The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

ELECTRONIC OPERATOR'S LEGAL RESPONSIBILITY FOR PERSONAL DATA LEAKAGE

ANDI WIDIATNO[1], MELLA ISMELINA FARMA RAHAYU[2] AND ARIAWAN GUNADI[3]

[1]Tarumanagara University. Email: andiwidiatno.untar@gmail.com
[2]Tarumanagara University. Email: mellaismelina@yahoo.com
[3]Tarumanagara University. Email: ariawang@fh.untar.ac.id

ABSTRACT

The development of the industrial revolution has brought the development of digital technology in a country, Indonesia is no exception. The current intensity of information is very often reported about the leakage of personal data collected by e-commerce providers. Reports of data leakage cases since May 2020 Up to now. Protection of personal data is also in line with the purpose of the founding of the Republic of Indonesia. This is stated in the 1945 Constitution of the Republic of Indonesia. However, despite the importance of data protection, until now there has never been an electronic operator, both nationally and internationally, who has been asked to take legal responsibility for the leakage of personal data that afflicts Indonesian citizens. The purpose of this study is to see a normative juridical description of the legal responsibilities of electronic providers for personal data leakage. This type of research is a normative juridical research with a qualitative approach. The results of the study are that there is still no law that protects personal data from data leakage so that many certain people can provide data so that data leaks occur.

Keywords: Personal Data, Legal, Data Leakage, Electronic Provider, Liability.

INTRODUCTION

The intensity of information is currently very often reported about the leakage of personal data collected by e-commerce organizers, such as Tokopedia, Gojek, and Bukalapak. A total of 91 million user data and more than 7 million personal data were reportedly leaked and sold on internet black market sites /dark web and sold at a price of US $ 5,000 or around Rp. 74 million.1 Along with the development of internet users in Indonesia. A series of cases regarding data leakage case reports since 2020 exactly in May 2020, the Tokopedia company experienced data leaks as many as 91 million users and 7 million merchants. The stolen data has been transacted in the empire market at a price of US$ 5,000. Second, the company Bhineka.com experienced a leak of user data as much as 1.2 million data. The data is sold on the dark web at a price of US$ 1,200. Third, the state agency Election Commission in May 2020 leaked data of 2.3 million voters in the 2014 elections. The data is sold on Raid Forums which cannot be known at a price. Fourth, there was a leak of user data in the Bukalapak company as much as 13 million user data. The data was sold in Raid Forums for US$ 5,000. Fifth, there was a leak of Covid-19 data in June 2020. A total of 230 thousand covid-19 patient data was leaked and traded on Raid Forums, the price of which is not yet known. Sixth, data leaked from the Cermati Company in 2020 which has leaked as much as 2.9 user data. The data has been traded for

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

US$2,200. Seventh, the case experienced by the Kredit Plus Company in August 2020 experienced a data leak of 819,976 customer data. The data is traded inside Raid Forums and its price is not yet known. Furthermore, data from BPJS Kesehatan on May 12, 2021 leaked as many as 100,002 participant data from 279 million data and is still under investigation. The data was sold on Raid Forums for 0.15 Bitcoin or worth Rp. 87.1 Million (at an exchange rate of Rp. 580,914,000).2 in addition to the leakage of personal data, there are problems regarding electronic operators in the Fintech field. Kominfo noted that from January to June 2021, it has blocked 447 illegal Fintechs in Indonesia. This phenomenon adds to a series of problems regarding electronic operators in Indonesia. It was noted from reports that there were complaints about this problem from 194 account complaints in 2020 increased to 2,403 account complaints obtained by the Ministry of Communication and Informatics.[3]

Protection of personal data is part of the concept of the right to privacy.4 The concept of the right to privacy itself is the idea of maintaining personal integrity and dignity.5 The concept of protection of personal data hints that the individual The owner of electronic information or documents in the form of personal data has the right to determine whether to share or exchange their personal data or simply become data used for verification without wanting the data not duplicated.6 In addition, the owner also has the right to determine the terms of the transfer of personal data. Furthermore, data protection also deals with the concept of privacy rights. The right to privacy has evolved so that it can be used to formulate a right to protect personal data.[7]

In fact, the individual owner of the information cannot refuse a request from the organizer as a condition for obtaining access or facilities for a product. Seeing the development of electronic money with various discounts and attractive offers organized by electronic money organizers such as: OVO, DANA, SHOPEE, LINKAJA, etc.8 then there are also online transportation providers such as Gojek and Grab. The potential violation of the right to privacy of personal data has shifted in the activities of mass collection of personal data (digital dossier) carried out by the government slowly but surely has shifted to private parties.9 Digital dossier which is a collection of a person's personal data in large quantities using digital technology has been started since 1970 by governments especially in European countries and the United States.[10] Now, the private sector is also a digital dossier using internet technology. The digital dossier practices carried out by private parties have the potential to violate a person's right to privacy over their personal data.[11]

Direct selling practices are practices that sellers take to market goods by means of direct marketing.12 Seeing the development of this way of marketing, the data bank industry has developed that specifically collects consumer information. Until now, there are more than 550 data collection companies or now called data banks (databases) that trade consumer information. Companies that make transactions via the internet will get consumer information by purchasing this information from the services of this data collection company. The transaction value of the sale of consumer personal data in 2018 globally has reached 3 billion US dollars.[13] monitoring such rapid growth has given birth to electronic organizing companies as data banks that globally have placed them into companies that have large revenues. Customer personal information has become an invaluable asset to the aforementioned

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

companies.[14] As a result, various ways are used to collect as much personal data as possible in ways that often do not respect a person's right to privacy. Other consequences of leakage of personal data in Indonesia could be related to terrorism activities. Perpetrators of terrorism can use leaked personal data of citizens for the purpose of adding members of their terrorist membership.[15] As a result the right to the security of a person's personal data can be inflicted and violated. Protection is unlikely to rely on regulations set forth in the form of laws and regulations, however, with the regulation regarding the protection of personal data, it is more or less expected to minimize the threat of misuse of personal data in multisectoral. Personal data protection arrangements are intended to protect the interests of internet users (cyber netizens) in surfing cyberspace and provide economic benefits to Indonesia.[16]

Personal data in electronic information and/or documents has been regulated in article 26 of Law Number 11 of 2008 concerning Information and Electronic Transactions as a manifestation of what is outlined in Article 28 G paragraph (1) of the 1945 Constitution, that: "Every people have the right to protection for themselves, their families, honor, dignity, and property under their control, and have the right to feel safe and protected from threats of fear to do or not do something that is a human right. "In addition, there is Article 28 H of the Law -The 1945 Constitution, which states: "Every person has the right to have personal property rights and these property rights may not be taken over arbitrarily by anyone". Protection of personal data is also in line with the objectives of the establishment of the Republic of Indonesia. This is stated in the fourth paragraph of the Preamble to the 1945 Constitution of the Republic of Indonesia (hereinafter abbreviated as the 1945 Constitution). The fourth paragraph of the Preamble of the 1945 Constitution states that the national goals are (1) to protect the entire Indonesian nation and all of Indonesia's bloodshed; (2) promoting public welfare; (3) educate the life of the nation; and (4) participate in carrying out world order based on freedom, eternal peace and social justice.

There are previous studies related to the issue of criminal liability for electronic providers. There is a research conducted by Sandra Wijaya in his thesis entitled "Corporate Criminal Liability of Web-Based Electronic Information Technology Service Providers and Applications for Leaking Users' Personal Data".[17] corporate crime of web-based information technology and applications for the leakage of personal data. Furthermore, this study also emphasizes that the handling of corporate crime still has weaknesses in the rule of law and the need for legal discovery from law enforcement. In contrast to this research, which does not only discuss the organizers of web-based electronic systems, but tries to thoroughly discuss electronic providers. Researchers are more focused on the study of the legal responsibility of electronic providers for the leakage of personal data in both civil and criminal ways. This responsibility is in order to provide protection for Indonesian citizens. And pay attention to what has happened and what needs to be improved. These efforts are made to find a protection model that is in accordance with the Indonesian culture in the future. The point of novelty or originality in this dissertation research is to determine the ideal model for the legal responsibility of electronic providers for personal data leakage. The purpose of this study is to see a normative juridical description of the legal responsibilities of electronic providers for personal data leakage.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

RESEARCH METHODS

This research is a normative juridical research with a qualitative approach that looks at and analyzes legal norms in existing laws and regulations as well as court decisions and business practices that develop within the scope of the application of information technology into an electronic system to matters relating to the accountability of electronic providers. , and the application of law over and within the discipline of criminal law.[18]

RESULTS AND DISCUSSION

A. Provisions of Legislation related to Personal Data Protection

Regulations regarding personal data are still partially regulated in various laws and regulations in Indonesia. These regulations are partially spread out in laws, government regulations and their derivative regulations.

1. Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998 concerning Banking (Banking Law).

Banking activities will certainly involve customers. The customer will store his data at the bank to be able to use existing bank products. The foundation of both parties is the principle of trust and confidentiality. Banks must be able to maintain customer trust and protect the privacy of customers who have provided and entrusted their personal data to the bank. The following are related articles in the Banking Law:

1) Article 1 paragraph (28) of the Banking Law states that bank secrecy is everything related to information regarding depositors and their deposits.
2) Article 40 of the Banking Law states that regarding bank secrecy, banks are required to keep confidential information about depositors and their deposits, except in certain cases which are permitted.
3) Article 47 paragraph (2) of the Banking Law, those with the obligation to uphold bank secrecy are: First. Member of the Bank's Board of Commissioners; Second. Member of the Board of Directors of the Bank; Third. Bank employees; and, Fourth. Other affiliated parties of the Bank.
4) Articles 41 to 44 of the Banking Law regarding exceptions to the obligation to maintain bank secrecy: first, for tax purposes, exemptions can be granted to tax officials based on orders

Management of Bank Indonesia at the request of the Minister of Finance (Article 41); secondly, for the settlement of bank receivables that have been submitted to the State Receivables and Auction Agency/Committee for State Receivables, an exception may be granted to Officials of the State Receivables and Auctions Agency/PUPN with the permission of the Management of Bank Indonesia (Article 41A); third, For the purposes of justice in criminal cases, an exception may be granted to the police, prosecutors or judges with the permission of the Management of Bank Indonesia (Article 42); fourth, in civil cases between banks and their customers an

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

exemption may be granted without having to obtain permission from the Management of Bank Indonesia (Article 43); fifth, in the context of exchanging information between banks and other banks, exemptions can be granted without having to obtain permission from the leadership of Bank Indonesia (Article 44); sixth, approval, request or power of attorney from a depositing customer in writing may be granted an exception without having to obtain permission from the Management of Bank Indonesia [Article 44A paragraph (1); seventh, request for a legal heir from a depositor who has passed away (Article 44A paragraph (2).

2. Law Number 36 of 1999 concerning Telecommunications.

Telecommunications operators are closely related to the transmission, interconnection and transfer of data and information activities quickly. Of course, this transfer of information and personal data can occur very easily and quickly. Of course, it is data that moves. The following are articles related to data protection in this law:

1. Article 18 paragraph (1) stipulates the obligation of telecommunications operators to record or record in detail the use of telecommunications services.
2. Article 22 of the Telecommunications Law prohibits access to telecommunications or special telecommunications networks and services without rights, illegally, or by manipulation.
3. Article 40, the acquisition of information transmitted through telecommunications networks is prohibited in any form.
4. Article 42 paragraph (1) of the Telecommunications Law requires telecommunications service providers to keep the information sent and received by telecommunications service customer's secret through the telecommunications network and services they provide. Exceptions to this secrecy are among others for the benefit of the criminal justice process at the written request of the attorney general or the head of the police and investigators.
5. Article 56 and Article 57 of the Telecommunications Law, Regulation of criminal sanctions for violating the privacy protection articles on the personal data of telecommunications service users. Violations of these articles are punishable by criminal sanctions in the form of fines or imprisonment.

3. Law Number 8 of 1999 concerning Consumer Protection.

Data and information guaranteed by the Consumer Protection Act is information about goods and services, not information about consumers' personal data. However, consumer protection according to Article 2 of the Consumer Protection Act is based on benefits, fairness, balance, consumer security and safety, and legal certainty is not translated into provisions for consumer personal data protection. Supposedly, consumer protection includes data and information protection.

Personal data about consumers are often obtained when consumers use services or buy goods. For example, when consumers use health services or banking services, the data obtained by

ISSN 1533-9211

DOI 10.5281/zenodo.7359284

business actors is then misused for promotional purposes, whether products are from the same business actor or even the data changes hands to parties outside the business actors who deal directly with consumers.

Promotion itself is regulated in the Consumer Protection Act. The definition of Promotion is explained in the General Provisions contained in Article 1 paragraph (6), namely: Activities of introducing or disseminating information on goods and/or services to attract consumers' buying interest in goods and/or services that will be and are being traded.

Promotional activities that are widely practiced by service providers and sellers of goods become a separate problem when using personal data obtained from other parties, without the consumer's consent. Furthermore, promotions that are usually through the media of telephone, short messages, letters or electronic mail can be promotions that consumers don't want, even disturbing for some people. This is partly because telephone numbers, residential addresses, and so on are a person's privacy. From this it can be seen that consumers are indirectly harmed by promotional activities that use consumer personal data.

4. Law Number 39 of 1999 concerning Human Rights

Article 29 paragraph (1) of the Human Rights Law recognizes the right of everyone to the protection of personal, family, honor, and dignity and property rights. The right to privacy needs to be recognized as part of the protected human rights. The right to privacy has become very important with the development of modern society where the exchange and transfer of information can occur quickly and easily. Do not rule out the transfer of data or personal information of a person illegally and used without the permission of the owner.

Article 14 paragraph (2) of the Human Rights Law stipulates that one of the rights to self-development is the right to seek, obtain, store, process, and convey information using all available facilities. Article 32 of the Human Rights Law stipulates that independence and confidentiality in communication relations through electronic means are guaranteed, except by order of a judge or other legal authority in accordance with the provisions of the law.

The arrangements contained in Article 14 paragraph (2) and Article 32 of the Human Rights Law above show that there is a balance between the right to obtain (search, obtain, store) and convey information, with the right to acknowledge confidentiality in communications, including personal data. To store information especially relating to someone's personal information. It can be concluded that the guarantee of the recognition of a person's right to privacy in Article 32 of the Human Rights Act is primarily in the protection of a person's personal information and data.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

5. Law Number 23 of 2006 concerning Population Administration as amended by Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration.

Based on this law there are articles related to the protection of personal data. These articles include:

1) Article 1 point 9 states that population data is individual data and/or structured aggregate data as a result of Population Registration and Civil Registration activities.
2) Article 1 number 22 states that personal data is certain individual data that is stored, maintained, and kept true and protected by confidentiality. In the sense of personal data contained in the Population Administration Law there is a mandate to protect the confidentiality of personal data.
3) Article 2 guarantees the right of every resident to obtain protection of personal data, legal certainty over document ownership, as well as information regarding data on the results of population registration and civil registration of himself and/or his family.
4) Article 2 letter f states that residents have the right to obtain compensation and restoration of their good name as a result of errors in population registration and civil registration and misuse of personal data by implementing agencies.
5) Article 8 paragraph (1) letter e of the Population Administration Law stipulates the obligation of the executing agency to carry out population administration affairs which include guaranteeing the confidentiality and security of data on population events and important events. Confidentiality and security of data on population events and important events has become the responsibility of the population administration implementing agency.
6) Article 79 paragraph (1) which states that population data and documents must be stored and protected by the state.
7) Article 85 paragraph (3) which states that the truth must be guarded and confidentiality protected by the organizers and implementing agencies.
8) Article 84 paragraph (1) states that personal data of residents must be protected. The personal data includes, among others, Family Card (KK) numbers; Population Identification Number (NIK); date/month/year of birth; information about physical and/or mental disability; NIK of biological mother; father's ID; and some contents of noteworthy events.
9) Article 85 paragraph (1) which states that personal data of residents must be stored and protected by the state.
10) Article 87 paragraph (1) stipulates that users of personal data of residents who are government or private agencies can obtain and use personal data from officers at the organizers and implementing agencies who have access rights. What is meant by users

ISSN 1533-9211

DOI 10.5281/zenodo.7359284

of resident personal data are government and private agencies that require data information in accordance with their fields.

