Corporate Criminal Liability Telecommunication Company Against Consumer Personal Information Data Leakage in Indonesia

Sumartini Dewi(✉) and Sri Wulandari

Universitas 17 Agustus 1945 Semarang, Semarang, Indonesia
sumartini.dewi@gmail.com

Abstract. In the digital era like today, personal data has its own urgency to get protection for its security. The number of cases of personal information data leakage, shows that current personal information data could be a "commodity" to be traded. It is possible that cases of personal information data leakage can occur in the scope of telecommunication companies in Indonesia. This is because telecommunications service companies in Indonesia have a large database of consumer personal information. This study aims to find out what is meant by personal information data and how is the corporate criminal liability of telecommunications companies if there is a leak of personal information data belonging to its customers. This article is a literature study using a normative juridical approach. The definition of personal data, although there is no law in Indonesia that provides a specific legal definition, is certain personal data that is stored, maintained, kept true and protected by confidentiality. Indonesia still does not have a law that specifically regulates the legal protection of personal information data comprehensively.

Keywords: Personal Information Data · ITE Law · Corporate Responsibility · Criminal Law

1 Introduction

In the current era of digitalization there has been a wave of major changes in people's personal and work lives by creating opportunities for innovative business models and lifestyles. With the shift in the types of basic human needs, telecommunication services have become one of the main human needs in almost all over the world. All humans in the world today rely a lot on the need for information services from telecommunications technology which is increasingly developing rapidly.

These significant changes have brought positive as well as negative impacts for every individual involved. Examples of potential negatives from digital transformation that can arise include misuse of information data, cyber attacks and other new crimes. As a result, innovative technology actually brings new social problems and higher responsibilities, especially for companies or corporations. Especially for corporations engaged in telecommunications services.

A. Endah Kusumaningrum et al. (Eds.): ICLEH 2022, ASSEHR 723, pp. 198–209, 2023.
https://doi.org/10.2991/978-2-38476-024-4_23

A corporation is an association or organization in the form of a legal entity that has a physical structure, personality and is a legal creation, so by its creation, its death is determined by law [1]. As an entity whose birth and death are determined by law, all types of activities, both internal and external, are also determined by law. Through a legal product issued by the Ministry of Communication and Information of the Republic of Indonesia, the Telecommunications Law number 36 of 1999 has become the legal umbrella for companies engaged in providing telecommunications services in Indonesia. Currently, there are 5 (five) cellular operator legal entities legally registered with the Ministry of Communication and Informatics, including: PT. Cellular Telecommunications, PT XL-Axiata Tbk, PT. Indosat Tbk, PT Smartfren Telecom Tbk, and PT Smart Telecom [2]. Meanwhile, the Central Statistics Agency (BPS) noted that there were 959 new companies that had received permits to provide telecommunications services in Indonesia in 2020 [3].

In 2020, the Ministry of Communication and Informatics revealed that there were indications of leakage of personal data of telecommunication company customers or cellular operators [4]. Protection of customer data in telecommunications service companies or cellular operators in Indonesia has been regulated in the Minister of Communication and Informatics Regulation (Permenkominfo) Number 12 of 2016 concerning Registration of Telecommunications Service Customers. In the regulation, it has been explained that mobile cellular network operators are required to keep the data and/or identity of customers confidential. These telecommunications companies must also have ISO 27001 certification for information security in managing customer data.

Data security or customer identity is one of the rights protected by the constitution. However, the right to protection of the privacy of information or the security of personal data in Indonesia has not become a priority at this time. It is proven that until now there is still a lot of misuse of customer personal information data, including for business purposes. There is still a lot of customer information data that becomes a buying and selling commodity on the internet [5]. Many consumers from telecommunications service users are starting to get disturbed and complain about the leakage of personal data.

The case of leakage of personal data in the cyber world is not only stalking consumers of telecommunication services, with the changing business models and innovations of current service providers, leakage of customer data in Indonesia can occur in various companies that use the collection of customer personal data as one of the conditions for transactions in their companies.. At the end of 2020, it was revealed that the hotel service provider, RedDoorz, sold 5.8 million customer data for 2000 US dollars or around Rp. 28.2 million rupiah [6]. In addition, the e-commerce company Tokopedia has also sold 91 million user data [7]. The leaked personal data are names, email addresses, numeric passwords to customer biometric data (fingerprints to facial recognition data). This is also experienced by Telkomsel consumers whose personal data is spread on social media. Denny Siregar, a social media activist, admitted that his personal data had been distributed illegally on Twitter social media. His personal data was spread through a screenshot of the Telkomsel provider system which was then shared illegally via Twitter. This proves that there is a big chance of leakage of personal data of telecommunication company customers in Indonesia.

