturan Kapolri tentang Manajemen Penyidikan Tindak Pidana* (*Regulation of the National Police Chief on the Administration of Criminal Investigation*), Peraturan No. 14 Tahun 2012 (Regulation No. 14 Year 2012)

U.S. v. Hill, 459 F.3d 966, 73, 973 (9th Cir. 2006)

U.S. v. George, 975 F.2d 72, 78 (2d Cir. 1992).

Publications

Afiah, Ratna N. Barang Bukti dalam Proses Pidana. Jakarta: Sinar Grafika, 1989.

Asshiddiqie, Jimly. Menuju Negara Hukum yang Demokratis. Jakarta: Bhuana Ilmu Populer, 2009.

BPHN. "Naskah Akademis RUU Perlindungan Data Pribadi, Draft 2016." Jakarta: Badan Pembinaan Hukum Nasional, 2016.

Depkominfo. "Naskah Akademis RUU tentang Informasi dan Transaksi Elektronik." Jakarta: Depkominfo.

Dewi, Sinta. "Privacy: An Overview of Indonesia Statutes Governing Lawful Interception." Central European Journal of International and Security Studies 12, no. 4 (2018): 586-97.

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

Grande, Elisabetta. "Rumba Justice and the Spanish Jury Trial," in Comparative Criminal Procedure, ed. Jacqueline E. Ross and Stephen C. Thaman. Massachusetts: Edward Elgar Publishing Limited, 2018.

Harahap, M. Yahya. Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan. Jakarta: Sinar Grafika, 2016.

Lugar, Richard G. "The Report from the Committee on Foreign Relations on the Council of Europe Convention on Cybercrime." Washington: US Senate Committee on Foreign Relations, 2003.

Mahkamah Konstitusi. Buku I: Latar Belakang, Proses, dan Hasil Pembahasan UUD 1945. Naskah Komprehensif Perubahan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945: Latar Belakang, Proses, dan Hasil Pembahasan 1999-2002. Revised ed. Jakarta: Sekretariat Jenderal dan Kepaniteraan Mahkamah Konstitusi, 2010.

Purbopranoto, Kuntjoro. Hak-Hak Asasi Manusia dan Pancasila. 4th ed. Jakarta: Pradnya Paramita, 1969.

Rosadi, Sinta D. "Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia." Brawijaya Law Journal 5, no. 1 (2018): 143-57.

Sitompul, Josua. "Perlindungan Privasi dan Data Pribadi: Suatu Telaahan Awal." Buletin Hukum Perbankan dan Kebanksentralan, 2013, 71-94.

---. "Indonesian Cybercrime Verdicts Collected 2016-2018," https://doi.org/10.17026/dans-zrh-cfub.

Websites

Dignan, Larry, "Top Cloud Providers 2018: How AWS, Microsoft, Google Cloud Platform, IBM Cloud, Oracle, Alibaba Stack Up." https://www.zdnet.com/article/cloud-providers-ranking-2018-how-aws-microsoft-google-cloud-platform-ibm-cloud-oracle-alibaba-stack/. Accessed 26 May 2018.

GDPR.EU, "What is GDPR, the EU's new data protection law?," https://gdpr.eu/what-is-gdpr/. Accessed 19 November 2019.

Haryanto, Agus T., "Draft RUU Perlindungan Data Pribadi Dibahas Bulan Depan." https://inet.detik.com/law-and-policy/d-4426709/draft-ruu-perlindungan-data-pribadi-dibahas-bulan-depan. Accessed 30 April 2019.

Kemp, Simon, "Digital in 2018: World's Internet Users Pass the 4 Billion Mark." https://wearesocial.com/blog/2018/01/global-digital-report-2018. Accessed 25 May 2018.