11) Article 79 paragraph (2), the right of access to personal data and population documents is granted by the minister as the person in charge of access rights to officers at the organizers and implementing agencies of population administration.
12) Article 86 paragraph (1) also states that the Minister as the person in charge gives access rights to officers at the organizers and implementing agencies to enter, store, read, change, rectify and delete, copy data and print personal data.
13) Article 77 which prohibit anyone from changing, adding or subtracting without rights, the contents of the data elements in the population document. Prohibition of illegal access and misuse of personal data or residence documents contained in the population administration system.
14) Article 93 which threaten imprisonment and a fine for every resident who intentionally falsifies letters and/or documents to the Implementing Agency in reporting Population Events and Important Events.
15) Article 94 threatens to punish anyone who without rights intentionally changes, ads, or reduces the contents of the data elements in the population document.

Everyone without the right to access the population data base in Article 86 paragraph (1) shall be punished with imprisonment and a fine in Article 95. Likewise for any person or legal entity without the right to print, issue and/or distribute blank population documents in Article 96. In the event that officials and officers at the Organizers and Implementing Agencies assist in committing a criminal act, the officials concerned are also threatened with punishment as stated in Article 98 paragraph (2).

6. Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law)

The definition of an electronic system according to Article 1 point 5 of the ITE Law is a series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce, transmit, or disseminate electronic information. Based on the understanding of the electronic system, it can be seen that what is included in the electronic system is the internet network, e-banking services, e-government, social networks, electronic media, websites, and so on.

Utilization of information technology, protection of personal data is one part of the right to privacy. To provide a sense of security for users of electronic systems, the ITE Law regulates the protection of personal data and privacy rights as stipulated in Article 26 paragraph (1) of the ITE Law, which reads: any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

To clarify the meaning of the protection of privacy rights protected by the ITE Law, in the explanation of Article 26 it is explained that personal rights in the article contain the following meanings:

1) The right is the right to enjoy a private life and be free from all kinds of interference.
2) Personal rights are the rights to be able to communicate with other people without spying.
3) Privacy rights are the rights to monitor access to information about a person's personal life and data.

Article 26 of the ITE Law, the use of any personal information and data through electronic media carried out without the consent of the data owner is a violation of privacy rights. Although there is an acknowledgment of the protection of privacy rights and personal data in electronic information and transactions in the ITE Law as contained in Article 26 and its explanations, the obligations of protection and protection measures that should be carried out by related parties such as electronic system operators or the government are not yet contained in the ITE Law. ITE Law.

7. Law Number 14 of 2008 concerning Public Information Disclosure (Public Information Disclosure Act).

Article 1 paragraph (1) of the Law on Public Information Disclosure stipulates that information is information, statements, ideas, and signs that contain values, meanings, and messages, both data, facts and explanations that can be seen, heard, and read. Presented in various packages and formats in accordance with the development of information and communication technology electronically or non-electronically. Meanwhile, the definition of public information is information that is produced, stored, managed, sent, or received by a Public Agency related to the administration of the state or the organizer and operation of other Public Bodies relating to the public interest. From the definition of public information, it can be seen that public bodies as regulated in the law collect data and information related to its implementation. The collection of data and information also includes the collection of data and information belonging to the public which are collected in such a way as to comply with the provisions of the applicable laws and regulations. The protection of public data and information collected by public bodies is regulated in Article 6 paragraph (3) of the Law on Public Information Disclosure. Based on these rules, there is public information that cannot be provided by public bodies, namely:

1) Information that can harm the country;
2) Information related to the interests of protecting business from unfair business competition;
3) Information relating to personal rights;
4) Information related to job secrets; or
5) The requested public information has not been mastered or documented.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

In this provision, it is clear that public bodies cannot provide public information, one of which relates to private rights. Furthermore, Article 52 of the Law on Public Information Disclosure stipulates that public bodies that intentionally do not provide, do not provide, or do not publish public information in the form of public information on a regular basis, public information that must be announced immediately, public information that must give on the basis of a request in accordance with this law, and causing harm to another person is subject to a maximum imprisonment of 1 (one) year and a maximum fine of Rp. 5,000,000.00 (five million rupiah).

8. Law Number 36 of 2009 concerning Health (Health Law).

The protection of the patient's medical history is contained in Article 57 paragraph (1) of the Health Law which recognizes the right of everyone to the confidentiality of his personal health condition that has been presented to the health service provider. Furthermore, Article 57 paragraph (2) stipulates the provisions for the exception to the confidentiality of personal health conditions which do not apply in the case of:

1) Statutory orders;

2) Court order;

3) Permit in question;

4) Community interest; or

5) The interest of the person.

Although there is an acknowledgment of the patient's right to obtain protection for his personal data in the form of a medical history, the protection of the patient's personal data is not fully regulated in the Health Law. In the Health Act, there are no sanctions or penalties for violations of privacy committed on the patient's medical history. There are no administrative or criminal sanctions, either for unauthorized access or misuse of patient's personal data by unauthorized parties.

9. Law Number 40 of 2014 concerning Insurance (Insurance Law).

Article 67 of the Insurance Law regulates the issue of information protection by other parties appointed or assigned by the Financial Services Authority in carrying out the supervisory function and part of the regulatory function. Such parties are prohibited from using or disclosing any confidential information to other parties, except in the context of carrying out their functions, duties, and authorities based on the decisions of the Financial Services Authority or required by law.

10. Law Number 21 of 2011 concerning the Financial Services Authority (Financial Services Authority Law).

Article 33 paragraph (1) of the Law on the Financial Services Authority regulates the confidentiality of information. Every individual who has served or has served as a member of the Board of Commissioners, official or employee of the Financial Services Authority (hereinafter referred to as OJK) is prohibited from using or disclosing any information that is

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

confidential to other parties, except in the context of carrying out his functions, duties and authorities based on a decision. OJK or required by law.

Furthermore, Article 33 paragraph (2) stipulates that any Person acting for and on behalf of the OJK, employed at the OJK, or as an expert staff at the OJK, is prohibited from using or disclosing any confidential information to other parties, except in the context of implementing its functions, duties, and authorities are based on OJK decisions or are required by law.

Financial services authorities have also regulated the confidentiality of consumer personal data in OJK Regulation No. 1/POJK.7/2003 which essentially requires financial service actors, namely banks, securities companies, investment advisors, pension fund managers, insurance companies, financing institutions, pawn companies and companies. Guarantees to keep data or information about consumers to third parties unless there is consumer approval or statutory obligations.

If the financial service actor has obtained consumer data from another party, it must be accompanied by a written statement that the consumer has agreed to provide personal data or information to any party, including the financial service actor. Consumers may change the agreement to disclose data or personal information that has been previously provided in writing.

11. Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP PSTE).

This government regulation further regulates the substance of personal data protection in electronic transactions. Protection regarding the privacy of one's personal data must be upheld because the development of electronic systems is increasing and massive. The following are the articles in this rule:

1) Article 1 paragraph (27) states that personal data is certain individual data that is stored, maintained, and kept true and protected by confidentiality. In this definition, apart from explaining what personal data is, there is also a mandate to protect the confidentiality of personal data.
2) Article 1 paragraph (6) PP PSTE describes electronic information as one or a set of electronic data, including but not limited to writing, voice, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail (electronic mail). , telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or perforations. This electronic information can be contained in an electronic system or in the form of an electronic document.
3) Article 9 paragraph (1), which stipulates that electronic system administrators are required to guarantee the confidentiality of the source code of the software used.
4) Article 12 paragraph (1), which states that electronic system operators in operating their electronic systems are required to guarantee the availability of service level agreements, the availability of information security agreements for information technology services

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

used, as well as information security and internal communication facilities that are organized.

5) Article 15 paragraph (1), which states that Electronic System Operators are given the following obligations, including: first, to maintain the confidentiality, integrity and availability of the personal data they manage; secondly, guarantee that the acquisition, use and utilization of personal data is based on the consent of the owner of the personal data, unless otherwise stipulated by laws and regulations; and third, guaranteeing that the use or disclosure of data is carried out based on the consent of the owner of the personal data and in accordance with the purposes conveyed to the owner of the personal data at the time of data acquisition.

6) Article 15 paragraph (2) states that the operator of the electronic system is obliged to notify the owner of the personal data in writing if there is a failure in protecting the confidentiality of the Personal Data they manage.

7) Article 22 paragraph (1), obliges electronic system operators to maintain the confidentiality, integrity, authenticity, accessibility, availability and traceability of electronic information and/or electronic documents in accordance with the provisions of laws and regulations.

8) Article 38 paragraph (2) stipulates that electronic agent operators are required to have and carry out standard operating procedures that meet the principles of controlling user data security and electronic transactions. The control principles for securing user data and electronic transactions include confidentiality, integrity, availability, authenticity, authorization, and denial. What is meant by "confidentiality" is in accordance with the legal concept of confidentiality of information and electronic communications.

