Jurnal Penelitian Hukum De Jure
Volume 23, Number 1, March 2023
P-ISSN: 1410-5632, E-ISSN: 2579-8561
Accredited No: 10/E/KPT/2019
This work is published under license *Creative Commons Attribution-NonCommercial 4.0 International CC BY-NC 4.0)*

INSECURITY TO CONSUMER DATA PROTECTION IN THE eHealth SECTOR

Edy Santoso[1], Andriana[2]
Magister Ilmu Hukum, Universitas Langlangbuana, Bandung, Indonesia[1]
Fakultas Teknik Elektro, Universitas Langlangbuana, Bandung, Indonesia [2]
Email: edys39768@gmail.com

Submitted: 28-1-10-2022; Accepted: 30-03-2023
DOI: http://dx.doi.org/10.30641/dejure.2023.V23.115-130

ABSTRACT

In Indonesia, the eHealth application has been widely used. It has also been recognized by World Health Organization (WHO) that Information and Communication Technology (ICT) provides a cost-effective and secure value to support various health sectors. The research method uses normative research which more emphasizes the use of positive law and comparisons of law with other countries. Meanwhile, the approach used in this study is a "qualitative empirical". A primary legal material implementing statutory regulation in the field of Cyber law, and practically discusses how it is implemented in eHealth. This research examines two things in depth. Firstly; Is a "Data breach" committed by the electronic service providers? Secondly; Is a "Data theft" modus operandi achieved by the perpetrator? This study concludes that a "data breach" can occur due to "carelessness" or "bad faith" on the part of the service provider. Thus, bad faith behavior may intentionally process the data for illegal commercial purposes, either by processing it alone or by cooperating with other parties who use the data. Meanwhile, "Data theft" caused by "illegal access" activities there are carried out by the perpetrator, causing data can be changed, damaged, and deleted. Data related to eHealth is included in the category of special data that is protected by the laws and regulations in Indonesia. Thus, service providers should participate in providing data protection efforts by making "self-regulation" and providing training to service users, in an effort to avoid crime under Law Number. 27 of 2022 on Personal Data Protection.

Keywords: data breach; data protection; data theft; eHealth.

1. INTRODUCTION

In 1999 a national study of telemedicine in Australia promoted the concept of *electronic health (*eHealth).[1] Here, Mitchell also pointed out that "eHealth can be considered to be the health industry equivalent of e-commerce.[2] It is e-commerce in the field of services that specializes in the health sector. This sector is a sector that is developing very rapidly in the future. The latest technologies used, such as e-commerce, net banking, healthcare and personal data on cloud storage need high security.[3]

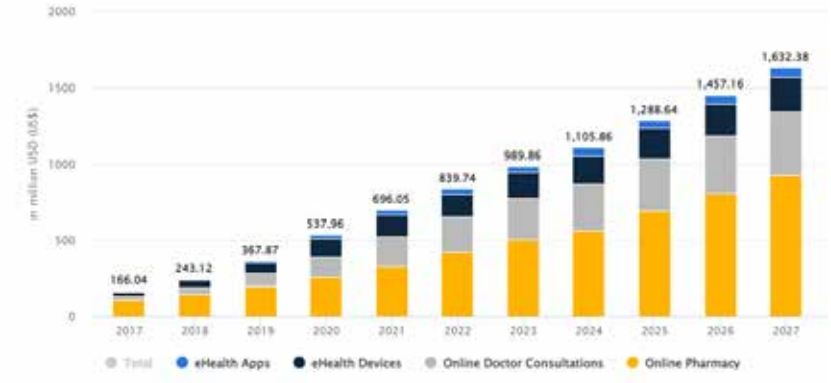
Referring to data from the Indonesian Internet Service Providers Association (IISPA). In Indonesia, internet penetration in 2021-2022 reach 77.02%.[4] Referring to the number of Internet penetrations above 70%, the author is optimistic that service users in the eHealth sector will continue to increase, in line with the development of e-commerce in this service sector. Although, in 2019, users of health applications only reached 10% of the total population in Indonesia.[5]

1 John Mitchell, "Increasing the Cost-Effectiveness of Telemedicine by Embracing e-Health," *Sage Joulnals* 6, no. 1 (2000), https://journals.sagepub.com/doi/10.1258/1357633001934500.
2 Vincenzo Della Mea, "What Is E-Health (2): The Death of Telemedicine?," *Journal of Medical Internet Research* 3, no. 2 (2001): 6–7.
3 Charu Virmani et al., "Analysis of Cyber Attacks and Security Intelligence: Identity Theft," *Indian Journal of Science and Technology* 13, no. 25 (2020): 2529–2536.
4 APJII, "APJII Di Indonesia Digital Outloook 2022," last modified 2022, accessed February 14, 2023, https://apjii.or.id/berita/d/apjii-di-indonesia-digital-outloook-2022_857.
5 Media Infokes, "Penggunaan Aplikasi Kesehatan Digital Di Indonesia, Hanya 10% Dari Total Penduduk," last modified 2019, accessed October 4, 2022, https://media-infokes.com/2019/08/22/penggunaan-aplikasi-kesehatan-digital-di-indonesia-hanya-10-dari-total-penduduk/.

Based on data from Statista for Indonesia, revenue in the eHealth segment is projected to reach US$989.80m in 2023. It is expected to show an annual growth rate (CAGR 2023-2027) of 13.32%, resulting in a projected market volume of US$1,632.00m by 2027. Meanwhile, user penetration will be 20.08% in 2023 and is expected to hit 26.23% by 2027. With this data, the average revenue per user (ARPU) is expected to amount to US$17.49[6].

This data shows a significant development in the use of the eHealth application. The emergence of eHealth is one of the new styles of medical services. It allows health facilities to easily manage medical record data, pharmacies, and hospitals at affordable prices for both clinics and hospitals through the ICT platform. It can be said as a technological innovation in medical services which provides many conveniences for medical activities, such as consultation, treatment, and transactions. Here, eHealth takes part in the role of convenience in providing health services in over the world.

