International Conference Restructuring and
Transforming Law 2025
Volume 3, Issue 2, Maret 2025
e-ISSN : 2963-931X
icrtlaw@ums.ac.id

LEGAL REGULATIONS REGARDING CYBERSECURITY AND CORPORATE LEGAL LIABILITY IN CASES OF CORPORATE DATA LEAKAGE IN INDONESIA

Elvrida Mutiara Singgih

Law Study Program, Faculty of Law, Universitas Muhammadiyah Surakarta

C100200081@student.ums.ac.id

Diana Setiawati

Law Study Program, Faculty of Law, Universitas Muhammadiyah Surakarta

Ds170@ums.ac.id

ABSTRACT

This research discusses criminal law enforcement against current information technology in overcoming cyber crime, and to find out legal liability related to cases of company data leakage in Indonesia. This research uses a normative approach. This research uses main data and additional data. The data collection technique in this research uses literature study, while the analysis technique used in this research uses qualitative analysis. The results of this study are in the form of criminal law enforcement policies against current information technology in overcoming cyber crime, in overcoming cyber crime regulated in Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions Article 27 to Article 31. Then legal liability related to cases of corporate data leaks in Indonesia, regulated in the Personal Data Protection Law which regulates data protection.

Keywords: Cyber Crime, Data Protection, Personal Data Protection Law.

INTRODUCTION

The advancement of information technology in the current era is growing increasingly rapidly, this phenomenon develops in various aspects of life side by side with society. The rapid development of technology has an impact on the existence of new technology in the form of internet media and can cause the relationship between the world to be unlimited and internet media can cause social, economic and cultural changes on an ongoing basis. But besides that, technology can bring positive and negative effects to life, the positive impact caused by internet technology is that people can use internet technology to communicate with other people

without restrictions by chatting via online, online shooping shopping, Cyber Bank, online business, m-banking and others. However, on the other hand, the negative effects arising from technological developments are also very large, for example, crime in the online world or other terms cyber crime.(1) The dynamics caused by the development of information and the development of communication around society in addition to bringing good influence also brings negative influence due to the gaps in use that lead to crime, the term is called cyber crime or crime in online sites.(2)

The biggest cyber threats target large companies and government institutions. One of the cyber crime cases that occurred in Indonesia was the leak of job applicant data at PT Pertamina Training & Consulting with more than 163,000 data, the leak allegedly occurred in 2022. PT Pertamina Training & Consulting data leakage was carried out by a member of the raid online forum with an account named *"Astarte".* Information on prospective workers' data comes from Pertamina's PTC website and is not traded but seized for free."(3)

According to the leaker, 163,181 files with a data size of up to 60 GB were successfully shared. The 60 GB of information is separated into 12 connections, through which personal information belonging to PTC Pertamina applicants can be downloaded for free. The data contains the applicant's identity, starting with full name, address, place of birth, title, religion, and mobile phone number (telephone), besides that the Astarte account also includes data on identity cards, family cards, BPJS cards, school diplomas, academic transcripts and others. Based on the laws and regulations, the cyber crime case described has violated the Electronic Information and Transaction Law Article 32 paragraph (1), (2), and (3) that in the article explains the prohibition in the act of transferring personal data belonging to others without the permission of the relevant party. In Article 32 of the Electronic Information and Transaction Law, anyone who violates it will get a criminal penalty, even though the case above the data obtained was leaked free of charge or free of charge, the case still violates the laws and regulations, because the data collection was carried out without the permission of the relevant party.

Cyber crime cases in Indonesia today must certainly get special attention from law enforcement officials, in order to reduce crime in cyberspace that disturbs the community. These crimes, if

not handled immediately, will cause impacts from various aspects. The government has initiated regulations regarding cyber crime as many argue that the Criminal Code does not sufficiently cover cyber crime. The document includes Law No 19 of 2016 on the amendment of Law No 11 of 2008. However, on the other hand, the imposition of punishment in the perpetrators of cyber crime in the implementation statement is not appropriate and inappropriate. This phenomenon occurs because of the intersection between the perpetrators and the rules of prisoner development in correctional institutions. The laws and regulations made which aim to reduce criminalization are not implemented properly. There are crimes of supervision or social work that replace punishment. There are still many phenomena of lawlessness in cyberspace at this time, and the parties involved suffer great losses from the impact obtained.(4)