9) Article 39 paragraph (1) regulates the obligations of Electronic Agent Operators, which include: first, to test identity authenticity and check the authorization of Electronic System Users conducting Electronic Transactions; second, have and implement policies and procedures to take action if there are indications of data theft; third, ensuring control over authorization and access rights to systems, databases, and Electronic Transaction applications; fourth, develop and implement methods and procedures to protect and/or keep the integrity of data, records, and information related to Electronic Transactions confidential; and fifth, have and implement standards and controls over the use and protection of data if the service provider has access to the data. The regulation of the obligations of the electronic agent operator above shows the protection of personal data in the electronic documents used.

10) Article 55 paragraph (3) which regulates electronic signature creation data states that the entire process of electronic signature creation must be guaranteed security and confidentiality by the electronic signature operator or electronic signature service supporter. Then the electronic signature creation data is stored in an electronic media that is in the control of the signer. Data related to the signer must be stored in a place or data storage facility that uses a trusted system. The system must be able to detect changes and

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

meet the following requirements: first. Only authorized persons can enter new data, change, exchange, or replace data; secondly, the identity information of the signer can be checked for authenticity; third. Other technical changes that violate security requirements can be detected or known by the operator; and fourth. The signer shall maintain confidentiality and be responsible for the electronic signature creation data.

11) Article 68 paragraph (1) regulates reliability certificates issued by reliability certification bodies covering categories: security against identity, security against data exchange, security against vulnerability, rating of consumers, and security of confidentiality of personal data.

12) Violation of the personal data protection efforts, the electronic system operator or agent will be given administrative sanctions as contained in Article 84. The administrative sanctions can be in the form of written warnings, administrative fines, temporary suspension, as well as being removed from the list of electronic system operators, electronic agents, electronic certification provider, or reliability certification body.

12. Presidential Regulation Number 26 of 2009 as amended several times, most recently with Presidential Regulation Number 126 of 2012 concerning the Third Amendment to Presidential Regulation Number 26 of 2009 concerning Application of National Identity Cards Based on National Population Registration Numbers (Perpres KTP).

Perpres KTP is an implementing regulation that has been amended 3 times from Presidential Regulation No. 26 of 2009 concerning the Application of National Identity Cards Based on National Population Identification Numbers which was previously amended by Presidential Regulation Number 35 of 2010 concerning Amendments to Presidential Regulation Number 26 of 2009 concerning Application of National Identity Card Based on National Identity Number, and amended the second time by Presidential Regulation Number 67 of 2011 concerning the Second Amendment to Presidential Regulation Number 26 of 2009 concerning Application of National Identity Card Based on National Identity Number. The following articles are related to the protection of personal data:

1) Article 6 paragraph (1) of Presidential Regulation Number 35 of 2010 concerning Amendments to Presidential Regulation Number 26 of 2009 concerning the Application of National Identity Cards Based on National Population Identification Numbers, the KTP contains security codes and electronic records as a means of data verification and validation population identity.

2) Article 1 point 8 of Presidential Regulation Number 26 of 2009 concerning the Application of National Identity Cards Based on National Population Identification Numbers, security codes are identity identification tools that show the identity of residents precisely and accurately as self-authentication which ensures that population documents belong to people. The electronic record contains biodata, signatures, passport photos, and fingerprints of the residents concerned.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

Personal data of residents is stored in a population database with limited access. Access is only given to people and interested parties based on the legal basis of the Population Administration Law. Government and private parties who need data information in accordance with their fields can obtain and use personal data from officers at the organizers and implementing agencies who have access rights.

This Prepres does not regulate and explain obligations regarding the protection of personal data belonging to residents. However, the draft of the Presidential Decree on KTP is in accordance with the spirit of the Population Administration Law. In addition, the Presidential Decree on KTP stipulates that the Electronic ID Card is an ID card that has been equipped with a chip and a special security system (Article 10 a Paragraph (1)).

13. Bank Indonesia Regulation Number: 7/6/PBI/2005 concerning Transparency of Bank Products and Use of Customer Personal Data (PBI No. 7/6/PBI/2005).

PBI No. 7/6/PBI/2005 is a concrete form of an implementing regulation issued by Bank Indonesia in order to protect the privacy of bank customers for their personal data. PBI No. 7/6/PBI/2005 was stipulated based on the consideration that transparency regarding the use of personal data submitted by customers to banks is needed to increase protection of customers' personal rights in dealing with banks.

1) Article 9 paragraph (1) PBI No 7/6/PBI/2005, states as follows: "Banks are required to request written approval from customers in the event that banks will provide and or disseminate customer personal data to other parties for commercial purposes, unless stipulated other by other applicable laws and regulations." In requesting the customer's approval for the use or dissemination of the customer's personal data, the bank must explain the purpose and consequences of using the data. This is especially for the use of customer personal data for commercial purposes, used by other parties to gain profit.
2) Article 10 paragraph (2) further stipulates that in seeking approval from the customer concerned, it must be done by signing an agreement form that has been specially made for approval of the use of the customer's personal data. The approval request clause is opt-in in nature. Means that banks are prohibited from doing things that are the purpose of including the clause, before the customer gives approval to the clause.
3) Article 11 PBI No. 7/6/PBI/2005 states that if a bank is going to use the personal data of a person and/or group of people obtained from another party for commercial purposes, then the bank is required to have a written guarantee from the party concerned which contains written consent from the people concerned to personal data disseminated by the bank.

Violations by banks regarding the transparency of the use of personal data by banks which have been regulated in PBI No. 7/6/PBI/2005 is subject to administrative sanctions and is used as material for calculations in the component of assessing the soundness of a bank on aspects of bank management.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

B. STUDY

Normative Studies and Case Studies of Personal Data Leaks

Information technology that is growing rapidly nowadays seems to be a currency that has two sides. On the one hand, technological advances encourage an increase and increase in human civilization, on the other hand, technological advances encourage acts against the law, including new criminal acts. Cybercrime is one of the terms that emerged with the advancement of existing technology.19 Forms of negligence committed by children can sometimes lead to leakage of personal data. This phenomenon can happen in the community because children who experience negligence in using technology and there are factors of parents who are not technology literate can be the cause of the leakage of personal data. The cases of personal data leakage in 2019-2022 are as follows:

1. Cases of Personal Data Leakage in 2019

a. Cases of data leaks are tried out computer assisted test (CAT) simulations.

This case is one of the cases that occurred in 2019 with a fraudulent modus operandi. This activity was organized by @cpnsindonesia.id, they took the data of people who registered in the form they provided and it was from this that the personal data of citizens was taken. The ministry confirmed that BKN had never collaborated with other parties in conducting simulations based on CAT.[20]

b. Facebook data leak case.

The case that befell 70 thousand user data consisting of women on Tinder, based on a report by the whith ops cyber security company. 70 thousand users consisting of women, this photo has been spread on cybercrime forums. The perpetrator used this photo to commit fraud against other people, aka catsifhing and the Facebook case with Cambridge Analytica, when around 87 million Facebook users' personal data was shared with third parties without the data owner's knowledge.[21]

c. Bukalapak Leak Case

In 2019, a Pakistani hacker with the alias “Gnosticplayers” claimed to have hacked a database containing 13 million data belonging to Bukalapak users and sold it on the dark web. The data contains information such as the user's email, telephone number, and date of birth. After this data leak case arose, Bukalapak investigated internally and admitted that there was a data leak. However, Bukalapak claims that this data leak did not affect sensitive information such as usernames, addresses and financial information.[22]

2. Cases of Personal Data Leakage in 2020

a. Tokopedia Leaks

In early May 2020, Tokopedia experienced a hack that affected the data belonging to 91 million Tokopedia users. Reports of hacking and data leaks were first revealed by Under the Breach,

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

an Israeli cybersecurity company. The findings were based on hacker uploads who shared a database of 15 million Tokopedia users on the internet forum, Raid Forums.