Figure 1. eHealth in Indonesia



Statista.com

In 2001, G Eysenbach defined the term and concept of eHealth as "*referring to health services and information delivered or enhanced through the Internet and related technologies.*[7] This definition is expected to provide quite a broad meaning to be applied to a dynamic environment such as the Internet. Another thing that can be conveyed is that at the same time realizing that eHealth includes more than just "Internet and Medicine".[8] In this regard, WHO defines eHealth as the cost-effective and secure use of ICT in support of health.[9] In 2020, Dymyt, and Malgorzata, stated that "Progress of digital technologies contributes to the dynamic development of eHealth[10] Furthermore, eHealth can provide high-quality health services that significantly influence patient safety.[11]

In the Decree of the Indonesian Minister of Health (KepMenKes) Number 192/MENKES/SK/VI/2012[12] it is stated that eHealth is the use of ICT in the health sector, especially to improve health services. This regulation contains the vision to achieve Healthy Indonesia 2025, so the Grand Design for Health Information System Reform is prepared, which is divided into three roadmaps.

---

6 Statista, "EHealth - Indonesia," last modified 2022, accessed March 26, 2023, https://www.statista.com/outlook/dmo/digital-health/ehealth/indonesia.

7 Gunther Eysenbach, "What Is E-Health?," *Journal of Medical Internet Research* 3, no. 2 (2001): 1–5.

8 Ibid.

9 WHO, "EHealth," last modified 2022, http://www.emro.who.int/health-topics/ehealth/.

10 Malgorzata Dymyt, "The Role of EHealth in the Management of Patient Safety," Journal of e-health Management 2020 (2020): 1–13, https://ibimapublishing.com/articles/JEHM/2020/341252/.

11 Ibid.

12 *Decree of the Minister of Health Number 192/MENKES/SK/VI/2012 Regarding Roadmap of Strengthening Action Plan Indonesian Health Information System*, n.d.



Figure 2. Grand Design Framework for Health Information System Reform (ISR)

The 2011-2014 roadmap focuses on Strengthening the Health Information System Reform (ISR) Foundation in terms of Regulations/Policies, Resources, and the ISR Integration Process. Meanwhile, the 2015-2019 and 2020-2024 roadmap: continue, maintain/maintain and perfect the integration and strengthening of ISR. This regulation is a follow-up related to the National Health System (SKN) policy, which is regulated in the Decree of the Indonesian Minister of Health (KepMenKes) No. 374/MENKES/SK/V/2009 concerning the National Health System (NHS)[13].

However, technology has a role to change social behaviours in various community activities. Here, the essence of social networking services is in disclosing privacy and sharing personal information.[14] Thus, the impact that will arise is not only positive but also negative simultaneously changing human behaviors. In contrast, the Internet can be said to be "the indispensable tool" in creating an Information Society.[15] Meanwhile, from the opposing side comes a new type of crime that can virtually harm the community.

In this case, Howard reminded the flow of personal data of internet users continues to occur to companies providing digital services (social media, search engines, e-commerce, and others)-as long as internet users actively use these services.[16] Thus, the public must be vigilant in the use of Internet-based digital media, because their personal data is very vulnerable to being used by irresponsible parties. Here, business people not only have an obligation to protect data during the processing of personal data, but also have an obligation to protect it like protecting assets.[17] It is as Almunia said that "Today, personal data are a type of asset for companies".[18]

---

13 *Decree of the Minister of Health of the Republic of Indonesia No. 374/MENKES/SK/V/2009 Concerning the National Health System (NHS)*, n.d.

14 Anahiby Anyel Becerril, "The Value of Our Personal Data in the Big Data and the Internet of All Things Era," *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal* 7, no. 2 (2018): 71–80.in which we transit, is preceded by a digital economy based fundamentally on information. And although estimates have been made on whether the data moving in the digital economy flow are from sensors or machines or come from each of us, one thing is certain, all information has a monetary value. Within this flow of information are our personal data. Every moment that we use an electronic device we leave behind vestiges of our life, which are collected by the machines to generate value to the companies. In this way our information is subject to market rules, supply and demand. We have become intangible beings, mercantilized, giving our bodies of data to the science, innovation and technological development. With the use of technologies such as Big Data and IoT, more information less is better. The speed with which our information is collected and treated as well as commercialized is undermining confidence in the digital market. Concern about the misuse of our personal data, or about the information we know about us, raises fundamental questions about privacy, ownership of information and human rights. The question of who should benefit from products and services based on digital data (generated by users

15 M. Castells, *The Information Age*, III. (Oxford: Blackwell, 1998), 336.

16 Agus Sudibyo, *Jagad Digital* (Jakarta: Kepustakaan Populer Gramedia, 2019), 174.

17 Maria Bottis and George Boucha, "Personal Data v. Big Data: Challenges of Commodification of Personal Data," *Open Journal of Philosophy* 8 (2018): 206–215, http://www.scirp.org/journal/ojpp.

18 Joaquín Almunia, "Speech - Competition and Personal Data Protection, Commissioner Joaquín Almunia," *European Commission*, last modified 2012, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_860.

In this regard, Martin, Kelly D. et all argue that consumers are of the view that data is very vulnerable to privacy violations.[19] The concern here is related to data privacy which is ignored by business actors. Thus, the author is very concerned that every business actor should pay attention to aspects of consumer data protection, especially related to medical record data which is part of eHealth services.

