# Personal Data Protection According to the Implemented Law in Indonesia and Japan

**Ermania Widjajanti, Andi Widiatno Hummerson, Vience Ratna Multiwijaya, Dwi Alfianto**
andi.widiatno@trisakti.ac.id

Faculty of Law, Universitas Trisakti, Indonesia

***Article Info***
*Received:*
*Revised:*
*Accepted:*

***Keywords:***
*Cyber Law; Personal Data Protection; Comparative Law*

***Abstract***
*The rapid development of technology creates various new things that can make human life easier, one of which is the cyber world which involves the internet. The presence of the cyber world brings many benefits to human life, with cyber, humans can do various things without being limited by distance and time. However, apart from bringing many positive things, the presence of the cyber world certainly creates new opportunities for crime, one of the threats in the cyber world is personal data. Indonesia and Japan, two countries that have significant economic and technological development in the Asian region, are not immune from the threat of personal data theft. Although both have different legal and cultural frameworks, both strive to protect the personal data of their citizens from increasingly complex cyber threats. In this way, a comparison will be made regarding the crime of personal data theft between Indonesia and Japan starting from the cultural history of respecting personal data in each country, the birth of regulations in each country, the criminal law system in each country, and also the regulations governing and has criminal sanctions in each country. The methodology used in this writing is a normative research. It is concluded that theft of personal data poses a significant challenge in the digital era, causing identity fraud, financial loss, and privacy violations. Indonesia and Japan, both Asian nations, have varying legal frameworks but both strive to protect citizens' data from cyber threats. Indonesia's regulations, passed in 2008, cover information and electronic transactions, intellectual property rights, and protection. Japan, on the other hand, has been addressing data protection since 2000, with regulations like APPI, My Number Act, and Act on Prohibition of Unauthorized Computer Access.*

## I. Introduction

Comparative Law is a legal discipline that aims to find similarities and differences and also discover close relationships between various legal systems. Comparative law can be useful in terms of improving the quality and practical development of legal knowledge in the legislative and judicial fields and can also maintain legal harmonization between countries.

The rapid development of technology creates various new things that can make human life easier, one of which is the cyber world which involves the internet. The presence of the cyber world brings many benefits to human life, with cyber, humans can do various things without being limited by distance and time. However, apart from bringing many positive things, the presence of the cyber world certainly creates new opportunities for crime, one of the threats in the cyber world is personal data.

Theft of personal data has become one of the main challenges in today's increasingly advanced digital era. Stolen or misused personal data can result in serious consequences for individuals, including identity fraud, financial loss, and detrimental privacy violations. Therefore, protecting personal data is very important in a society that relies on information technology.

Indonesia and Japan, two countries that have significant economic and technological development in the Asian region, are not immune from the threat of personal data theft. Although both have different legal and cultural frameworks, both strive to protect the personal data of their citizens from increasingly complex cyber threats. In this way, a comparison will be made regarding the crime of personal data theft between Indonesia and Japan starting from the cultural history of respecting personal data in each country, the birth of regulations in each country, the criminal law system in each country, and also the regulations governing and has criminal sanctions in each country. Therefore, in this writing, discussion will be made about the comparison of personal data theft according to the criminal law in Indonesia and Japan.

## 2. Research Method

The legal research method used by the author is normative juridical research, namely research that uses law as a basis for study which is based on principles and doctrines. (Nurhayati et al. 2021) This is because the author in carrying out the analysis uses a contextual approach and a regulatory approach - invitation.

In relation to data use, the author uses secondary data as the main data consisting of primary legal materials (Civil Code, ITE Law) and secondary legal materials (law books and legal journals). This data was obtained by collecting both what was found through library research (library study) and digital searches using the internet.

## 3. Results and Discussion

### Cultural History of Respecting Personal Data in Indonesia

Traditionally, Indonesia has a culture that respects individual privacy and honor. The norms present in society teach to respect other people's privacy and keep personal information confidential. Concepts such as "Disgrace" (bringing shame or shame) and "Sopan Santun" (ethics and manners) are an integral part of Indonesian society, which emphasizes the importance of maintaining privacy and respecting personal boundaries.