From the explanation above, the author understands the urgency of the discussion of this article, that there are no scientific articles that discuss the protection of personal information data of company customers and how the corporate criminal liability of telecommunications companies occurs in the event of leakage of personal information data of customers. The purpose of writing the article is to know the definition of personal data and to find out how the form of corporate criminal liability for telecommunications companies occurs in the event of a leak of customer data. The author will review this in an article with the title "Corporate Criminal Liability of Telecommunication Companies Against Leaking of Consumer Information Data in Indonesia."

2 Research Method

The article that the author has compiled uses a normative juridical approach. In this article, the method used uses library materials or secondary data as the basic material for study by conducting a search on regulations and literature related to the problems studied [8]. The legal materials used in this article consist of primary and secondary legal materials. Primary legal materials consist of statutory regulations, official records or treatises related to this study. While secondary legal materials are related to legal materials that provide clarification to primary legal materials, such as books, literature, articles, papers and other materials taken from legal experts.

3 Findings and Discussion

1. Definition of Personal Information Data.
   Based on the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 Article 1 paragraph (1), personal information data is defined as certain individual data that is stored, maintained, and kept true and protected by confidentiality [9]. Whereas in the Personal Data Protection Bill, the definition of personal data is any certain data about a person's life either identified and/or can be identified separately or combined with other information directly or indirectly through electronic or non-electronic systems [10].

   In the bill, personal data is then classified into two types, general data and specific data. General personal data includes full name, gender, nationality, religion, and/or other personal data which is combined so as to identify a person. Furthermore, specific personal data is personal data that describes certain conditions of the owner, such as health information data, biometric records, genetic data, political views, criminal records, data regarding children, personal financial data and other data in accordance with the laws and regulations.

   The definition of personal data is also explained in the international rules of The Data Protection Act 1998 (DPA) in the second article, namely as a collection of information that can identify a person directly or indirectly. From the definition stated in the DPA, information data can consist of a collection of information that clearly identifies a person's personality as well as information data that can be used as a guide to identify someone's personality. DPA further explains the further context

of the definition of personal data above if the information is obtained from archiving activities involving automatic or non-automatic data archiving systems.

In DPA, personal data information is categorized into two types. Information obtained from the process of electronic systems and information obtained from manual processes in the filing system. The intended information data is both data used for the identification process and data that clearly describes a person's personal information.

Positive law in Indonesia has attempted to translate the definition of personal information data into several of its legal products. Law No. 8 of 2008 concerning Electronic Transaction Information interprets personal data as part of personal rights (privacy rights) in Article 26 paragraph (1) [10]. While in PP No. 82 of 2012 concerning Electronic System and Transaction Operators provides a definition of personal data as certain individual data that is stored, maintained, kept its truth and confidentiality protected.

2. Personal Information Data Protection Regulations

The process of collecting personal information in the filing system is now completely done electronically. This is one of the consequences of the digital revolution that creates innovations in obtaining, storing, manipulating and transmitting large amounts of data in real time, extensive and complex [11]. The digital revolution has brought a revolution in processing large volumes of data or what is known as "Big Data" [12]. Big Data processing is used by applying complex analysis techniques and cross-data to develop artificial intelligence systems and insights [13].

Data processing through Big Data systems raises special attention related to more sensitive information related to a person's personality. Sensitive information is one part of a person's right to privacy that deserves protection [14]. Therefore, special legal rules are needed that provide a protection space for the right to privacy of personal information that is in digital information systems as it is today.

The legal protection of personal data is increasingly evolving with the development of information technology. Data protection refers to practices, protections and binding legal rules aimed at protecting personal information data and ensuring that data owners can still control the information they have [15]. In other words, the data subject can decide absolutely whether they want to share some information or not, who can access the information, for how long or for what purposes the information is needed by other parties. Therefore, legal protection of personal information data must apply to automatic data processing as well as manual data processing. Laws or legal products to protect a person's privacy with respect to their personal data must include all data processing on computer, phones, IoT devices (Internet Of Things), as a paper document. This also applies to public (government) and private organizations.