In the health sector, the risks associated with data breaches and data theft are unavoidable. The first risk of "data breach" cases in the USA between 2009 and 2021 were approximately 4,419 healthcare data breaches of 500 records. Meanwhile, in 2021, an average of 1.95 healthcare data breaches of 500 or more records were reported each day.[20] Furthermore, healthcareitnews.com writes that, on the dark web, medical record data can be sold for up to $1000 per document. It is the impact of a data leak. Sales of data, in the case above, will have a lot of risk. This can have an impact on the financial sector. With the ownership of this data, criminals can access the victim's financial data and steal it. This is one of the risks that will be experienced by the victim, not to mention the use of data for certain purposes, which can be detrimental to the victim.

Here, the channels of communication and commerce provided by the Internet easily transcend national boundaries.[21] However, problems in the jurisdiction field, for example, personal jurisdiction applies with a defendant amenable to our jurisdiction if the person is present here.[22] It is very difficult to prove the existence of perpetrators in cyberspace. This worrying thing in Indonesia will also happen. Cases such as administrative data theft, hacking for insurance claim fraud, insurance card fraud, drug prescription fraud, and Use of health information for extortion.

In this regard, Solove (2008) argued that the above problems were caused by the lack of regulation in the management of personal information.[23] According to the author, it will become a big problem in the future if it is ignored. Therefore, research related to legal issues in eHealth is very important to be carried out related to violations and crimes of illegal use of personal data.

To anticipate the legal problems above, on September 20, 2022, through the Plenary Meeting of the house of representatives, the bill of Personal Data Protection Law was passed into law (PDP Law 2022).[24] This new regulation is expected to be used as a "legal umbrella" in the digital sector. The passage of the bill into law is also a major success and progress in realizing personal data governance in Indonesia. Thus, for eHealth service providers, both public and private, to improve security systems, comply with responsibilities, and maintain the personal data they manage, both general and specific data, as absolute compliance with personal data protection regulations. Furthermore, standards and criteria for health data are regulated in Regulation of the Minister of Health Number 18 of 2022 Regarding the Implementation of One Health Sector Data Through a Health Information System (PerMenKes 18/2022).

To examine efforts to protect consumer data in eHealth activities, the author will examine various laws and regulations that allow providing protection from the side of national regulations. In addition, it is also important to review the protection measures taken by electronic service providers related to eHealth. Where in this case, business actors are also required to try to provide protection to their patients' personal data, as consumers.

Therefore, one of the problems that have been raised generally relates to the theft and misuse of patient data, which in this case is a consumer. This is the focus of this research. Thus, this research examines two things in depth. Firstly, is a "Data Breach" committed by the electronic service providers? Secondly, is a "Data Theft" modus operandi achieved by the perpetrator.

---

19 Kelly D. Martin, Abhishek Borah, and Robert W. Palmatier, "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing* 81, no. 1 (2017): 36–58.

20 HIPAA Journal, *Healthcare Data Breach Statistics*, 2022, https://www.hipaajournal.com/healthcare-data-breach-statistics/.

21 Clive Walker and David Wall, *The Internet, Law and Society* (UK: Person Education Limited, 2000), 14.

22 Walker and Wall, *The Internet, Law and Society*.

23 Rita O. Koyame-Marsh and John L. Marsh, "Data Breaches and Identity Theft: Costs and Responses," *IOSR Journal of Economics and Finance (IOSR-JEF)* 5, no. 6 (2014): 36–45, www.iosrjournals.org.

24 Kominfo, "Rapat Paripurna DPR Sahkan RUU PDP," last modified 2022, accessed October 16, 2022, https://aptika.kominfo.go.id/2022/09/rapat-paripurna-dpr-sahkan-ruu-pdp/.

2. RESEARCH METHOD

A "qualitative empirical" approach is applied in this research. Thus, it did not do primary data collection through questionnaires. As a primary legal material, it is a statutory regulation in the field of Cyber law. This research will also touch on how the law can be applied in practice.[25] The "socio-legal" method will be used. This would examine legal principles, and examine written regulations as well as consider social realities. The goal is revealed, and knowing what is being faced.[26]

In reality, people often experience legal problems related to the use of eHealth. Thus, it is closely related to cyber law. Where, the use of ICT is very dominant in society and has indirectly greatly influenced people's lifestyles. It is used by criminals to target their prey using application. This requires the application of laws that are "*lex specialist*". It should reflect social attitudes and behaviors and then flow into the right channels.[27]

This study uses a normative approach. The matters discussed will refer to the relevant legislation. In addition, a comparative legal study approach will also be used, particularly in relation to the regulations in force in the European Union. Furthermore, this study also uses secondary data types derived from primary legal materials and secondary legal materials.[28] Here, it is important to pay attention to the integration between social and legal research. Social is related to human behavior and legal is related to normative law. It will be very important in creating better public administration in society.[29]

Primary legal material means material whose law has binding legal force. It will include various laws and regulations in the field of cyber law, such as Law Number. 27 of 2022 on Personal Data Protection (PDP Law),[30] and the Law Number. 19 of 2016 on Electronic Information and Transactions (ITE Law).[31] To discuss more deeply related to data protection, this study also uses the Regulation of the Minister of Communication and Informatics Number. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems (Permen DP)[32] and Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records[33] as well as Regulation of the Minister of Health Number 18 of 2022 Regarding Implementation of One Health Sector Data Through a Health Information System (Permen 18/2022)[34].

3. DISCUSSION AND ANALYSIS

Data theft is very scary. The provision of data information in public areas such as newspapers, magazines, social media, mobile applications, and websites should receive attention. Providing information to the public may be a risk related to data security. It is not only electronic media but also print media that has its own risks. Case of Vereniging Weekblad Bluf! v. the Netherlands,[35] 9 February 1995, in the case of confidentiality of information already made public because of the newspaper's own actions.[36]

---

25 Philip Langbroek et al., "Methodology of Legal Research: Challenges and Opportunities," *Utrecht Law Review* 13, no. 3 (2017): 1–8.