Apart from the traditional culture of Indonesian society, technological developments and globalization also influence people's views regarding personal data. Developments in information and communication technology, as well as the influence of globalization, play an important role in changing the way Indonesian people understand and manage personal data. The spread of the internet and social media, for example, has brought new challenges in managing privacy and protecting personal data. The growth of the internet and social media has changed the way people interact and share personal information, creating a need for stronger personal data protection.

### Cases of Personal Data Theft in Indonesia

Along with the development of information and communication technology, of course, there is also the risk of crimes against personal data, whether it is leakage of personal data, theft of personal data, disclosure of personal data, use of personal data that does not belong to them, or falsifying personal data.

Personal data leaks have occurred several times in Indonesia, starting with the Bank Indonesia data leak in 2022 where the data was stolen by the Conti ransomware group, as much as 228 GB of data from the Indonesian bank database was stolen, including customer and transaction information.

Apart from that, a KPU data leak also occurred in 2022. Bjorka, the hacker who hacked this data, admitted that 105 million NIK, family card, full name, residence and gender data were sold under the file name "Indonesian Citizenship Database

From KPU 105M".

Apart from cases like those above, there are also widespread cases of theft of personal data for misuse in online lending services, one of the cases is the Berlian Bestari case which was decided by the Bantul district court in 2023 with decision number 270/Pid.Sus/2023/Pn Btl. Berlian Bestari, a 34 year old woman, one day found an ID card with the identity of Hanni Aulia Larassakti, who was her co-worker. Before returning the ID card, it turned out that Berlian Bestari had already taken a photo of the ID card. Until finally Berlian Bestari used the KTP identity to create a Shopee paylater account (an online cash loan service). When creating the account, Berlian Bestari also asked for Hanni Aulia's account number on the pretext of borrowing an account because her husband wanted to send money, even though the account number was needed. to match personal data as a condition for disbursing online loan money. Until finally one day Hanni Aulia wanted to apply for a loan from the bank as business capital, but after BI Checking the loan application could not be processed because it turned out there was a bad loan in Hanni Aulia's name, on this basis Hanni Aulia reported this incident. After an examination, Defendant Berlian Bestari was proven to fulfill the elements of Article 67 paragraph (3) of Law Number 27 of 2022 concerning Personal Data Protection which states "Every person who deliberately and unlawfully uses Personal Data that does not belong to him as intended in Article 65 paragraph ( 3) be sentenced to a maximum imprisonment of 5 (five) years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah)."

**The Birth of the Personal Data Protection Regulation in Indonesia**

Due to the rapid development of information and communication technology, there was also an urgency to establish laws and regulations that regulate this matter, so in 2008 Indonesia passed Law Number 11 of 2008 concerning Information and Electronic Transactions which provides a legal basis for protection. personal data within the scope of electronic transactions, although this regulation does not regulate personal data in depth. Then in 2012 Indonesia issued Government Regulation (PP) Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions. After that, in 2016 Law Number 19 of 2016 was passed concerning amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. Even though there is already a law regarding information and electronic transactions, this regulation does not specifically discuss the protection of personal data, therefore in 2019 Government Regulation Number 71 of 2019 concerning Personal Data Protection was passed, this government regulation further regulates the protection of personal data in Indonesia, this government regulation is also the basis for the establishment of the Personal Data Protection Supervisory Agency which was established in 2020 as the institution responsible for supervising

and enforcing personal data protection in Indonesia. BPDP plays an important role in providing guidance, supervision and law enforcement regarding personal data protection.

Until 2022, Law Number 27 of 2022 concerning Personal Data Protection was finally born, which specifically and specifically regulates the protection of personal data starting from types of personal data, rights of personal data subjects, processing of personal data, obligations of personal data controllers and personal data processors. , transfer of personal data, prohibitions on the use of personal data, and also criminal sanctions.