In Indonesia, awareness of the security of personal information data is still low, this can be seen from the habit of Indonesian people easily providing information related to themselves such as name, residential address, occupation to monthly income to other people, who do not even have any interest in the information submitted. Even so, the Indonesian government has guaranteed the right to privacy of its citizens. The provisions related to ensuring the protection of personal data set out in Article 28G, paragraph (1) of the 1945 Constitution stipulate that everyone has

the right to protection of person, family, honor and dignity and property under their control, and have a right to a sense of security. To be safe and protected from the threat of fear to do or not to do something is a human right. In addition to defending the constitution, Indonesia is also a party to the International Covenant on Civil and Political Rights (ICCPR), which has been ratified through Law no. 12/2005, also affirms the obligation of the Indonesian government to protect the privacy and personal data of its citizens [16].

This is also consistent with the Human Rights Act No. 39 of 1999 in Section 14 (2), Section 29 (1) and Section 31. Section 29 (1) (1) provides for the recognition of everyone's right to protection. Protect your privacy. Right to self, family, honor, dignity and property. This safety applies now no longer most effective to direct relationships, however additionally to non-public data and data. Article 14(2) states that one of the rights to self-development is the right to seek, collect, store, process and transmit information using any kind of means. Facilities available. This relates to Section 31 of the Human Rights Act, which states that confidentiality of communications by electronic means shall be guaranteed unless ordered by a judge or other judicial authority as required by law. According to law.

Although Indonesia does not yet have legal products that legally and specifically regulate the protection of the personal data of its citizens, several legal products published have links or there are materials related to personal data (protection, collection, processing, use, disclosure of data). Personal). The author will summarize it into several sectors: Telecommunications and computing, population and records, finance/banking/taxation, commerce and industry, health services, security and policy.

In the telecommunications and informatics sector, Telecommunications Act No. 36 of 1999 has provided protection for the privacy concerns the security of one's Personal information and contact information. The protection is intended specifically against acts of wiretapping. i. However, in this rule, telecommunications operators are given the authority to record telecommunications, on the grounds of proving the correct use telecommunications utilities at the request of telecommunications service users. This means that telecommunications service providers are authorized to provide information about their consumer conversations to anyone as long as they are users of telecommunications services.

The Electronic Information and Transactions Act No. 11 of 2008 begins to provide protection of personal data in a broader area. Article 26, paragraphs 1 and 2, stipulates that the consent of the data owner must be obtained when transferring the personal data of an individual (prohibition of arbitrary transfer of personal data). If the personal data of an individual is voluntarily transmitted, the owner of the personal data can file a claim for damages in court. However, this has its weaknesses. In other words, evidence procedures in Indonesian civil courts make it difficult for data owners to file legal challenges against the loss of personal data.

The difficulty of proving this has been experienced in the case of a lawsuit by a group of people in Indonesia against Facebook, the world's largest social media company, in the Cambridge Analytica case [17]. Following Mario Costeja's 2014 European Court of Justice (ECJ) decision, which also influenced the 2016 amendments to the ITE Act, the right to be forgotten clause was created. According to

DPR members, Indonesia has also adopted the concept of the right to be forgotten. This proposal was subsequently incorporated into Article 26(3) of Law No. 19/2016 amending Law No. 11/2008 on ITE. It states that operators of electronic systems have a duty to keep unrelated electronic information and/or electronic documents under control. Pursuant to a court order and at the request of the data subject to erase his control.

In its implementation, regulations on the protection of personal data relating to the operation of electronic systems, including communications and informatics, are formulated in PP No. 82/2012 and many Permenkominfo. Beginning of this paper. Part of the relevant Permenkominfo, for example Permenkominfo No. 20/2016 on the protection of personal data in electronic systems, Permenkominfo No. 21/2017 on his second amendment of Permenkominfo No. 12/2016 on registration of telecommunications service customers. Protection of personal data according to the Permenkominfo, in the ministerial regulation the protection of the process: acquisition and collection; processing and analysis; storage; appearance, announcement, delivery, dissemination, and/or opening of access; and destruction of personal data [18].