26 Soerjono Soekanto, *Pengantar Penelitian HUkum* (Jakarta: UI Press, 1986), 3.

27 S. N Jain, "Legal Research and Methodology," *Journal of the Indian Law Institute* 14, no. 4 (1972): 487–500, https://www.jstor.org/stable/43950155.

28 Z Amiruddin & Asikin, *Pengantar Metode Penelitian Hukum* (Jakarta: Raja Grafindo Persada, 2003), 118.

29 Pradeep M.D., "Legal Research- Descriptive Analysis on Doctrinal Methodology," *International Journal of Management, Technology, and Social Sciences* 4, no. 2 (2019): 95–103.

30 *The Law Number. 27 of 2022 on Personal Data Protection*, n.d.

31 *The Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 on Information and Electronic Transactions*, n.d.

32 *Regulation of the Minister of Communication and Informatics No. 20 of 2016 Concerning Protection of Personal Data in Electronic Systems*, n.d.

33 *The Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 Concerning Medical Records*, n.d.

34 *Regulation of the Minister of Health, No 18 of 2022 Concerning Implementation of One Data in the Health Sector Through the Health Information System.*, n.d.

35 European Court of Human Rights, *Vereniging Weekblad Bluf! V. the Netherlands*, Series A v (1995).

36 Geoffrey Robertson and Andrew Nicol, *Media Law*, Fifth Edit. (London, UK: Penguin Books, n.d.).

Insecurity in cyberspace is more terrible. The ease of accessing data illegally to information technology systems owned by organizations or individuals is very vulnerable to breaking into. Thus, the security issue for an information system is the most important priority to be maintained. Causing this data is very easy to access which will be related to data protection.

Referring to the 2019 Deloitte survey report, the respondents had, 84.4% were satisfied, while the other 15.6% of them were dissatisfied with the digital health care application. However, there were some concerns that the respondents had including: data privacy, miscommunication, diagnostic accuracy, inexperienced doctors, and legal protection. In this survey, there are still around 16% who are concerned about regulation & legal security issues.

Figure 3. Reason for Not Using eHealth Application



The existence of data either through a data storage system on a computer[37] or even those related to the internet must receive the highest security priority. Because, this data will be vulnerable to being used for various purposes such as business, professionalism, and other interests. Of course, it will cause data owners to be harmed both materially and immaterially.

Referring to Article 8 of PerMenKes 18/2022 regarding the Implementation of One Health Sector Data Through a Health Information System. Health Information is classified as secret information, limited information; and public information that must get protection. Given that this data is very vulnerable to misuse by irresponsible parties.

In addition, developing countries should prepare good ICT infrastructure. Tragedy cases of power outages (blackouts) in most parts of Indonesia on August 4-5, 2019, made all ICT-based service systems paralyzed. The public cannot take their money at an ATM and also cannot use internet-based electronic transactions that cannot be used. This is an event that gives lessons, there is a risk experienced by people who save their money based on ICT.[38] It could happen as well to eHealth users who use ICT facilities.

Regarding data theft, there have been cases of selling CDs. It is also possibly related to the sale of data containing medical records. In 2019, cases of illegal personal data sale and purchase violations occurred in Indonesia. Tangerang District Court handed down 9 months in prison and a fine of IDR 1 billion to Adi Warnadi Ismentin.[39] The perpetrator was proven to have sold a customer database and was sentenced by the Information and Electronic Transactions Law (IET Law). The perpetrator collects consumer data from the domain site www.database.org. Customer data from various banks, including name, telephone number, address, date of birth, card number, and card type.

37 Ibid.

38 Nik Martin, "Indonesia's Jakarta Hit by Major Power Blackout," last modified 2019, accessed October 2, 2019, https://www.dw.com/en/indonesias-jakarta-hit-by-major-power-blackout/a-49884728.

39 Andi Saputra, "Jual Database Nasabah Perbankan, Warga Tangsel Dibui 9 Bulan," *Detik News*, last modified 2019, accessed October 2, 2022, https://news.detik.com/berita/d-4588549/jual-database-nasabah-perbankan-warga-tangsel-dibui-9-bulan.

The price per CD is sold from IDR 500 thousand to IDR 3 million. Within a year, the perpetrator can get profit from around IDR 60 million more. In this case, the Tribunal states that the perpetrators have intentionally and without right or violated the law to transfer electronic information and/or electronic documents to the electronic systems of other people who are not entitled, such action. Violates Article 48 paragraph 2 *juncto* Article 32 (2) of the ITE Law.[40] Where the violation is when the perpetrator, has intentionally and illegally moved or transferred Electronic Information and/or Electronic Documents to Other Persons' Electronic Systems that are not entitled.

The case above is an example of the importance of providing data protection. Under the European Union as contained in the General Data Protection Regulation (GDPR), the definition of 'personal data' is 'any information relating to an identified or identifiable natural person as the data subject. In Article 4, Personal data consists of specific Personal data and general Personal data. Here, personal data related to the financial sector is part of the personal data included in the specific data. This is what is emphasized to get protection under the PDP Law.

In relation to this condition, it's not surprising that legal issues in the digital era are getting the world's attention, one of which is the issue of data protection. Starting from the reform of data protection regulations in the European Union as contained in GDPR in 2016. This regulation provides data protection efforts both inside and outside the European Union Region. These regulations, inspire other countries to make improvements to their country's regulations, taking into account the latest developments in information technology.

Consumers, who in the above case are referred to as service users, will of course allow their personal data or medical data to be processed and stored in a system owned by service providers. Here, the author argues, there are 2 (two) risks faced by consumers, namely first, the risk of "data breaches" where business actors misuse data to be used for business purposes for the service provider, and second, the risk of leaking data stored in the system owned by the service provider.

The second risk is often called the risk associated with "data theft". eHealth, which is facilitated by ICT infrastructure, is of course very vulnerable to this type of crime. Criminals will try to retrieve data, for business purposes as well as for financial purposes. Given this situation, several developed countries are very concerned about this issue. Several countries have made or revised personal data protection rules, and some countries have also prepared data protection rules related to this eHealth activity.