**Criminal Law System in Indonesia**

Indonesia has 2 (two) criminal law systems, namely criminal law originating from western countries, specifically from the Netherlands, which is known as the Criminal Code (KUHP) and customary criminal law. Both are laws that go hand in hand. However, customary criminal law is not contained in standard regulations, either in the Criminal Code or other specially formed statutory regulations. So that in its implementation, customary criminal law does not have legal certainty and protection. Western criminal law (KUHP) and customary criminal law have several fundamental differences, both material and formal.

**Regulations that regulate and have criminal sanctions**

a. Law Number 11 of 2008 concerning Information and Electronic Transactions

   This law is the first regulation that regulates information and electronic transactions, passed on April 21 2008. This law regulates information and electronic transactions starting from information, documents and electronic signatures, electronic system operators, domain names, intellectual property rights, and protection of personal data, prohibited acts, and also criminal sanctions. However, this regulation does not regulate personal data protection in depth, personal data protection is only contained in article 26 which reads:

   (1) Unless otherwise determined by statutory regulations, the use of any information via electronic media that concerns a person's personal data must be carried out with the consent of the person concerned.
   (2) Any person whose rights as intended in paragraph (1) have been violated may file a lawsuit for losses incurred based on this Law.

   This regulation only regulates that the use of information relating to personal data must be carried out with the consent of the person concerned and if it is

violated, they can file a lawsuit for damages.

b. Law Number 27 of 2022 concerning Personal Data Protection

Passed on October 17 2022, this law is the first law to regulate personal data protection in depth. This law specifically regulates personal data protection starting from types of personal data, rights of personal data subjects, processing of personal data, obligations of personal data controllers and personal data processors, transfer of personal data, prohibitions on the use of personal data, and also criminal sanctions.

Prohibited actions relating to personal data are regulated in Chapter 13 Articles 65 and 66

Article 65:

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

Article 66

"Every person is prohibited from creating false Personal Data or falsifying personal data with the intention of benefiting themselves or others which could result in harm to others. Then criminal sanctions for prohibited acts are regulated in Chapter 14 articles 67 and 68."

Article 67

"(1) Any person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or another person which may result in loss to the Personal Data Subject as intended in Article 65 paragraph (1) shall be punished with a maximum imprisonment 5 (five) years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah).
(2) Every person who intentionally and unlawfully discloses Personal Data that does not belong to him as intended in Article 65 paragraph (2) shall be punished by a maximum imprisonment of 4 (four) years and/or a maximum

fine of Rp. 4,000,000,000, 00 (four billion rupiah).
(3) Every person who deliberately and unlawfully uses Personal Data that does not belong to him as intended in Article 65 paragraph (3) shall be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000, 00 (five billion rupiah)."

Article 68

"(1) Any person who deliberately creates false Personal Data or falsifies Personal Data with the intention of benefiting himself or another person which may result in harm to other people as intended in Article 66 shall be punished by imprisonment for a maximum of 6 (six) years and /or a maximum fine of IDR 6,000,000,000.00 (six billion rupiah)."

**Criminal Concerning Personal Data Theft In Japan**

Japan has had personal data privacy protection regulations since 2000. *The Data Protection Act* is a legal regulation adopted by the Japanese Federal Government. The formulation of legal rules related to the protection of privacy and personal rights was initiated by *Keidanren*, namely *the representative body* which specifically regulates industrial and trade issues in Japan. Regulation of personal data as a form of protection for the Japanese government in the era of trade competition in the European Union, *the Data Protection Act was born*. The principles of personal data protection in *the Data Protection Act* are that personal data is confidential, the owner of the registered personal data knows with certainty the purpose of using his personal data by any party, there is agreement in the form of a privacy policy as a form of data use that is not in accordance with the agreement, the owner of the personal data has the right to make changes or corrections to personal data, and if there is a violation of the use of personal data, then there is a need for reinstatement or compensation resulting from violations that occur at a later date.