This Permenkominfo provides two years (transition period) for operators of electronic systems to adjust their various personal data protection obligations. However, in fact, two years after his order from the Minister of Communications and Information, the majority of electronic system operators in Indonesia are not fully compliant with the personal data protection obligations regulated by the Minister of Communications and Information. Not. Again, regulations that are only at the level of ministerial decrees and that threaten sanctions only in the form of administrative sanctions are considered less binding and obligatory for operators of electronic systems.

3. Telecommunication Company's Corporate Criminal Liability Against Leakage of Customer's Personal Information Data.

Criminal responsibility is actually not only a question of legal issues, but also questions about values, norms and morality or general decency adopted by a community group. This needs to be done in order to achieve the principle of justice. Roeslan Saleh defines criminal responsibility as the continuation of objective reproaches that exist in a criminal act and subjectively fulfills the requirements to be convicted for the act [19].

In criminal responsibility, the meaning of the burden of criminal responsibility is imposed on the perpetrators of criminal offenses related to the basis for imposing criminal sanctions. A person will have a responsible nature if a thing or act committed by him is against the law. Chairul Huda said that the existence of a crime was based on the principle of legality. Means that a person can be subject to a criminal if there is an element of error and contrary to the law [20]. If the law uses the word error/omission as part, there are three components that can determine whether an act can be subject to criminal responsibility or not, including: unlawful acts, reckless/negligent acts, the maker can be blamed (can be held accountable for his mistakes or negligence).

In determining that a corporation can be subject to criminal liability, the corporation must be proven to have committed an act that is prohibited and has an error. This means that it must be ensured that corporate criminal acts are used as a theoretical basis to determine whether or not a corporation is wrong. It is important to note that based on the traditional view of the Criminal Code, which is still dominant to this

day, it is still influenced by the principle of "*societas delinquere non-potest*", as a result it is impossible for corporations to have faults with themselves because they do not have a "heart".

A corporation cannot commit a crime without going through an intermediary, both based on the theory of functional actors and identification theory, so the determination of the corporation's fault is to examine whether the management acting for and on behalf of the corporation has an error. if this is later found, the corporation can be found guilty of the crime it has committed. This was also explained by Mardjono Reksodiputro that the errors contained in the management could be transferred to the corporation's own fault [21].

Based on the principle of absolute liability (Strict Liability) related to the criminal liability of the telecommunications service provider corporation for the leakage of user data, it allows the emergence of urgency and can be applied in efforts to overcome criminal acts committed by corporations as a form of corporate responsibility in the settlement of criminal cases in court. Until now, the regulation of corporate responsibility that uses the principle of strict liability is only limited to the arrangements contained in Law Number 32 of 2009 concerning Environmental Protection and Management, but its implementation in the field has not been fully in accordance with what is expected [22]. Meanwhile, in the case of a telecommunications service provider corporation that is proven to have committed an unlawful act that resulted in the leakage of its customer's personal information data, it can only be subject to administrative sanctions, as stipulated in the Regulation of the Minister of Communication and Information Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems.

The Ministerial Regulation only contains provisions for administrative sanctions if there is a loss due to the failure of personal data protection carried out by a business entity, with efforts to resolve deliberations or through alternative settlements, if it is not completed it is allowed to file a civil lawsuit and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions in court and also subject to administrative sanctions. However, this does not eliminate criminal responsibility. Furthermore, in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions in criminal provisions, corporations are not touched to be criminally responsible, because they are limited to the provisions of Articles 27 to 37 as contained in Article 52 paragraph (4). Telecommunication service provider corporations for leaks of user's personal data cannot be held criminally responsible based on the three laws and regulations above.

In the implementation of corporate criminal responsibility, there are obstacles due to the difficulty of proving the perpetrators of the crime, in this case the corporation itself. As non-state actors, corporations have impunity, namely immunity from the law for the various crimes they have committed so that even though they commit crimes there is no attempt to process corporations with criminal law to the fullest.

This results in if later found cases of leakage of personal information data belonging to customers using telecommunications services, then the criminal liability of the telecommunications service provider corporations will encounter obstacles in the criminal liability process. In its implementation, law enforcement must be able to

determine who is responsible for the leakage of personal information data, whether the management, control holder of the corporation or the corporation directly.