As for the second risk namely "data theft" many cases occur in Indonesia. In January 2022, as many as 6 million patient data from many hospitals in Indonesia were leaked and sold on RaidForums. The leaked data is not only population data but also patient medical data such as medical photos, patient administration data, laboratory test results, ECG, and radiology data.[41]

According to Alfons Tanujaya, "Leaked medical data can be misused and result in huge losses for the owner".[42] In the author's opinion, if the management of the eHealth application does not pay attention to its security system, then there will be a risk of "data theft" which will harm the service user.

3.1. Data Breach

In the concept of consumer data protection, Regulation of the Minister of Communication and Informatics Number. 20 of 2016 Concerning Protection of Personal Data in Electronic Systems (Permen Data Protection)[43] has regulated "The Right to be Kept Confidential" and "The Right to Erasure". It provides data protection efforts, especially for organizations that provide electronic services. In the author's opinion, these principles include the following matters:

---

40 *The Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 on Information and Electronic Transactions*.

41 Herman Herman, "6 Juta Data Pasien RS Bocor, Ini Risiko Yang Mengintai," *7 January 2022*, last modified 2022, accessed September 28, 2022, https://www.beritasatu.com/lifestyle/876043/6-juta-data-pasien-rs-bocor-ini-risiko-yang-mengintai.

42 Ibid.

43 *Regulation of the Minister of Communication and Informatics No. 20 of 2016 Concerning Protection of Personal Data in Electronic Systems*.

1. Granting the right to maintain the confidentiality of consumer data so as not to leak to other parties;
2. Granting the right to delete the data if it is no longer related to the services provided;
3. Granting rights to an adequate security system to avoid illegal access by other parties.
4. Granting the right to the integrity of the data that has been inputted, processed, and stored.
5. Granting the right to provide education to consumers to always keep secret codes such as "username" and password".

In theory, data breaches are defined as unauthorized or unintentional disclosures by organizations that result in the loss of customers' personally identifiable information (PII),[44] such as a financial secret number. Organizations that provide services are "trustees" to maintain personal data, especially in the field of eHealth. It is what the author is concerned with at the first risk, in using this eHealth service. These databases and electronic devices are vulnerable to attacks by hackers. It allows criminals to gain access to the personal information of millions of people and sell it to the highest bidder. This mode allows identity theft to occur.[45] Data breaches compromise consumer privacy and have a significant negative impact on a decision regarding patient privacy in eHealth services.

As quoted by Shankar, Nithya, and Mohammed, Zareef[46] that Culnan and Williams (2009) view data breaches are part of a privacy issue that cannot be underestimated. It is a challenge for data controllers to create a culture concerned with protecting the privacy and implementing good governance processes to ensure that these data breaches do not occur in the future.[47] For this reason, a systems approach and education for consumers is very important for data controllers to do.

This case can happen to even bona fide organizations, such as Yahoo. In 2016, Yahoo confirmed that at least 500 million of its user accounts had been leaked to the public.[48] In this case, according to Trautman and Ormerod (2017), the data controller has failed to conduct an investigation. This shows the management capabilities of poor data controllers.[49] In this case, the authors identify the reasons organizations can experience data breaches, which are caused as follows:

a. Employees Mistake

According to Verizon's 2022 Data breaches Investigations Report, 82% of data breaches involved a human element.[50] Here, human error is one of the biggest security threats that organizations face.[51] This includes incidents in which employees expose information directly (for example, by misconfiguring databases) or by making a mistake that enables cyber criminals to access the organization's systems.[52] Employees still make mistakes that may lead to data breaches, cause of follows:[53]

---

44 K. K. Peretti, "Data Breaches: What the Underground World of Carding Reveals," *Santa Clara Computer & High Tech* 25, no. 2 (2008): 375–413.

45 Rita O. Koyame-Marsh and John L. Marsh, "Data Breaches and Identity Theft: Costs and Responses," *IOSR Journal of Economics and Finance (IOSR-JEF)* 5, no. 6 (2014): 36–45.

46 Zareef Shankar, Nithya Mohammed, "Surviving Data Breaches: A Multiple Case Study Analysis," *Journal of Comparative International Management* 23, no. 1 (2020): 35–54.

47 Culnan, M. J. and C. C. Williams, "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly* 33, no. 4 (2009): 673–687.

48 Jamie White, "Yahoo Announces 500 Million Users Impacted by Data Breach," *2021*, last modified 2021, accessed October 4, 2022, https://lifelock.norton.com/learn/data-breaches/company-data-breach.

49 L. J. Trautman and P Ormerod, "Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach," *American University Law Review* 66 (2017): 1231–1291.

50 verizon.com, "2022 Data Breach Investigations Report," last modified 2022, accessed October 4, 2022, https://www.verizon.com/business/resources/reports/dbir/.

51 Luke Irwin, "Human Error Is Responsible for 82% of Data Breaches," last modified 2022, accessed October 4, 2022, https://www.grcelearning.com/blog/human-error-is-responsible-for-85-of-data-breaches#:~:text=According to Verizon's 2022 Data,to access the organisation's systems.

52 Ibid.

53 Ekran, "How to Prevent Human Error: Top 4 Employee Cybersecurity Mistakes," last modified 2019, accessed October 9, 2022, https://www.ekransystem.com/en/blog/how-prevent-human-error-top-5-employee-cyber-security-mistakes.