If examined from the point of view of tackling online crime cases, in dealing with cyber crime cases that occur in Indonesia criminal law has several aspects in encouraging these regulations, these aspects consist of aspects of the responsibility of the apparatus in criminal cases and punishment which are included in aspects of evidence, aspects of criminalization, and judicial aspects. It is explained that the criminalization aspect is a policy in which it regulates a criminal act. Therefore, the nature of the criminal policy on Electronic Information and Transactions is part of the criminal policy and by using the means provided by the criminal. This is included in the formulation or legislation policy. Thus, to overcome cases of data leakage that occur in government agencies or companies the role of the law is needed in its responsibility in protecting public data so that it does not leak and is not used by irresponsible individuals.(5)

Based on the description of the problem above, the researcher wants to examine: 1. How is the current criminal law enforcement policy on information technology in overcoming cyber crime? 2. How is legal liability related to cases of company data leakage in Indonesia?

METHOD

This research design is about legal regulations regarding cybersecurity and corporate legal liability in cases of corporate data leakages in Indonesia. This research uses normative law, normative law is an approach that is carried out by analyzing the laws and regulations related to the problems being discussed. (6) The sources in this research come from books, the internet,

and literature. The main data sources in this research come from legislation. (7) The main data sources used in this research are the 1945 Constitution, Criminal Code, Law No. 27 of 2022 on Personal Data Protection, and Law on Electronic Information and Transactions No. 19 of 2016. Supporting data sources used are law books, legal principles, legal journals, previous research results, as well as the views of experts and doctrines. The data collection technique in this research uses literature study, namely by collecting legal materials such as collecting primary and secondary materials. (8) While the analysis technique used in this research uses qualitative analysis which is carried out through interpretation of legal materials. (9)

RESULTS AND DISCUSSION

Current Criminal Law Enforcement Policy Against Information Technology in Overcoming Cyber Crime

Cyber crime is a cyber crime that is on the rise, cyber crime is very troubling to anyone, be it the community or government agencies and companies. Therefore, enforcement policies in Indonesia should be tightened in order to reduce cyber crime. The term enforcement is a common basis that functions as a guide for the government in an effort to prosper its people and prioritize the common interest, phenomena that occur in society or obstacles in the management of central regulations that must be addressed so that law enforcement in Indonesia is carried out properly and without any obstacles that occur.(10)

To prevent criminal law from becoming a social problem, criminal law is an important part of Indonesia's political policy. The main system of legislation is the Criminal Procedure Code, the main foundation of which is the Criminal Code.(11)

In sociology, the Electronic Information and Transaction Law is needed by the community to enact regulations that govern people's lives, previously there were no specific regulations governing information technology. On the contrary, the law only slightly regulates information technology and does not discuss actions that are considered crimes against technology. In addition to meeting philosophical standards, the Electronic Information and Transaction Law also meets social standards. The philosophical foundation of the Electronic Information and Transaction Law is found in Article 28F of the 1945 Constitution which states that "Everyone

has the right to seek, obtain, possess, store, process, and convey information using all available channels".

The act of cyber crime is regulated in the Electronic Information and Transaction Law No. 19 of 2016 on the amendment of Law No. 11 of 2008 on Electronic Information and Transactions, that the contents contained in the Electronic Information and Transaction Law No. 19 of 2016 on the amendment of Law No. 11 of 2008 on Electronic Information and Transactions contain prohibitions that should not be performed, the prohibition is regulated in:

1. Article 27

a. Actions that violate decency contained in Article 27 paragraph (1) which explains that "Every person intentionally and without the right to distribute and or transmit and / or make accessible Electronic Information and / or Electronic Documents that have content that violates decency", but the Article does not explain the actions that have been taken.

b. Article 27 paragraph (2), states that "Every person intentionally and without the right to distribute and/or transmit and/or electronic documents and/or electronic documents that have gambling content."

c. Article 27 paragraph (3), which states that "Every person intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information that contains insults and/or defamation."

d. Article 27 paragraph (4), which states that "Every person intentionally and without right distributes and/or transmits and/or makes accessible electronic information and/or electronic documents that contain extortion and/or threats."

Violation of decency is expressly prohibited in Article 27. If you violate Article 27, you will be fined a maximum of IDR 1,000,000,000.00 or imprisonment for a maximum of 6 (six years). In this article it is strongly emphasized that we should not, steal, distribute personal data belonging to others because this is deviant and unlawful behavior.