The author has the opinion that the obstacles that will be encountered in the process of investigation, investigation, and proof in criminal acts of telecommunications service providers corporations will be as difficult as handling cyber crimes in Indonesia. That's because the problem regarding the locus delicti (the crime scene), in cyber crime investigators can find difficulties in determining the accurate location or place of the crime. The problem with the tempus delicti (time of the crime), investigators cannot determine when the crime occurred precisely, because the perpetrators of cybercrimes usually also have the ability to be able to confuse the time and date of the crime. The problem of evidence is also a separate problem for law enforcement officers. The limited ability of law enforcement, in this case Polri investigators to handle this cyber crime, is limited both in terms of human resources and in terms of equipment.

Difficulties in investigating, investigating, prosecuting and proving criminal acts committed by corporations providing telecommunications services for user data leaks, therefore it is necessary for the court to apply the principle of strict liability of absolute corporate responsibility, so that this becomes a reference also in the process of handling cases in court. The complexity of proving corporate guilt makes it possible to accept the principle of strict liability in the concept of criminal law in Indonesia in the context of corporate criminal liability, making the element of error in the form of intentional or negligence not necessary to prove the same as in the context of human legal subjects [23].

The theory of normative error that causes error is not absolute and must be seen as a human psychological condition characterized by intentional or negligence. Thus the fault lies not only in human legal subjects but also in corporations because it will be very difficult to determine whether there is an error in the corporation if the error is solely seen as a psychological problem.

Regarding the problems studied, it becomes an interesting object of discussion, what if the same applies to cases of leakage of user data by corporations. The corporate criminal responsibility for the leakage of personal data can also be expanded, that the burden of proof is on the corporation. The element of error in the use of the principle of absolute liability (strict liability) does not necessarily disappear, but it's just that the burden of proof that was previously on the prosecutor (prosecutor) has been transferred to the party suspected of committing the crime of leaking personal data (suspect). This in procedural law is called reverse proof, which is known in Law Number 20 of 2001 concerning Amendments to Law Number 31 of 1999 concerning Eradication of Corruption Crimes.

The parameters of law enforcement (judges) in assessing corporate errors so that judges can impose criminal penalties against corporations are listed in Article 4 paragraph (2) of the Supreme Court Regulation Number 13 of 2016, namely the corporation can obtain benefits or benefits from the crime or the crime is committed to the interests of the Corporation, the Corporation allows the occurrence of a crime, and the Corporation does not take the necessary steps to prevent, prevent a greater impact and ensure compliance with applicable legal provisions in order to avoid the occurrence of a criminal act. This means that if the telecommunications service

provider corporation allows a criminal act to occur in this case is the leakage of customer's personal information data, the intended omission is to allow hacking by an irresponsible third party, not to report to the Communications and Information Technology for the hacking attempt, and not notify the service user in writing of any data leakage.

Specifically, until now Indonesia does not have legal instruments, both legal arrangements and law enforcement processes, against the leakage of personal information data of its citizens. The regulations that specifically regulate the legal protection of personal information data are currently only draft, both contained in the National RKUHP, the Personal Data Protection Bill, and the National RKUHAP. However, referring to Article (3) of the Supreme Court Regulation Number 13 of 2016 concerning Procedures for Handling Criminal Cases by Corporations, as a guide for law enforcement officers in handling criminal cases committed by corporations, to impose criminal liability for service providers corporations telecommunications for the leakage of personal data can only be passed on to people who have a working relationship for and for the telecommunications service provider corporation.

It can be underlined that if the corporation violates the provisions of the rights and obligations of the corporation that have been regulated in the legal regulations in Indonesia, the corporation will be represented by a manager to be examined for any leakage of user's personal data based on structural internal rules in a corporation. Then the question arises, whether the leak of user data was caused by a deliberate error or other factors. Because the error factor can occur with intentional elements and negligence carried out by management, employees or employees.

Based on the above description, according to the wisdom of the author, it is necessary to comprehensively regulate the law with the intention of criminal liability for this corporation, there must be an update on the principles and even the criminal procedural law regarding procedures for handling disputes over the leakage of personal data in order to make it easier to resolve cases in an effort to resolve cases. Cases of criminal acts committed by corporations based on electronic information technology for the protection of personal data, besides that, criminal acts related to personal data are a big threat to Indonesia and even other countries because of the advancement of the world of technology by using the internet network that has a connection without bricks.