1. Incorrectly sending valuable data by e-mail to recipients who are not entitled to it;
2. Carelessness in emailing documents with sensitive data;
3. Failure to accidentally publish confidential data on a public website;
4. Misconfiguring assets to allow for unwanted access

This problem is a concern for an organization. Employees who have the responsibility to protect consumer data must have high integrity not to leak consumer data either intentionally or unintentionally, thus causing harm to consumers, both material and immaterial. This has been regulated in Article 3 of the ITE Law that the use of Information Technology is carried out based on one of them by applying the "prudence principle". And another important principle in the use of information technology is also "good faith".

b. Social Engineering

According to the U.S. Department of Justice, quoted by Fatima Salahdine, and Naima Kaabouch, social engineering attacks are one of the most dangerous threats in the world.[54] According to them, social engineering can be classified into two (2), namely human-based or computer-based. Here, social engineering trick victims into obtaining specific data that can be used to financially benefit the perpetrators of the crime. Of course, these things can be used for a specific purpose, or even sold on the black market and the dark web.[55]

Whereas the human-based uses a traditional approach that relies on communication relationships between individuals so that criminals can dig up information and try to steal it. While the computer-based approach emphasizes the use of the system. This can be done using computer technology and telecommunications technology. The use of software used will attempt to steal important consumer data.

In 2020, Abeer F. AL-Otaibi and Emad S Alsuwat in the conclusion of their research stated that "the threat of social engineering has become the main threat and is considered the biggest and most dangerous security threat which is a violation faced by individuals and institutions".[56] Through social engineering, an organization can lose important data and information. Social engineering will attack with the art and technique of manipulating or luring users and institutions into obtaining important data that criminals want.

Therefore, article 36 of the PDP Law stipulates that the Personal Data Controller is obliged to prevent the Personal Data from being accessed illegally. Prevention can be done by using a security system for Personal Data that is processed and/or processed Personal Data using an electronic system in a reliable, secure and responsible manner. Therefore, this requires an adequate security system, considering today's "cyber-attack" will target a weak security system and provide benefits for criminals.

c. Malicious Insiders

In various organizational activities, of course, some employees who have bad intentions. It can also happen to organizations associated with electronic service providers. An employee's violation can be in the form of seeking his own profit by ignoring the interests of the organization, as well as consumers. They can position themselves as, malicious insiders, inside persons, informants, and whistle-blowers are all capable of leaking data to the outside.[57]

Given their role as "inside persons", they will know more about what the organization is doing, trending issues, important data related to consumer data and company data, and other confidential matters. Inside person, given the responsibility and trust to maintain these things. Therefore, inside persons are more dangerous when committing violations than outside persons, especially in terms of leaking confidential data.

In this regard, insider attacks accounted for 34% of all data breaches in 2018 as addressed by IBM.[58] For a business organization, this is a significant amount, and can affect public trust in service delivery, especially

---

54 Fatima Salahdine and Naima Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet* 11, no. 4 (2019).
55 Ibid.
56 Abeer F. AL-Otaibi and Emad S Alsuwat, "A Study on Social Engineering Attacks: Phishing Attack," *International Journal of Recent Advances in Multidisciplinary Research* 07, no. 11 (2020): 6374–6380.
57 Diogo A.B. Fernandes et al., "Chapter 25 - A Quick Perspective on the Current State in Cybersecurity," in *Emerging Trends in ICT Security*, 2014, 423–442, https://www.sciencedirect.com/science/article/pii/B9780124114746000256.
58 Abolaji B. Akanbi et al., "A Stacked Ensemble Framework for Detecting Malicious Insiders," *International Journal of Innovative Research in Computer Science & Technology* 8, no. 4 (2020).

related to the issue of maintaining the confidentiality of consumer data. Furthermore, malicious insider threats can take various forms such as insider Information Technology (IT) sabotage and insider fraud.[59]

These insiders cause electronic data or information to be spread to unauthorized persons. It needs to refer to Article 32 (2) of the ITE Law has regulated this violation that every person intentionally and without rights or against the law in any way transfers Electronic Information and/or Electronic Documents to another person's Electronic System who has no rights.

3.2. Data Theft

According to Kaspersky, the definition of "data theft" is the act of stealing digital information stored on computers, servers, or electronic devices to obtain confidential information or compromise privacy.[60] This is an illegal activity carried out by perpetrators to access data sources and steal them. Thus, various devices such as business databases, desktops, handheld devices, phones, flash drives, and cameras can all be used by thieves to steal data.[61]

Identity (ID) theft happens when someone steals your personal information to commit fraud.[62] Service providers should have the commitment to provide data protection to prevent illegal access. This can be realized by strengthening the tough security system. In the online agreement, this commitment must be contained. It is not only for the benefit of consumers but also for the interests of service providers. Here, data theft is a major problem for many businesses because of security, reputation, and financial loss.[63]

Historically, since 1997, the Federal Trade Commission (FTC) identified that the number of complaints regarding "identity theft" has increased. In this case, the Consumer Sentinel Network (CSN), which is part of the FTC, reported that in 2013, they had received more than 2 million complaints from consumers. 14% fall into the "identity theft" category.[64] The stolen data is generally in the form of specific data, such as bank account and credit card information, including medical record data. Regarding EHealth services, the risk for consumers who use this facility is data theft in the form of "Medical Records".

It is something that needs to be protected. The medical record contains documents that contain patient identity data, examinations, treatment, actions, and other services that have been given to patients. For that specifically, it is protected under the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records.[65]

Here, medical Reports mean any reports generated by outside consultants of the User engaged to perform medical or medical-related testing or examination on or of such patient.[66] If the security system owned by healthcare providers is not strong, then perpetrators can access it. They have access to personal data to delete, alter, modify or prevent access to it illegally.

In this case, the authors identify "data theft" efforts related to eHealth services, which can be in the form, as follows:

a. Cyber Attack

A successful cyber-attack on the target will have an impact on various levels of impact, ranging from individual users, service provider organizations, and even the computing systems used. The most significant impact is usually felt on the data stored in the system or the data transmitted over the network. These impacts

---

59 Ibid.

60 Kaspersky, "What Is Data Theft and How to Prevent It," accessed October 2, 2022, https://www.kaspersky.com/resource-center/threats/data-theft.