2. Article 28

a. Article 28 paragraph (1) "Every person intentionally and without the right to spread false and misleading news that results in consumer harm in electronic transactions."

b. Article 28 paragraph (2) "Every person intentionally and without the right to disseminate information aimed at creating a sense of hatred or hostility of individuals and/or certain community groups based on ethnicity, religion, race and intergroup (sara)."

Article 28 is used in cases with hate speech, such as in the view of ethnicity, religion, race, and intergroup, basically the act of people who spread insults against other people, religions, races, and cultures will be subject to imprisonment for a maximum of six years and a maximum fine of IDR 1,000,000,000.00.

3. Article 29

"Every person intentionally and without the right to send electronic information and/or electronic documents containing threats of violence or fear that are personally directed."

Article 29 contains the threat of violence, for criminal offenders who have violated will be subject to imprisonment of four years and a maximum fine of IDR 750,000,000.00.

4. Article 30

a. Article 30 paragraph (1) explains that "Every person intentionally and without right or unlawfully accesses another person's computer and/or electronic system by any means."

b. Article 30 paragraph (2) explains that "Every person intentionally and without rights or unlawfully accesses a computer and/or electronic system by any means with the aim of obtaining electronic information and/or electronic documents."

Article 30 contains data hacking carried out by hackers, then someone who violates Article 30 will be punished with a maximum fine of IDR 600,000,000.00 and imprisonment of six years.

5. Article 31

a. Article 31 paragraph (1), explains that "Every person intentionally and unlawfully intercepts or taps certain electronic information and/or electronic systems belonging to another person."

b. Article 31 paragraph (2), explains that "Every person and without the right against the law intercepts electronic transmissions and/or electronic documents that are not public from, to, and within a computer and/or electronic system belonging to another person, both those that do not cause any changes and those that cause changes, deletions, and/or termination of electronic information and/or electronic documents that are being transmitted."

Article 31 regulates the misuse of electronic goods or the tapping of other people's property. Wiretapping is an act of lawbreaking including criminal offenses and fines.

The researcher's analysis that cyber crime is a crime that occurs in cyberspace, cyber crime is very detrimental to related parties. With the existence of cyber crime, many people are worried, one example of cyber crime is data hacking. Data hacking often occurs in the digital world, which causes many people to experience data leakages. In these cases, of course, law enforcement must be alert in overcoming these crimes, so as not to have an impact on all aspects of life. Therefore, law enforcement policies in overcoming cyber crime have been regulated in legislation in which there are prohibitions that should not be done in cyberspace. The Law on Electronic Information and Transactions No. 19 of 2016 explains that there are prohibitions on immoral acts in electronic media, distribution of documents containing gambling, defamation, threats, spreading false news, hacking, etc. In every act that violates the articles of the Law on Electronic Information and Transactions. In every act that violates the articles of the Electronic Information and Transaction Law No. 19 of 2016, criminal sanctions and fines will be imposed.

A. **Legal Liability Related to Data Leakage Cases in Indonesian Companies**

Indonesia in the current era is facing a serious phenomenon related to data leakage cases due to the rapid development of information technology. Therefore, the law must try to overcome the impact of technology, so as not to harm the State. The impact of technology is very influential on company performance, therefore companies and government agencies must continue to provide special security so that cyber crime cases do not attack companies and government agencies.

E-commerce business actors can be considered as personal data controllers under Law No. 27 of 2022 on Personal Data Protection. Therefore, individuals have legal responsibility for the handling of personal information in their possession and have reached the arrangements contained in the Personal Data Protection Regulation. Therefore, Article 2 paragraph 1 of the Personal Data Protection Regulation sets standards that apply to everyone. According to Article 2 paragraph 2 of the Personal Data Protection Law, what is meant by "Personal activities" or "Household activities" are basically activities that are personal, non-commercial, and non-professional in the private sphere. The exception of this article is one way to maintain human rights, especially the right to privacy guaranteed by Article 28G paragraph 1 of the 1945

Constitution that Individuals who have processed personal data as long as it is used for personal or household activities are considered as personal data controllers under the Personal Data Protection Law, unless the individual in other words, according to the Personal Data Protection Law, the individual is not responsible or obliged to act as a personal data controller. The Personal Data Protection Law is indispensable in maintaining the privacy of data in companies and government agencies.