The Personal Information Protection Act ("APPI") regulates privacy protection issues in Japan and the Personal Information Protection Commission ("PPC"), a central agency acts as the government's watchdog organization on privacy protection issues.

The APPI was originally passed in 2003 but was amended and the amendments entered into force on 30 May 2017. On 5 June 2020, the Japanese Diet approved a draft law to further amend the APPI ("APPI Amendment"). The APPI amendments came into force on April 1, 2022. In addition, there is a separate data protection law for the public sector. However, the data protection law for the public sector has been integrated into APPI and will come into force on 1 April 2022 (the

data protection law for local governments will come into force after 1 April 2023).

Regulations in Japan relating to the protection of personal data include the following:

***a. The Act on the Protection of Personal Information (APPI)***

*APPI* is a federal personal information protection law that regulates the handling of personal information by individuals and organizations, including government agencies, businesses, and non-profit organizations. The law is overseen by the Personal Information Protection Commission (PPC), an independent administrative body established in 2005, after APPI had been in effect for two years.

*APPI* requires organizations that wish to collect personal information to obtain consent from individuals before collecting, using or sharing it, but only in certain cases, such as if the information is sensitive or will be transferred to a third party or outside Japan. More in line with US law, in most cases APPI does not require consent for the collection or use of personal information that is not sensitive or meets other criteria.

The law has several requirements regarding security measures that must be taken to protect all personal information that has been collected. But overall, the law is less rigid regarding things like the specific actions required in the event of a data breach compared to many other laws. APPI's recent changes change that, and it's likely the requirements will continue to evolve.

***b. Personal Information Protection Commission (PPC)***

The Personal Information Protection Commission (*個人情報保護委員会, Kojin jōhō hogo iinkai, PPC* ) is a Japanese government commission tasked with protecting personal information. This Commission was established on 1 January 2016 to replace the Special Personal Information Protection Commission. The commission consists of eight commissioners and a chairman appointed by the Prime Minister with the approval of the National Diet. The number of commission members increased from four to eight in February 2016.

***c. My Number Act***

The Japanese government enacted the My Number Law (in Japanese and English), which came into effect in January 2016. This law establishes a unique 12-digit number, called My Number, or Social Benefits and Tax Number, or Individual Number, for every resident of Japan, whether Japanese or foreign. Giving everyone one number for all purposes (such as a US Social Security number) is designed to simplify and make more efficient taxation and application of social benefits such as national pensions, health insurance, and unemployment.

The Personal Information Protection Commission (PPC), which acts as a centralized data protection authority, was established under the Personal Information Protection Act (Japan and the United Kingdom). In PPC's role in

overseeing and monitoring compliance with the My Number Act, PPC has published the My Number Guidelines (Japanese) to ensure that organizations properly handle and protect personal data, including *My Number data* , as required by law .

d. ***Act on Prohibition of Unauthorized Computer Access (UCAL)***
The purpose of this Law as stated in article 1 of this Law is to prevent computer-related crimes committed via telecommunications channels and maintain order related to telecommunications as realized through the access control feature by prohibiting unauthorized computer access and establishing penalties for this as well as assistance measures. that the prefectural public safety commission must take to prevent the recurrence of similar actions, thereby contributing to the development of an advanced information and telecommunications society.

e. ***Japan Penal Code***
This law applies to anyone who commits a crime in Japanese territory

f. ***Unfair Competition Prevent Arc***
The purpose of this Law as stated in article 1 of this Law is to provide measures to prevent unfair competition and to compensate for losses or damage caused by unfair competition, to ensure fair competition between companies, and the implementation of which of international agreements related to it, thereby contributing to the healthy development of the national economy.

g. ***Telecommunication Business Act (The "TBA")***

h. ***Basic Act on Cybersecurity (The "BAC")***

i. ***the Japanese Foreign Exchange and Foreign Trade Act (the "FEFTA")***

**Sanctions Against Cybercrime According To Regulations / Laws In Japan**

a. ***Hacking***
Hacking is Unauthorized Access under UCAL, punishable by imprisonment of up to three years or a fine of up to JPY 1 million. If hacking is done through Improper Command Notes, this is also punishable under *the Penal Code* (KUHP). Additionally, if a business is hindered by such hacking, the crime is punishable by imprisonment for up to five years or a fine of up to JPY 1 million ( *Penal Code* , Article 234-2).