Shortly after the incident was revealed, Tokopedia notified all of their users while starting an investigation and ensuring users' accounts and financial information were not affected by this hack. The data leak case was immediately investigated by the Ministry of Communication and Information. After going through a long process, Tokopedia was finally given a written sanction by the Ministry of Communication and Information.

b. Data Leaks on Bhineka.com

At the end of May 2020, an Israeli cybersecurity consultant, Under the Breach, revealed that data from the KPU's 2.3 million Indonesian population was leaked and offered in one of the hacking forums. In the uploaded PDF file, this data contains information such as, name, address, Population Identification Number (NIK), Family Card Number, and others. After being traced, the data is voter data in 2013. The Indonesian KPU confirmed that the leaked data was the Permanent Voters List (DPT) in 2013. The KPU confirmed that the DPT data was in accordance with the existing regulations at that time, where the election data were “open". However, the resolution of this data leak case is still unclear.

c. Covid Data Leak

In June 2020, Raid Forums user "Database Shopping" claimed and sold a database containing data on 230 thousand Indonesian citizens related to Covid-19. The perpetrator said the data was successfully hacked on May 20, 2020. However, it did not say where it came from and it was offered on June 18, 2020. Based on Cyber threat. id's search, the sample data offered contained the date of the report, name, nationality, gender, age, telephone, residential address, contact type, case relationship, risk start date, risk end date, sick start date, outpatient date, outpatient health facility, hospitalization date, illness complaint, sampling date, type of examination, date of sending sample, date of taking results, final status, rapid test date, rapid test results, PCR test date, and PCR test results. Not only that, there are also a number of names that have undergone examination. Most of those that appear in the sample.

d. Creditplus data leak

In early July 2020, Cyble Inc., a cyber-security company from Atlanta, United States of America, found 896,170 data belonging to KreditPlus customers being sold on internet forums. Data sellers with “Megadimarus” accounts (having a credible reputation with GOD status) claim to have a database containing names, email addresses, passwords, physical addresses, telephone numbers, employment data, company data, and family data. Through Raid Forums, Kreditplus customer data was offered on June 27 2020. Then, on July 16, the Shiny Hunters account offered this data again. Unfortunately, until now there has been no explanation whatsoever from KreditPlus and this data leak case just disappeared.

e. Data leak in POLRI database

In June 2020, the Founder of the Indonesian Ethical Hacker Community, Teguh Aprianto, via his Twitter, revealed allegations that there was a leak of data on members of the National Police

ISSN 1533-9211

DOI 10.5281/zenodo.7359284

in an internet forum. He uploaded a screenshot containing the personal information of a member of the Indonesian National Police, starting from a photo of himself, his position history, rank, and so on.

Hojatking's account claims to have succeeded in breaking into the National Police database on May 31, 2020. Hojatking is selling full access to the database for US$ 1,200 (equivalent to Rp. 17 million). Meanwhile, for information on bugs (security holes) in the application, it sells for US $ 2,000 (Rp. 28.5 million). Even though it was said to be a hoax, this data leak was reinforced by a video uploaded by the perpetrator of the Polri database breach, which shows how he can enter and access the Polri personnel database like an admin. The database contains data on 14,785 active personnel, 909 personnel outside the Work Unit, 31 personnel currently in education, 1,594 retired personnel, 515 deceased personnel, 9,081 active positions, and several other data.

3. Cases of Personal Data Leakage in 2021

a. Personal Data Leakage at BPJK Health

In May 2021 a RaidForums user named Kotz sold a database containing personal information of Indonesian residents. The data sold includes NIK KTP, salary, cell phone number, address, and email. Kotz claimed to have obtained the data from the website bpjs-kesehatan.go.id, and would sell the database for 0.15 BTC (equivalent to Rp. 84.3 million or around US$ 6,000). The database consists of 279 million and 20 million of them are equipped with personal photos. Kotz claims the data also contains a list of people who have died. This data leak case was initially handled by the Ministry of Communication and Information and the BSSN, but was eventually transferred to the police and there has been no latest update regarding this case.

b. BRILIFE SHARIA Data Leaks

In July 2021, data allegedly belonging to 2 million BRI Life insurance customers was offered on a hacking forum by a user named "Reckt". But not long after that the thread he made to offer customer data disappeared. Previously, the Israeli cybersecurity company, Hudson Rock, had also identified hacks that occurred on several computers belonging to employees of BRI Life and Bank Rakyat Indonesia (BRI). The hack is believed to have allowed the hacker to gain early access to the company.

The BRI Life customer data is now being sold on a hacking forum for US$7,000 or the equivalent of Rp100 million. The data seller also attached a number of data samples which he documented in the form of a 30-minute video measuring 250 GB. The database does not only contain the personal data of 2 million customers. But it also contains 463,000 documents including bank account details, copies of ID cards, results of health checks in a laboratory, and taxpayer data. From the results of the investigation, BRI Life itself has found evidence of hackers infiltrating the BRI Life Syariah system. However, BRI Life claims that the hacked system contained no more than 25,000 thousand individual sharia policy holders and the data is not related to BRI Life or other BRI Group data.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

c. Personal data leak in eHAC

In August 2021 a research team from vpnMentor found that around 1.3 million data belonging to users of the Indonesian Electronic Health Alert Card (eHAC) application developed by the Indonesian Ministry of Health were exposed on the internet. The discovery was immediately reported to the Ministry of Health in July 2021 twice but was not responded to and was reported back to the BSSN in August 2021. The database, which is open on the internet, includes data on Covid-19 health tests including the identity and type of passenger, hospital identity, address. And home visit times, test types, test results, and so on. This case was investigated, but was finally stopped because no data theft was found.

d. Leakage of personal data at KPAI

A data leak occurred in October 2021, a RaidForums user "C77" offered data belonging to KPAI. It provides sample data to attract buyers. Each data is valued at 8 credits. KPAI has also admitted that it has experienced a data breach which resulted in the exposure of online complaint data on the KPAI website. However, they ensured that the hacking and theft of data had no impact on the services on the KPAI website. Judging from the sample data distributed, the database is arranged in the form of a table in .csv file format which contains, among others, identity, name, identity number/KTP, nationality, telephone, cellphone, religion, occupation, education, address, email, place of date birth, gender, province, city, and age.

Deputy Director of Research at the Institute for Community Studies and Advocacy (ELSAM), Wahyudi Djafar, regretted the leak of personal data at the state institution. He explained that based on the uploaded data sample, the data suspected of having leaked included 13 elements of personal data (name, identity number, email, telephone, occupation, education, place and date of birth, address, city, province, and nationality), as well as a number of data. Sensitive personality (religion and gender).[23]

4. Cases of Personal Data Leakage in 2022

a. Leakage of personal data at the Ministry of Health

The Ministry of Health is suspected of having experienced a data leak. This information was released on social media reddit and social media twitter. The form of data that was leaked was in the form of patient medical data and patient radiology images with a file size of 720 GB.[24] the Indonesian Ministry of Communication and Informatics responded to this in its Press Release No. 3/HM/KOMINFO/01/2022 which was issued on January 6 2022. In essence, this is a response to reports regarding leaks of patient data managed by the Ministry of Health. KOMINFO requests that the relevant staff continue to communicate intensively with the Ministry of Health and initiate follow-up actions. Furthermore, the Ministry of Health has also taken internal steps to respond to leaks that have occurred and coordinated with the National Cyber and Crypto Agency.

b. Leakage of personal data at PT Pertamina

Personal data from job applicants at PT Pertamina Training Consulting was allegedly leaked on Raid Forums. PTC which has a position as a subsidiary of Pertamina is engaged in human

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

resource development through training, consulting and management. The personal data that was allegedly leaked included ID cards, family cards, BPJS cards, birth certificates and diplomas, grades transcripts and data such as CVs, SKCK, photos, driver's licenses and drug-free certificates, health certificates. Leaked 163,181 files totaling 60 GB.[25]

Personal Data Review with Public Information Disclosure Settings

Public Information Disclosure will of course be very closely related to the conception of information. Understanding information, the word information comes from the word informare which means to give shape and to inform which means to inform. From the two definitions concerned, so inform can be interpreted as notification of a certain matter in order to form his views on something conveyed based on his knowledge. Constitution. Number 14 of 2008 concerning Public Information Disclosure (hereinafter referred to as the Public Information Disclosure Law) defines information as statements, statements, ideas and signs that contain values, meanings and messages, both data, facts and explanations that can be seen, heard, and read presented in various packages and formats in accordance with developments in information and communication technology, electronically or non-electronically.