61 Source Defense, "What Is Data Theft?," last modified 2022, accessed October 3, 2022, https://sourcedefense.com/glossary/what-is-data-theft/.

62 usa.gov, "Identity Theft," last modified 2022, accessed October 3, 2022, https://www.usa.gov/identity-theft.

63 Source Defense, "What Is Data Theft?"

64 Koyame-Marsh and Marsh, "Data Breaches and Identity Theft: Costs and Responses."

65 *The Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 Concerning Medical Records*.

66 Law Insider, "Medical Reports Definition," last modified 2022, accessed October 4, 2022, https://www.lawinsider.com/dictionary/medical-reports.

can be related to their confidentiality, integrity, or availability.[67] In general, this cyber-attack has been regulated in the ITE Law. Particularly in Article 30 which regulates the prohibition of unauthorized access and breaking through, overtaking, or breaking into security systems.

b. Hacking

Hacking is used as a method to commit other crimes such as theft of identity in cyberspace.[68] This crime mode threatens sensitive personal data in different ways from other modes. Another modus operandi involves the consumer's negligence, but for this mode, the active subjects for data theft are the perpetrators themselves. The mode can be done online, through the Internet network, or offline not through another network.

Perpetrators must have expertise in the field of IT and networking, to break through the security system of financial organizations. The key is indeed in the security system, whether it can be easily penetrated or not. For eHealth service providers that do not have a relatively secure system, it will be easy to penetrate. The threat is consumer data can be known by the perpetrators, including the use of cloud computing systems. Here, cloud computing is an umbrella term for anything that involves delivering hosted services over the internet. These services are divided into three main categories namely infrastructure, platform and software.[69]

Article 16 (2e) of PDP Law, stipulates that personal data controllers must protect the security of Personal Data from unauthorized access, unauthorized disclosure, unauthorized modification, misuse, destruction, and/or loss of personal data. These actions can be carried out by people who have knowledge in the field of qualified information technology, so they can know that the security systems are owned by other parties.

Furthermore, according to the Norton Cybersecurity Insights Report, in 2015 as many as 594 million people around the world have become victims. From that data, as many as 21% of Americans email has been hacked. In addition, as much as 12% of their financial data was stolen after shopping through online platforms. These cases are part of the risks of using public Wi-Fi services, which do not guarantee the security of user data.[70]

c. Deceptive Phishing

Another form of crime related to cybercrime is phishing. Generally, phishing is the act of trying to trick the recipient of a message, by sending an email with malicious intent. This is done so that the recipient opens and follows the instructions given by the criminal. The modus operandi can not only be sent via email, but also SMS and social media. The ultimate goal is to trick sensitive personal data owners, and access victim data. Specifically, what is part of cybercrime is called Deceptive Phishing. Deceptive phishing is to trick someone into clicking a malicious link in a seemingly legitimate phishing email than it is to break through a computer's defenses.[71]

Victims will suspect that the email came from the organization legally. The disadvantage of consumers here is that they are not careful to check the original domain name of their legal organization. The very dangerous thing is that phishing emails may have dangerous content, such as documents the form of PDF or Word documents that contain malicious software (malware). The danger associated with phishing is, there is a 'typo squatting' crime that allows the perpetrators to make a 'fake domain name' which makes users get miss entering the wrong domain name.

---

67 Kenneth Okereafor and Oluwasegun Adelaiye, "Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era," *International Journal of Recent Engineering Research and Development (IJRERD)* 05, no. 07 (2020): 61–72, www.ijrerd.com.

68 Rizal Rahman, Nazura Abdul Manap, and Sohaib Mukhtar, "Hacking in Cyberspace Identity Theft: A Comparative Analysis of Malaysia, United Kingdom, and Iran," *Baltica* 23, no. 11 (2020): 67–86, https://www.researchgate.net/publication/347935764.

69 Wesley Chai and Stephen J. Bigelow, "Cloud Computing," last modified 2022, accessed February 14, 2023, https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing.

70 Norton, "Why Hackers Love Public Wi-Fi," last modified 2019, accessed October 12, 2022, https://us.norton.com/blog/wifi/why-hackers-love-public-wifi#.

71 Alexander S. Gillis, "Phishing," last modified 2020, accessed October 16, 2022, https://www.techtarget.com/searchsecurity/definition/phishing.

Generally, news contained in the e-mail or social media contains news forces users to access 'fake websites", and enter their sensitive financial data. It may contain programs or files that are harmful to computer users. The types of malware that can be installed on "'fake websites" include computer viruses, worms, trojan horses, and spyware. Software designed to perform illegal activities can function to commit theft, deletion, alteration, and conduct espionage activities.

Sensitive Personal data such as medical records, under threat due to all activities carried out through the Internet, especially those related to finance will be known by the perpetrators of crime. The medical record contains documents that contain patient identity data, examinations, treatment, actions, and other services that have been given to patients. For that specifically, it is protected under the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records.[72]

The information submitted generally requires the user to enter a number of sensitive personal data which will then be known by the perpetrators. Thus, the perpetrators will be free to enter sensitive personal data to access the official domain name, where users save money. Therefore, the term phishing covers not only getting the user account details, but it now covers access to data all personal and financial.[73] Thus, electronic system operators should follow the regulations set out in Permen 18/2022, because the standards for managing health data through the information system have been regulated. The most crucial thing is the data security factor. Here, the role of the information system administrator has the obligation to provide education and provide adequate security systems.

4. CONCLUSION

With the presence of eHealth services, it provides various conveniences for users to get various health facilities through electronic platforms. This provides a place and distance solution that will affect the cost of getting health services. However, this also has a negative effect with the emergence of legal issues due to the threat of criminals to consumer's data.