b. ***Phishing***
Article 7 of the UCAL prohibits phishing, while Article 4 of the UCAL prohibits obtaining identification codes through phishing. This action is punishable by imprisonment for up to one year or a fine of up to JPY 500,000 (Article 12). Additionally, anyone who obtains illegal profits by using identification codes obtained through phishing may be subject to a prison sentence of up to 10 years under Article 246-2 *of the Penal Code* .

c. **Identity theft or identity fraud ( *identity theft* )**

For identity theft or identity fraud, the same penalties/sanctions as Phishing are imposed, namely imprisonment of up to one year or a fine of up to JPY 500,000

**d. Electronic Theft ( *electronic theft* )**

In addition to the criminal penalties applicable to phishing, electronic theft is also subject to sanctions under the Unfair Competition Prevention Act. If a current or former employee:

1) obtain company trade secrets through theft, fraud, threats, or other illegal acts ("Illegal Acts"), including Unauthorized Access; or
2) using or disclosing an employer's trade secret obtained through illegal acts, with the aim of obtaining wrongful gain or causing harm to the owner of the trade secret, the employee is threatened with imprisonment for a maximum of 10 years or a fine of up to JPY 20 million, or both ( Article 21, Paragraph 1).

Additionally, if the employee commits any of the above acts outside Japan, the fine will be increased to JPY 30 million (Article 21, Paragraph 3).

Under the Copyright Law *of Japan* , anyone who uploads electronic data of a film or music, without permission from the copyright owner, so that others can download it, can be subject to a prison sentence of up to 10 years or a fine of up to JPY 10 million. , or both (Article 119 Paragraph 1). Furthermore, anyone who downloads electronic data protected by someone else's copyright, and is aware of such protection, is threatened with imprisonment for a maximum of two years or a fine of up to JPY 2 million, or both (Article 119, Paragraph 3). Additionally, anyone who sells, lends, manufactures, imports, stores, or uploads any device or program that can remove, disable, or alter technology intended to protect copyright (e.g., copy protection code) may be subject to imprisonment of up to three years or a fine of up to JPY 3 million or both (Article 120-2).

**Responsibility of business operators/entrepreneurs**

Pursuant to the APPI, a business operator must report the following Incidents involving the disclosure, loss or damage of Personal Data (defined in the APPI) it handles ("Data Breach") to *the PPC* (Article 26):

a. Data Breach of "Personal Information Requiring Special Treatment" (defined in APPI), such as employee health examination results;
b. Data Breach of Personal Data that creates a risk of financial loss to the data subject, such as credit card numbers;
c. Data Breaches caused by wrongful intent such as cyber attacks or internal fraud;
d. cases involving a large number of Data Breach events (more than 1,000 data subjects); And
e. when there is a possibility of the above things happening.

In addition, businesses that carry out "advanced encryption or other measures necessary to protect the rights and interests of data subjects" will be exempt from reporting or notification obligations, even if there is a Data Breach.

Business actors who become aware of the Data Breaches listed above or the possibility thereof must immediately submit an initial report regarding matters known to them at that time, and must submit a definitive report within 30 days, which report must include:

1) outline of Data Breaches;
2) details of affected Personal Data;
3) number of Data Breaches incidents;
4) causes of Data Breaches;
5) the presence of secondary damage and its details;
6) status of implementation of response/notification to data subjects;
7) status of implementation of public announcements;
8) steps to prevent recurrence; And
9) other things that PPC might find useful.