This regulation describes the context of public information as information that is generated, stored, managed, sent, and/or received by a public agency relating to state administrators and administration and/or organizers and administration of other public bodies in accordance with this Law as well as information other matters relating to the public interest.[26] After obtaining the definition of information, one must also look at the definition of public information. Public information based on the UU KIP has the meaning of information that is generated, stored, managed, sent, and/or received by a public body related to the organizers and administration of the state and/or the organizers and administration of other public bodies in accordance with this Law and other information related to public interest.[27]

Of course, information that exists in Indonesia is not immediately disclosed and becomes public consumption due to the presence of this Public Information Disclosure Law. There are arrangements regarding information that is classified (withheld) and has been regulated in UU KIP.

Data Study of Witnesses and Victims in Indonesian Law

A witness is someone who has the first information about a crime or dramatic event through their senses of seeing, hearing, smelling, touching and can help ascertain important considerations in a crime or incident. A witness who sees an incident directly is also known as an eye witness.[27] Witnesses are often summoned to court to testify in a judicial process. Deemed sufficient according to the evidentiary system regulated in Article 183 of the Criminal Procedure Code. Article 184 of the Criminal Procedure Code places witness statements in first place above other evidence in the form of expert testimony, letters, instructions, and statements from the defendant. Meanwhile Article 185 paragraph (2) states: "The testimony of a witness alone is not sufficient to prove that the defendant is guilty of the act he is accused of". However, Article 185 paragraph (3) also confirms: "The provisions as referred to in paragraph (2) do not apply if accompanied by other valid evidence". This can be interpreted that the testimony of

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

more than 1 (one) witness alone without being accompanied by other evidence, can be considered sufficient to prove whether a defendant is guilty or not. So important is the position of witnesses in uncovering a criminal act in Article 184 and Article 185 of the Criminal Procedure Code.

Seeing the importance of witnesses as emphasized in the provisions of Article 184-185 of the Criminal Procedure Code as described above, it is only natural for witnesses or victims in law enforcement efforts to be given protection, so that in giving their testimony before the court, witnesses feel safe and free from threats/pressures either physical or psychological. to himself and his family. The witness should not hesitate to explain the actual incident, even though his statement may incriminate the defendant. Therefore, Article 173 of the Criminal Procedure Code gives authority to the Panel of Judges to allow a witness to be heard without the presence of the defendant. The reason is clear, to accommodate the interests of the witness so that he can speak and give his testimony more freely without fear, worry or pressure. However, there is a guarantee of security and freedom from fear for witnesses when examined before the court for the information they provide. In fact, this guarantee of security and freedom from fear becomes very important so that witnesses do not hesitate to tell the truth. The end goal is how to create a sense of justice for the community, to achieve the legal system in Indonesia.

The existence of victims also has an important position in the criminal law enforcement process. Victims become someone who must get protection as well as witnesses. However, the regulation in the police investigation process does not regulate victims in it. The position of the victim in the investigation process is only for the purpose of proving the actions or mistakes committed by the perpetrator in a crime. Bearing in mind that in this case, the victim only serves as evidence for witness testimony.

Lack of legal protection for victims can cause victims to be passive and tend to be non-cooperative with officers. There is even a correlation between the lack of protection and the reluctance of victims to report to the authorities, especially after the victim reports, their role and position shifts in such a way that the judiciary feels that they are the only party that can represent all the interests of the victim.[28]

Personal Data Review with Consumer Protection Law

Technology in this modern era forms new habits. These new habits have positive and negative impacts. Of course this has an impact on the banking sector of the economy. Many startup companies have sprung up or known as start-ups in the online loan financial sector. This instrument is based on information technology or known as fintech peer to peer lending (P2P Lending).[29] these activities are included in e-commerce activities. Of course, this activity is very closely related to two things, namely personal data and aspects of consumer protection.

Referring to the juridical provisions regarding consumer protection, of course, refers to Law Number 8 of 1999 concerning Consumer Protection. Based on the law, there are several principles accompanying the implementation of consumer protection.[30]

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

The development of regulations regarding the protection of personal data in general will place Indonesia on a par with countries with modern and advanced economies. Of course, countries that have implemented laws regarding the protection of personal data. Indonesia can become a trusted business and investment center, provided that this key strategy can work within the Indonesian legal system.

Comparative Study of Personal Data Protection Studies in Other Countries

With regard to enforcement, using the standard theory of 'responsive regulation', Graham's conclusion is that South Korea and the Macao SAR have 'the widest range of enforcement mechanisms', and utilize them effectively. Hong Kong, while the lack of enforcement mechanisms until 2012, is compensated by a very strong enforcement activity. Laws in some countries such as Singapore, Malaysia and the Philippines are too new for judgment. There is little credible evidence of law enforcement in Japan, Taiwan and India. Related to this, the previous 'Asian civil law model' of ministry-based Enforcement is now limited to these three 'regulatory failure' countries, plus Vietnam, and is declining. Alternatively the specialist data protection authority (DPA) model, although not necessarily an independent one, has been adopted by recent Asian legislation (Singapore, Malaysia and the Philippines), and other previous laws.[31] The most significant legislative change in asia since 2014 is that Thailand and china now have much stronger data privacy laws, with Thailand being significantly affected by the eu's 'gdpr model', and china developing what may be alternative models of its own.

1. Thailand

A military coup in 2014 imposed a junta government, which in February 2019 enacted data privacy laws to replace old and ineffective laws that only applied to the public sector. This comes three weeks before Thailand's first general election since the coup. A military-backed party now leads the coalition government, including the Prime Minister and Cabinet members from the previous military government, and a largely appointed upper house.

Thailand's Personal Data Protection Act (PDPA) will come into force on 28 May 2020, a year after its promulgation. It is based on the GDPR influence bill proposed by the junta government in May 2018, but has many differences from the bill. Only a few important points form the basis of the Act in contrast to the 2018 Bill, which takes close to the EU GDPR, or is of international significance.[32] The PDPA is a comprehensive law, unlike the private sector-specific laws in other ASEAN countries (the Philippines excluded). This exempts some parts of the private sector (credit reporting has separate laws) or the public sector (courts, legislatures, security and law enforcement), but further exceptions can be made by decree.

Data exports from Thailand may occur to countries that have an 'adequate level of protection', as defined by the PDPC. However, 'adequate' is defined by criteria set by the PDPC, so it cannot be assumed that it will mean the same as it does in the EU. Additional provisions that allow data export include the form of Binding Corporate Rules (BCR), and unspecified 'safe safeguards', both of which must be based on standards set by the PDPC. The main meaning of the Thai law is that it is the first 'GDPR-based' law that has not yet been explicitly enforced in Asia. However, there are GDPR-affected bills in India and Indonesia.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

2. China

From 2011 to 2014 China enforced five main rules and most consistent laws and regulations related to data privacy, at various levels in its complex legislative hierarchy. A number of omissions (especially the lack of subject access) mean they are close to, but do not quite comprise, the minimum requirements for data privacy laws.[33] China Cybersecurity Law's data privacy provisions 2016 are China's most comprehensive and widely applicable data privacy collection. To 2017, beyond the previous law. However, the law still misses explicit user access rights, data quality requirements and special provisions for sensitive data, also because it does not have a specialist data protection authority (DPA), and becomes an uncertain scope in relation to data protection. Public sector. The omission (or ambiguity) of the former – explicit subject access rights – means that Chinese law as a whole does not yet include one of the most fundamental elements of data privacy law.

However, these doubts are now adequately resolved. The E-Commerce Law 2018 (entered into force January 1, 2019), China's second highest legislative body, both have broad scope within the private sector, and explicitly provides that users can make 'questions' about information. Since then, there have been two further significant developments.[34] The recommended standard entitled Information Security Engineering - Personal Information Security Specification promulgated by China's National Standardization Committee/China's National Standardization Committee, and effective 1 May 2018 is an important step forward in the evolution of data privacy protection China because of its comprehensive coverage; the potential breadth of the definition of 'personal information' (perhaps broader than other Chinese law, or European law); inclusion for the first time extra protection for 'personally sensitive information'; explicit inclusion of proper access; collection minimization, and appeals against automated processing. China has yet to finalize its legislative agenda on data privacy. A 'Personal Information Protection Law' and a 'Data Security Law', are each listed separately on the work program for the current National People's Congress (NPC). .[35] It should always be remembered that China's data protection laws coexist with the Social Credit System (SCS), which is emerging as the world's most pervasive and potentially totalitarian surveillance system, but is far from being resolved.36 The relationship between SCS and legislation Data privacy laws are not clear. Two years after the Cybersecurity Law was enacted, China is still finalizing data export and data localization rules under the law.