The analysis obtained from Perma Number 13 of 2016 concerning Governance, How to Handle Criminal Cases by Corporations, As has been regulated in Article 4 paragraph (2), this provision is the author's concern for corporations intentionally allowing criminal acts to occur. Leakage of user's personal data is a right that needs to be protected regardless of anyone. If the corporation overrides strict protections in securing which personal data, it is the obligation of the telecommunications service provider corporation.

The corporation does not fulfill the necessary steps in prevention, Preventive action for larger impacts and ensuring compliance with applicable legal provisions in order to avoid the occurrence of criminal acts. Basically, the service provider corporation has made it possible to prevent the leakage of user's personal data, but the privacy policy issued by the corporation has loopholes and is being targeted by irresponsible people.

Corporations as legal subjects are interpreted the same way as humans, Article 5 of the Supreme Court Regulation Number 13 of 2016 is stated as stipulating that in the event that one or more corporate management quits, or dies, it does not result in the loss of a corporate responsibility. In addition, Article 23 also stipulates that judges may impose criminal penalties against corporations or management, or corporations and management, either alternatively or cumulatively.

Then, to apply criminal penalties or sanctions imposed on a corporation based on the guidelines that have been regulated, Article 25 paragraph (1) of the Supreme Court Regulation Number 13 of 2016 is a principal or additional crime. The main punishment (fines) while the additional penalties are in the form of replacement money, compensation and restitution that are imposed on the corporation. Regarding the procedure for its implementation in accordance with the laws and regulations.

4 Conclusion

Based on the results of the discussion above, it is concluded that the definition of personal data information has a definition as any data regarding a person's life either identified and/or can be identified separately or combined with other information either directly or indirectly through electronic and/or non-electronic systems.. The definition also includes sensitive personal data, namely personal data that requires special protection consisting of data related to religion/belief, health conditions both physically and mentally (mentally), sexual life, personal financial data and other personal data that may can harm and harm someone. Corporate criminal liability for telecommunications service providers for user data leakage can be imposed by looking at the elements of the corporate error. Its implementation requires an expansion of meaning, in order to provide a deterrent effect on corporations to prioritize prudence and carry out their obligations as providers or operators of electronic systems in maintaining and secure the user's personal data to the maximum extent possible based on legal provisions. Therefore, it is necessary to ratify a draft law that specifically regulates the protection of a person's personal data and its procedural law in order to realize comprehensive protection and law enforcement for the criminal act of leaking personal data information.

References

1. Chairul Huda, 2006, Dari Tindak Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggung jawab Pidana Tanpa Kesalahan, Cetakan ke-2, (Jakarta, Kencana)
2. Roeslan saleh, 2010, Pikiran-Pikiran Tentang Pertanggung Jawaban Pidana, Cetakan Pertama, (Jakarta, Ghalia Indonesi)
3. Satjipto Rahardjo dalam Hartanti, 2005, Tindak Pidana Korupsi, (Sinar Grafika: Jakarta)
4. Soerjono Soekanto dan Sri Mamudji, 2001, Penelitian Hukum Normatif (Suatu Tinjauan Singkat), (Rajawali Pers, Jakarta)
5. Ade Risha Riswanti. Et al. (2013). Tanggung Jawab Mutlak (Strict Liability) Dalam Penegakan Hukum Perdata Lingkungan Di Indonesia. Kertha Wicara: Journal Ilmu Hukum. 1(3). 2–5. Retrieved from https://ojs.unud.ac.id/index.php/kerthawicara/article/view/6100