Regarding the above, reporting incidents is not an obligation. However, if a telecom operator does not report a serious incident, it will be subject to a fine of up to JPY 300,000. If the business operator does not report a serious incident based on the APPI, the PPC can provide recommendations or issue orders, and if the operator does not comply with the PPC's orders, he can be subject to imprisonment for a maximum of one year or a maximum fine. to JPY 1 million. In addition, if employees of a business entity do not comply with PPC orders, the business entity will also be subject to a fine of up to JPY 100 million.

## 4. Conclusion

Theft of personal data has become one of the main challenges in today's increasingly advanced digital era. Stolen or misused personal data can result in serious consequences for individuals, including identity fraud, financial loss, and detrimental privacy violations. Indonesia and Japan, two countries that have significant economic and technological development in the Asian region, are not immune from the threat of personal data theft. Although both have different legal and cultural frameworks, both strive to protect the personal data of their citizens from increasingly complex cyber threats.

Both Indonesia and Japan generally regulate personal data protection in depth. Indonesia only passed regulations protecting personal data in 2008 through Law Number 11 of 2008 concerning Information and Electronic Transactions which has undergone two amendments, namely the first amendment to Law Number 19 of 2016 and the second amendment to Law Number 1 of 2024 This regulation regulates information and electronic transactions starting from information, documents and electronic signatures, electronic system operators, domain names, intellectual property rights, and protection of personal data, prohibited actions, as well as criminal sanctions. However, this regulation does not regulate personal data protection in depth. Because there are no regulations that specifically regulate personal data protection, in 2022 Indonesia passed Law Number 27 of 2022 concerning Personal Data Protection which regulates types of personal data, rights of personal data subjects, processing of personal data, obligations of personal data controllers and processors. personal data, transfer of personal data, prohibitions on the use of personal data, and also criminal sanctions.

Compared to Indonesia, Japan is much earlier in respecting and protecting personal data. Regulations regarding personal data protection have existed since 2000, namely with the adoption of the Data Protection Act by the Japanese federal government. Not long after that, in 2003 *the Act on the Protection of Personal Information* (APPI) was passed, which was then amended in 2017 and 2022.

Both Indonesia and Japan regulate cybercrime crimes such as hacking, phishing and illegal access related to the protection of personal data. However, compared to Japan, Indonesia seems to be lagging behind in protecting personal data, Indonesia only passed a personal data protection law in 2022, while Japan has paid attention to protecting personal data since 2000. Apart from that, regulations regarding personal data are spread across several regulations. in Japan such as APPI, My Number Act, and Act on Prohibition of Unauthorized Computer Access. Japan strictly regulates the responsibilities of business operators/business actors relating to personal data in

APPI, if a data breach is found or there is a possibility of a data breach, the business actor must report to the PPC, otherwise a fine will be imposed, and if there is a serious incident and the business actor does not report, the PPC can issue an order which, if not implemented, the business actor can be sentenced to prison for a maximum of 1 year. The responsibility of business actors in protecting personal data is still underestimated in Indonesia. Indonesia also has an institution responsible for supervising and enforcing personal data protection which was only established in 2020, known as the Personal Data Protection Agency (BPDP), but this body does not appear to have maximally monitor the protection of personal data. The responsibility of business actors in protecting personal data is also not optimal, often regulations appear to only exist but are not fully implemented, such as when data leaks occur, this does not receive serious handling from the government and in some moments the government appears to not have full control over the protection of personal data.

## Refrences

NurhayatiNurhayati, Yati, Ifrani Ifrani, and M. Yasir Said. 2021. 'METODOLOGI NORMATIF DAN EMPIRIS DALAM PERSPEKTIF ILMU HUKUM', Jurnal Penegakan Hukum Indonesia, 2.1: 1–20

Djulaeka. 2014. Konsep Perlindungan Hak Kekayaan Intelektual Perspektif Kajian Filosofis HaKIKolektif-Komunal. Malang. Setara Press. p.134

Emawati Junus. 2007. Makalah PPT dalam Pentingnya Perlindungan Indikasi geografis SebagaiBagian dari HKI dan Pelaksanaannya di Indonesia. Jakarta. Ditjen HKI.