In overcoming data leakage in the company, procedures and implementation are provided, which include trust supported by the integrity of Human Resource, how to overcome data leakage is as follows

a. Develop a Safety Policy
b. Control the content in E-mail
c. Protection with data security applications
d. Enhance data security

In addition, the form of company liability for personal data leakage if based on consumer law there are several responsibilities:

a. Customer losses arising from labor errors and faulty products delivered or exchanged shall be borne by the business.
b. Businesses that advertise are responsible for the advertisement itself and everything it produces.
c. If the distributing business or the representative of a foreign producer is unable to import the goods, the importer shall be liable as the producer of the imported goods.
d. Demonstrating the existence of a misconduct component in an offender case is a burden and obligation on the employer so as not to foreclose the opportunity for the examiner to still provide evidence.

Businesses are obliged to comply with the applicable standardization guidelines in the implementing regulations of public authorities that serve as a reference in making best efforts and in accordance with the nature of their specialist organizations. Organizers are essentially responsible for all the impacts of others, but they can be indicators of best practice. As with good accountability, when viewed from the existence of a commitment, accountability

can be divided into two groups, namely (a). Responsibility before the occurrence of the phenomenon, (b). Accountability after the event.

Article 26 of the Electronic Information and Transaction Regulations states that any person who commits theft of personal data without consent shall be prosecuted. However, a breach of personal data information security may be prosecuted as an unlawful criminal offense based on its commission in view of the provisions of Article 1365 of the Civil Code, or under Article 1366 of the Civil Code.

Article 3 of the Electronic Information and Transaction Law, also explains that implementing every electronic system implementation, both private and government, must adhere to the precautionary principle and ensure the accountability of electronic systems that are reliable, safe, and accountable.

CONCLUSION

From the descriptions that have been presented above, the researcher concludes that:

a. Cyber crime is currently regulated in Article 27 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. He explained that cyber crime is a cybercrime that is on the rise, cyber crime is very troubling to anyone, be it the community or government agencies and companies. Therefore, enforcement policies in Indonesia should be tightened in order to reduce cyber crime.

b. Legal Liability Related to Data Leakage Cases in Indonesian Companies, According to Law No. 27 of 2022 on Personal Data Protection, e-commerce business actors can be considered as personal data controllers. So individuals have legal responsibility for the handling of personal information in their possession and fulfill the arrangements contained in the Personal Data Protection Regulation. Therefore, Article 2 paragraph 1 of the Personal Data Protection Law sets standards that apply to everyone. The provision in Article 2 paragraph (2) of the Personal Data Protection Law states that “Individual activities” or “Household activities” have the main training in confidential circles that are personal, not business, and not expertise.

REFERENCES

1. Setiawan D. Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Budaya. J SIMBOLIKA Res Learn Commun Study. 2018;4(1):62.
2. Ersya MP. Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. J Moral Civ Educ [Internet]. 2017;50–62. Available from: https://www.researchgate.net/profile/Jmce-Unp 2/publication/328886042_Permasalahan_Hukum_dalam_Menanggulangi_Cyber_Crime_di_Indonesia/links/5be971284585150b2bb09cc7/Permasalahan-Hukum-dalam-Menanggulangi-Cyber-Crime-di-Indonesia.pdf
3. Utin Indah Permata Sari. Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. J Stud Leg. 2022;2(01):58–77.
4. Lana A. Dampak Kejahatan Siber Terhadap Teknologi Informasi Dan Pengendalian Internal. Sos dan Pendidik. 2021;1(3):1–13.
5. Oksidelfa Yanto. Pemindahan atas Kejahatan yang Berhubungan dengan Teknologi Informasi. Yogyakarta: Penerbit Samudra Biru (Anggota IKAPI; 2021. hlm 16.
6. Soekanto S. Pengantar Penelitian Hukum. Jakarta: Universitas Indonesia Press; 2012.
7. Soekanto S. Pengantar Penelitian Hukum Jakarta. Jakarta: Universitas Indonesia Press; 2012.
8. Meray Hendrik Mezak. Metode dan Pendekatan Dalam Penelitian Hukum. Law Rev. 2006;Vol 5 No 3.
9. Soekanto S. Pengantar Penelitian Hukum. In: UI-Press, editor. pengantar Penelitian Hukum. Jakarta; 2010. p. 277.
10. Aldriano MA, Priyambodo MA. Cyber Crime Dalam Sudut Pandang Hukum Pidana. J Kewarganegaraan. 2022;6(1):2.
11. Mudadi & Barda Nawawi. Teori-Teori dan Kebijakan Pidana. Bandung: PT Alumni; 2010.