6. Alexandra Rengel. (2014). Privacy as an International Human Right and the Right to Obscurity in Cyberspace. Groningen Journal of International Law. 2(2), 37–38. https://doi.org/10.21827/5a86a81e79532
7. Changqing Ji, et al. (2012). Big Data Processing: Big Challenges And Opportunities. Journal of Interconnection Networks. 13(3), 3–5. https://doi.org/10.1142/S0219265912500090
8. Ibnu Rusydi, Zelvi Agustiana, Welnof Satria. (2020). Sosialisasi Dalam Mengantisipasi Kejahatan Internet Di Era Internet Of Think Dan Revolusi Industri 4.0. Reswara: Jurnal Pengabdian Kepada Masyarakat, 1(2), 133. https://doi.org/10.46576/rjpkm.v1i2.581
9. Mega Sonia Putri. (2018). Perlindungan Hukum Data Pribadi Bagi Pelanggan Jasa Telekomunikasi Terkait Kewajiban Registrasi Kartu SIM. Jurnal Cakrawala Hukum. 9(2), 196–197. https://doi.org/10.26905/idjch.v9i2.2772
10. M Rafifnafia Hertianto. (2021). Sistem Penegakan Hukum Terhadap KegagalanDalamPerlindungan Data Pribadi Di Indonesia. Jurnal Kertha Patrika, 43(1). 98–99. https://doi.org/10.24843/KP.2021.v43.i01.p07
11. Nadiah Tsamara. (2021). Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. Jurnal Suara Hukum. 3(1). 60–61 https://doi.org/10.26740/jsh.v3n1.p53-84
12. Sekaring Ayumeida Kusnadi. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. Al Wasath Jurnal Ilmu Hukum. 2(1). 2. https://doi.org/10.47776/alwasath.v2i1.127
13. Parida Angriani. (2021). Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif. DIKTUM: Jurnal Syariah dan Hukum. 19(2). 149–160. https://doi.org/10.35905/diktum.v19i2.2463
14. Reksodiputro, Mardjono Mardjono Reksodiputro.(2021). Kejahatan Korporasi Suatu Fenomena Lama Dalam Bentuk Baru. Indonesian Journal of International Law. 1(4). 696–699 https://doi.org/10.17304/ijil.vol1.4.566
15. Ridho Kurniawan, Siti Nurul Intan Sari D. (2014). Pertanggungjawaban Pidana Korporasi Berdasarkan Asas Strict Liability (Studi Pembaharuan Hukum Pidana Lingkungan Hidup). Jurnal Yuridis. 1(2). 161–163. https://doi.org/10.35586/.v1i2.148
16. W. Maisiri, H. Darwish, L. van Dyk. (2019). An Investigation Of Industry 4.0 Skills Requirements. South African Journal of Industrial Engineering. 30(3). 90–91. https://doi.org/10.7166/30-3-2230
17. Zelianin, A. (2022). Personal Data as a Market Commodity in the GDPR Era: A Systematic Review of Social and Economic Aspects. Acta Informatica Pragensia, 11(1), 123–140. https://doi.org/10.18267/j.aip.168
18. Agus Tri Haryanto. (2022, Januari 7). Usai Merger Indosat Ooredoo Hutchison, Ini Daftar Operator Seluler RI. https://inet.detik.com/telecommunication/d-5887931/usai-merger-indosat-ooredoo-hutchison-ini-daftar-operator-seluler-ri#:~:text=%22Saat%20ini%20terdapat%205%20badan,Bicara%20Kementerian%20Kominfo%2C%20Dedy%20Permadi.
19. Dessy Setyowati. (2020, July 5). 91 Juta Data Pengguna Tokopedia yang Bocor Masih Bisa Diunduh Gratis. https://katadata.co.id/desysetyowati/digital/5f01708894956/91-juta-data-pengguna-tokopedia-yang-bocor-masih-bisa-diunduh-gratis
20. Fahmi Ahmad Burhan. (2020, July 7). Data Pelanggan Terindikasi Bocor, Kominfo Minta Operator Investigasi. https://katadata.co.id/berita/2020/07/07/data-pelanggan-terindikasi-bocor-kominfo-minta-operator-investigasi
21. Lawrence Abrams. (2020 November 10). 5.8 million RedDoorz user records for sale on hacking forum. https://www.bleepingcomputer.com/news/security/58-million-reddoorz-user-records-for-sale-on-hacking-forum/

22. Monavia Ayu Rizaty. (2021, December 10). Sebanyak 959 Penyelenggara Telekomunikasi Beroperasi di Indonesia pada 2020. https://databoks.katadata.co.id/datapublish/2021/10/12/sebanyak-959-penyelenggara-telekomunikasi-beroperasi-di-indonesia-pada-2020
23. Pingit Aria. (2020 Januari 30). Cambridge Analytica dan Peran Negara dalam Perlindungan Data Pribadi. https://katadata.co.id/pingitaria/digital/5e9a498e8de68/cambridge-analytica-dan-peran-negara-dalam-perlindungan-data-pribadi