Mark Pendergrast. 2010. Uncommon Grounds : The History of Coffe and How It TransformedOur World. Ingram Publisher Service Us.

Muhammad Djumhana dan R.Djubaedillah. 2003. Hak Milik Intelektual Sejarah Tepri danPrakteknya di Indonesia Edisi Revisi. Cetakan Ketiga. Bandung. PT.Citra Aditya Bakti.

National Geographic. 2009. Coffe, Beyond The Buzz.

Philipus M. Hadjhon. 1988. Perlindungan Hukum Bagi Rakyat Indonesia. Bina Ilmu. Surabaya. Rachmadi Usman. 2003. Hukum Hak Atas Kekayaan Intelektual, Perlindungan dan Dimensi Hukumnya di Indonesia. Bandung. Alumni.

Saky Septiono. 2009. Perlindungan Indikasi Geografis dan Potensi Indikasi Geografis Indonesia.

Subdit Indikasi Geografis Ditjen HKI : Kementerian Hukum dan HAK RI.

Dara Qurhni Effida, Etty Susilowati, Kholis Roisah. 2015. Upaya Perlindungan Hukum Indikasi Geografis Terhadap Salak Sidimpuan Sebagai Kekayaan Alam Tapanuli Selatan. Jurnal Law Refor. Vol.11, Bo.2. Program Studi Magister Ilmu Hukum, Fakultas Hukum Universitas Diponegoro.

Devica Rully Masrur. 2018. Perlindungan Hukum Indikasi Geografis yang Telah Didaftarkan Sebagai Merek Berdasarkan Instrumen Hukum Nasional dan Hukum Internasional. LexJurnalica. Vol. 15 No.2. p.198

Haritsah, Budi Santoso, Rinitami Njatrijani. 2017. Perlindungan Indikasi Geografis Terhadap Kopi Arabika di Dusun Jumprit, Desa Tegalrejo, Kecamatan Ngadirejo, Kabupaten

Temanggung Provinsi Jawa Tengah. Diponegoro Law Journal. Vol.6, No.2. p.2. https://ejournal3.undip.ac.id/index.php/dlr/article/view/19575

Indra Rahmatullah. Desember 2014. Perlindungan Indikasi Geografis dalam Hak Kekayaan Intelektual Melalui Ratifikasi Perjanjian Lisabon. Jurnal Cita Hukum. Vol. II No.2. ISSN :2356-1440. Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta.

Siti Asfiyah. Oktober 2015. Perlindungan Hukum Potensi Indikasi Geografis Di Kabupaten Brebes Guna Pengembangan Ekonomi Masyarakat Lokal. Jurnal Idea Hukum, Vol.1 No.2. Magister Hukum Fakultas Hukum Universitas Jenderal Soedirman.

Tatty Ramli dan Yetti Sumiati. 2008. Impplikasi Pendaftaran Indikasi Geografis Terhadap PotensiPeningkatan Pertumbuhan Ekonomi Masyarakat. Jurnal Hukum Bisnis. Bo.27 No.4.

Winda Risna Yessiningrum. 2015. Perlindungan Hukum Indikasi Geografis Sebagai Bagian DariHak Kekayaan Intelektual. Jurnal Kajian Hukum dan Keadilan IUS, Vol. III, No.7. p.45

Yuni Zanesty Hutapea. 2020. Analysis of Factors Affecting Demand For Gayo Robusta Coffee (Coffee Camephora). Universitas Medan Area. http://repository.uma.ac.id/handle/123456789/12125

1945 Constitution of the Republic of Indonesia

Law Number 19 of 2013 concerning Protection and Empowerment of Farmers

Law of the Republic of Indonesia Number 20 of 2016 concerning Marks and Geographical Indications

Government Regulation No. 51 of 2007 concerning Geographical Indications http://www.aekiaice.org/

https://www.talkaboutcoffee.com/coffee-beans.html Coffe Beans – The Many Varieties of The Coffe Plant.https://ig.dgip.go.id/detail-ig/26#batas-wilayah