3. Japan

Japan's data privacy laws, at the center of which is the Act on the Protection of Personal Information (PPIA) of 2003. In 2015 Japan enacted reforms to bring Japan PPIA closer to international standards, including the creation of data protection authority, the Personal Information Protection Commission (PPC), which has enforcement powers, jurisdiction over the private sector (only), and the requirement to act independently. The bill was enacted significantly stronger than previously indicated by the initial draft. Nevertheless, that principle has many drawbacks, including the narrow concept of 'personal information'; low standards for both use changes (enabling 'appropriate' related uses) and disclosure to third parties (and 'opt-out' procedures); no deletion requirement; unclear provisions on access and correction; Does

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

not provide extra protection for sensitive information; and exceptions for 'presumed impossible' businesses violate individual rights".[36]

4. Korea

Korea has a number of data privacy laws, of which the most significant is the Network Act, covering information content service providers or covering information content service providers (ICSPs), the Credit Information Act and the Personal Information Protection Act (PIPA) which covers all sectors not covered by other Laws, and has an independent DPA (PIPC), but one without adequate powers. Overall, this law remains the strongest law in Asia, and in 2014 included (though not uniformly) many elements of the 1995 Directive and some elements of the GDPR are anticipated.[37]

The problem caused by the difficulty of obtaining evidence of damages to consumers in civil redress actions following a massive data spill was addressed by the amendment of all relevant laws in 2014-15. They provide that the defendants may be required by the court to pay statutory damages of up to KRW 3 million (approximately US$3,000) for each affected user for a data breach that negligent or willful protection requirements result in data loss, theft, or leakage, without the user having to prove the actual damage caused by the breach, and for damages up to three times the actual damage to the data subject (triple damages') if the data subject can prove: willful or gross violation of the law by the handler ; that the data subject of personal information is lost, stolen, leaked, falsified, falsified or damaged due to such breach; and the actual amount of damage resulting from such a breach.

The PIPA amendment also adds a statutory indemnity provision that allows data to be subject to a claim of up to KRW 3 million (approximately US$3,000) in damages when the data subject can prove: willful error or negligence on the part of the handler, and the fact that the data subject's personal information is lost. , stolen, leaked, falsified, forged or tampered with due to intentional error or negligence. This provision is for statutory damages and fixed advance penalties required by the GDPR.

The Network Act was also amended in 2014 to ensure that ICSPs may be required by: the Korean Communications Commission (KCC) to pay administrative fines of up to 3% (previously 1%) of ICSP's annual turnover for failure to obtain prior user consent. collection and use of personal information. The Credit Information Act was also amended in 2015, and a similar PIPA amendment is currently in the legislative process.

The fine is imposed for failure in the event of failure to protect customer data, and is 60 times higher than the previous fine. Korean progressive administration imposed fines of up to 3% of turnover from 2014 onwards in advance of the European Union, and Interpark fines of US$4.5 million larger than any fines in the EU before CNIL fines against Google of 50 million euros in January 2019, now dwarfed by the UK ICO proposing July 2019 fines against British Airways (£183m) and Marriott (£99m).

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

5. Lithuania

Although with a slight delay, Lithuania adopted the new wording of the Law on Legal Protection of Personal Data on 30 June 2018 (the Law on Protection of Personal Data). Almost a year later, on 16 May 2019 the first fine of €61,500 was imposed for breach of three articles of the General Data Protection Regulation (GDPR).[38]

The last two years have been a landmark for data protection in Lithuania. In the past year the Lithuanian State Data Protection Inspectorate (the SDPI) has focused on implementing personal data protection updates. This article focuses on how Lithuania applies GDPR to the regulatory environment.

Lithuania, a member state of the European Union, has followed closely the GDPR and has not been widely used in the implementation of its national policies. Among EU members, Lithuania is an exception as it has two supervisory authorities for data processing, namely the Office of the Inspector of Journalist Ethics and the Lithuanian State Data Protection Inspectorate (SDPI). The Journalist Ethics Inspector oversees the processing of personal data for academic, artistic or literary purposes. Also investigates complaints of privacy violations in the mass media. Because SDPI monitors and ensures that the provisions of the GDPR and the Law on Protection of Private Blood are implemented and implemented properly, SDPI is the main authority in this area. However, the cooperation of two supervisors has proven effective and successful in Lithuania.

6. France

The French state has the French Law No. 2018-493 ('Amendment Act') and include the GDPR provisions in Law No. 78-17 since January 6, 1978 concerning Information Technology, Data Files, and Civil Liberties which regulates the protection of personal data. For more details, the law has been rewritten through Ordinance No. 2018-1125 of 12 December 2018 ('Ordinance 2018'), which entered into force on 1 June 2019. The French data protection authority ('CNIL') acts as France's supervisory authority and its guidelines clarify the 1978 Act.

Nearly a month after the entry into force of the GDPR, apart from the emergency enactment procedure and the submission of provisions to the Conseil Constitutionnel to ensure compliance with the French Constitution, the Amendment Act was finally amended to Law No.78-17 on the Processing of Data, Data Files and Individual Freedoms with effect receded from May 25, 2018.

Decision No. 2018-687 which determines the modalities of application and certain provisions of the Act and establishes more precisely the time period and procedural rules applicable to the mission and powers of the CNIL, other enforcement decisions are enacted to complete the adaptation of French law to European personal data protection regulations.

In particular, Decree No. 2019-536 dated May 29, 2019 was published, which is the final step to align national laws with GDPR. Implementing Decree ensures consistency of the revised 1978 Act with European regulations, defines data subject rights, adapts procedural rules prior to CNIL, repeals Decree No. 2005-1309 and above all brought into force the Act as amended

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

by Ordinance No. 2018-1125. Therefore, it is still the provisions of the Act 1978 integrating the GDPR and its decree establishing the general framework applicable to the protection of personal data in France.

7. The Netherlands

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) is EU law that came into force in 2016 and, after a two-year transitional period, became law that applies directly in all EU Member States on 25 May 2018, without requiring implementation by EU Member States through national law. A Regulation is directly applicable and has consistent effect in all Member States. However, there are still more than 50 areas covered by the GDPR where Member States are permitted to legislate different domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among Member States.[39]

In the Netherlands, the General Data Protection Regulation (GDPR) and the Dutch GDPR Implementation Act primarily regulate the processing of personal data in the Netherlands. The relevant supervisory authority is the Dutch Data Protection Authority ('AP'), which is becoming increasingly active from both a guidance and enforcement perspective. The supervisory authority for data protection in the Netherlands is the AP.64 The AP often refers to the guidelines released by the European Data Protection Board ('EDPB'), but also publishes guidelines and explanations on various topics under the GDPR and the Act.

The privacy scope of this Act is equivalent to the personal scope of the GDPR. This applies to all automated processing by private and public organizations of the personal data of directly or indirectly identifiable natural persons. The law does not apply if the data is effectively anonymized according to the GDPR and EDPB guidelines, or if the data relates to a deceased individual. However, the Act does not apply to the processing of personal data: Insofar as such processing is subject to the Personal Records Database Act, the Elections Act, or Advisory Referendums as provided for in Article 2(2) of the GDPR; By the armed forces, insofar as the Minister of Defense decides this for the purpose of deploying the armed forces or providing them with the tasks described in Article 97 of the Constitution; To the extent subject to the Intelligence and Security Services Act 2002.

CONCLUSION

The principle of liability based on fault (fault liability/liability based on fault) is Article 1365, Article 1366, and Article 1367 of the Civil Code. The presumption of liability principle that the defendant is always considered responsible until he can prove his innocence (reverse proof). The rationale of the theory of reversal of the burden of proof is that someone is considered guilty, until the person concerned can prove otherwise. This is certainly contrary to the legal principle of the presumption of innocence which is commonly known in law. However, if applied in the case of consumers will appear, such principles are quite relevant. Article 22 of the Consumer Protection Law (UUPK) confirms that the burden of proof (the presence or absence of errors) is on business actors in criminal cases of violating Article 19 paragraph (4),

ISSN 1533-9211

DOI 10.5281/zenodo.7359284

Article 20, and Article 21 of the PK Law. The second principle and is only known in a very limited scope of transactions which in common sense can be justified. The principle of Absolute Liability (strict liability) is often identified with the principle of absolute liability. The principle of Liability with Limitations is often used by business actors to limit the burden of responsibility that should be borne by them, which is generally known as the inclusion of an exoneration clause in the standard agreement they make. Criminal liability is a form of determining whether a suspect or defendant is responsible for a crime that has occurred. In other words, criminal liability is a form that determines whether a person is released or convicted. The law that protects personal data from data leakage does not yet exist so that many certain people can provide data so that data leaks occur.

SUGGESTION

It is hoped that they will comply more with Law no. 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and Government Regulation Number 82 of 2012 concerning Implementation of Electronic Systems and Transactions (PP PSTE). One can be in terms of society which is one of the main targets of the rule of law. That's why people call the factual enforceability of the law is also the effectiveness of the law. Then regarding the basis for the entry into force or validity of a rule or legal norm lies in even higher regulations or legal norms, and in the end it comes to a highest rule or norm, namely the basic norm (grundnorm/basic norm). the enactment or validity of a postulate that has been considered so basically and agreed upon by the general public, not least if the legal norms are not in line with moral values.

BIBLIOGRAPHY

- Cash, "Tokopedia, Gojek and Bukalapak data leak when the personal data protection bill was absent" (online), available at https://industri.kontan.co.id/news/data-tokopedia-gojek-dan-bukalapak- leak-at-the-absent-personal-data-protection-bill (14 May 2020).
- CNN Indonesia. cnnsocmed &utm_medium=oa&utm_source=twitter&utm_content=infog (10 September 2021).
- Leski Rizkinaswara, From January to June 2021 Kominfo Handles 447 Illegal Fintech, available at https://aptika.kominfo.go.id/2021/07/sejak-januari-until-juni-2021-kominfo-tangani-447- fintech-illegal/ (1 November 2021).
- Sinta Dewi, "The Concept of Legal Protection of Data Privacy and Personal Data Associated with the Use of Cloud Computing in Indonesia". Yustisia Journal, Vol.5, No.1, (2016).
- Wahyudi Djafar and Asep Komarudin, Protection of Right to Privacy on the Internet-Some Key Explanations, (Jakarta: Elsam, 2014), p. 2.
- Fanny Priseyllia, "Personal Data Privacy Protection from a Legal Comparative Perspective", Jatiswara Journal, Vol.34, No.3, (2019).p. 239.
- Human Rights Committee General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honor and reputation (art. 17) as cited in Privacy International Report, (2013). Thing. 1-2.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

- Psalm Septian Rumapea, "Legal Protection against Electronic Money Embezzlement in Electronic Transactions", Journal of Rule of Law, Vol.18, No.3, (2019), p. 29.
- Nadiah Tsamara, "Comparison of Privacy Protection Rules for Personal Data between Indonesia and Several Countries". Suara Hukum Journal, Vol.3, No.1, (2021). p. 55.
- Daniel J. Solove, "The Digital Person, Technology and Privacy in the Information Age", (New York: West Group Publication, New York University Press, 2004), p. 13-17.
- Herwin Sulistyowati, "Legal Analysis of Crimes in Contract Validity in the Digital Era", UNIFICATION: Journal of Legal Studies, Vol.7, No.1, (2020), p. 110.
- Angfier A.Sinaga, "Juridical Review of the Liability of Business Actors Selling Their Products with a Direct Selling System", Journal of Civil Law, Vol.4, No.1, (2013), p. 6.
- Marcy E. Peek, "Information Privacy and Corporate Power: Toward a Reimagination of Information Privacy Law", Seton Hall Law Review, Vol 37, (2018), p. 6-7.
- Tal Z. Zarsky, "Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society", University Miami Law Review, Vol 58, (2004), p. 991.
- Liberth Jemadu, Citizens' Personal Data Leaked on the Internet can be used by Terrorists, can be accessed at https://www. -Internet-can-be-used-terrorists, December 1, 2021.
- Masitoh Indriyani, "Privacy Protection and Personal Data of Online Consumers on the Online Marketplace System", Justitia Jurnal Hukum, Vol.1, No.2, (2017), p. 191.
- Sandra Wijaya "Corporate Criminal Responsibility for Providers of Web-Based Electronic Information Technology Services and Applications for Leakage of User's Personal Data" (Master's Thesis, Islamic University of Indonesia, 2020) p. 1.
- Soerjono Soekanto & Sri Mamudji, Normative Legal Research (A Brief Overview), (Jakarta: Rajawali Pers, 2001), pp.13-14.
- Muhammad Hasan Rumlus, Hanif Hartadi, Policies for Combating Personal Data Theft in Electronic Media, Human Rights Journal, Vol.11, No.2, 2020, pp.285-299.
- Tribun Timur.com, "Accused of Misuse of Data for Cpns 2019 Tryout Test Participants, Cpns Account Clarification Indonesia.Id," Tribun News .Com, last modified 2019, https://makassar.tribunnews.com/2019/06/26 / accused-misuse-data-participant-tryout-test cpns-2019 this-cpns-account-cpnsindonesiaid.
- "70 Thousand Photos of Female Tinder Users Leaked In Cyber Crime Forum," KATADATA. CO.ID, https://katadata.co.id/berita/2020/01/21/70-ribu-foto-user-tinder-perempuan-bocor-in forumkejahan-siber.
- Oktarina Paramitha, 12 Data Leakage Cases in Indonesia Since 2019, https://cyberthreat.id/read/12752/12-Kasus-Kebocoran-Data-di-Indonesia-Sejak-2019 accessed on 08 April 2022.
- Mochamad Januar Rizki, KPAI Leaking Complaint Database, Urgency of Protecting Children's Personal Data. Link: https://www. Hukumonline.com/berita/a/database-pengaduan-kpai-bocor--urgensi-perlindungan-data-private-anak-lt61727bae9f8e8 accessed on April 8, 2022.
- Achmad Jatnika, Alleged Leaking of Patient Data Managed by the Ministry of Health, Here's the Response of the Ministry of Communication and Information, https://nasional.kontan.co.id/news/dugaan-kebocoran-data-patient-yang-dikelola-kemenkes-begini-respons-kemkominfo accessed on 08 April 2022.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7359284

- Liputan 6, Types of Data of Pertamina Job Applicants allegedly leaked on the hacker forum, nhttps://www.liputan6.com/tekno/read/4856633/tipe-data-pelamar-kerja-pertamina-yang-diduga-bocor- in-forum-hacker accessed on 08 April 2022.
- Law Number 14 of 2008 concerning Public Information Disclosure.
- Fariaman Laia, "Juridical Analysis of Legal Protection for Criminal Justice Witnesses in Indonesia, Journal of Arrow Justice", Vol.1, No.2, (2022), p. 28-42.
- Rena Yulia, Victimology, (Yogyakarta: Graha Ilmu, 2010), p. 58.
- Veronica Novinna, "Consumer Protection from the Dissemination of Personal Data by Third Parties: The Fintech Peer to Peer Lending Case", Journal of Masters in Law Udayana, Vol.9, No.1, (2020), p. 92-110.
- Ardiana Hidayah, "Legal Aspects of E-Commerce Consumer Data Protection", Cosmic Journal of Law, Vol.20, No.1, 2020, p. 56-63.
- Graham Greenleaf, "Asia's Data Privacy Dilemmas 2014-19: National diversity, cross-border gridlock", Revista PDP, No.4, (2019), p. 49-73.
- Op.Cit, Graham Greenleaf, "Asia's Data Privacy.., p.52.
- G Greenleaf and S Livingston 'China's Cybersecurity Law – also a data privacy law?' Privacy Laws & Business International Report, No.144, (2016), p. 1-7
- Article 24 of the E-Commerce Law "Where e-business operators receive an application for inquiry, modification, or deletion of user information, they must immediately investigate, or modify or delete user information, after verification of identity".
- NPC Observer https://npcobserver.com/2018/09/07/translation-13th-npc-standing-committee-five-year-legislative-plan/
- For an authoritative assessment, see R. Creemers 'China's Social Credit System: An Evolving Practice of Control' (2018) <https://ssrn.com/abstract=3175792 or http://dx.doi.org/10.2139/ ssrn.3175792>;
- Graham Green Leaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives, United Kingdom: Oxford University Press, 2014, p. 124. Access: https://books.google.co.id/books?id=0eAuBQAAQBAJ&pg=PA125&lpg =PA125&dq=See + Greenleaf, +Asian + Data + Privacy + Laws, +Ch.
- Graham Greenleaf, Japan and Korea: Different Paths to EU Adequacy, No. 156, Privacy and Business International Report, (2019). Pp.9-11.
- DLA Piper, Data Protection Laws of the World-Netherlands, www.dlapiperdataprotection.com