This study concludes that the threat of leakage of consumers' data can arise due to "data breaches" and "data theft". Data breaches can occur due to "carelessness" or "bad faith" from personal data controllers, such as negligence of employees who are not careful in maintaining data so that data is accidentally spread to irresponsible parties. Meanwhile, "bad faith" employees can intentionally process the data illegally for commercial purposes, either by processing it themselves or by make cooperation with other parties. Various unlawful acts in this category include employees' mistake, Social Engineering, and Malicious Insiders.

Meanwhile, "Data theft" is caused by "illegal access" activities carried out by perpetrators so that data can be changed, damaged, and deleted. Various unlawful acts in this category include cyber- attacks, hacking, and Deceptive Phishing. Data related to eHealth is included in the category of specific data that is protected by laws and regulations in Indonesia. The ratification of the PDP Law, will provide "legal certainty" as an effort to provide data protection. Data protection regulated by the PDP Law has adopted the fundamental principles of data protection regulated by the GDPR in the European Union (EU).

Here, the current legal culture in the EU is very careful to provide other people's personal data. In particular, institutions are very carefully considering the consequences of sanctions are very heavy. This is what needs to be developed in Indonesia, given the legal culture, it is still very easy to obtain personal data from certain parties. Thus, do not be surprised, some easily offer certain things, such as credit cards and insurance.

5. ACKNOWLEDGEMENT

First of all, the author would like to thank Allah SWT for the completion of this study, Kemendikbudristek, Republic of Indonesia for financial support. And thank to the Postgraduate Program of Law, University of Langlangbuana and Badan Pengembangan Sumberdaya Manusia (BPSDM), Ministry of Law and Human Rights, of The Republic of Indonesia for the valuable support.

72 *The Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 Concerning Medical Records*.

73 Gunter Ollmann, *The Phishing Guide*, *IBM*, 2007, https://www.scribd.com/document/219802442/The-Phishing-Guide-Understanding-Preventing-Phishing-Attacks-IBM-Internet-Security-Systems.

6. SPONSORSHIP

This writing received funding from a basic research grant from the Ministry of Education, Culture, Research and Technology, in 2022

REFERENCES

Akanbi, Abolaji B., Adewale O. Adebayo, Sunday A. Idowu, and Ebunoluwa E. Okediran. "A Stacked Ensemble Framework for Detecting Malicious Insiders." *International Journal of Innovative Research in Computer Science & Technology* 8, no. 4 (2020).

Almunia, Joaquín. "Speech - Competition and Personal Data Protection, Commissioner Joaquín Almunia." *European Commission*. Last modified 2012. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_860.

APJII. "APJII Di Indonesia Digital Outloook 2022." Last modified 2022. Accessed February 14, 2023. https://apjii.or.id/berita/d/apjii-di-indonesia-digital-outloook-2022_857.

Asikin, Z Amiruddin &. *Pengantar Metode Penelitian Hukum*. Jakarta: Raja Grafindo Persada, 2003.

Becerril, Anahiby Anyel. "The Value of Our Personal Data in the Big Data and the Internet of All Things Era." *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal* 7, no. 2 (2018): 71–80.

Bottis, Maria, and George Boucha. "Personal Data v. Big Data: Challenges of Commodification of Personal Data." *Open Journal of Philosophy* 8 (2018): 206–215. http://www.scirp.org/journal/ojpp.

Castells, M. *The Information Age*. III. Oxford: Blackwell, 1998.

Chai, Wesley, and Stephen J. Bigelow. "Cloud Computing." Last modified 2022. Accessed February 14, 2023. https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing.

Culnan, M. J., and C. C. Williams. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches." *MIS Quarterly* 33, no. 4 (2009): 673–687.

Dymyt, Malgorzata. "The Role of EHealth in the Management of Patient Safety." *Journal of e-health Management* 2020 (2020): 1–13. https://ibimapublishing.com/articles/JEHM/2020/341252/.

Ekran. "How to Prevent Human Error: Top 4 Employee Cybersecurity Mistakes." Last modified 2019. Accessed October 9, 2022. https://www.ekransystem.com/en/blog/how-prevent-human-error-top-5-employee-cyber-security-mistakes.

European Court of Human Rights. *Vereniging Weekblad Bluf! V. the Netherlands*, Series A v (1995).

Eysenbach, Gunther. "What Is E-Health?" *Journal of Medical Internet Research* 3, no. 2 (2001): 1–5.

F. AL-Otaibi, Abeer, and Emad S Alsuwat. "A Study on Social Engineering Attacks: Phishing Attack." *International Journal of Recent Advances in Multidisciplinary Research* 07, no. 11 (2020): 6374–6380.

Fernandes, Diogo A.B., Liliana F.B. Soares, João V. Gomes, Mário M. Freire, and Pedro R.M. Inácio. "Chapter 25 - A Quick Perspective on the Current State in Cybersecurity." In *Emerging Trends in ICT Security*, 423–442, 2014. https://www.sciencedirect.com/science/article/pii/B9780124114746000256.

Gillis, Alexander S. "Phishing." Last modified 2020. Accessed October 16, 2022. https://www.techtarget.com/searchsecurity/definition/phishing.

Herman, Herman. "6 Juta Data Pasien RS Bocor, Ini Risiko Yang Mengintai." *7 January 2022*. Last modified 2022. Accessed September 28, 2022. https://www.beritasatu.com/lifestyle/876043/6-juta-data-pasien-rs-bocor-ini-risiko-yang-mengintai.

Irwin, Luke. "Human Error Is Responsible for 82% of Data Breaches." Last modified 2022. Accessed October 4, 2022. https://www.grcelearning.com/blog/human-error-is-responsible-for-85-of-data-breaches#:~:text=According to Verizon's 2022 Data,to access the organisation's systems.

Jain, S. N. "Legal Research and Methodology." *Journal of the Indian Law Institute* 14, no. 4 (1972): 487–500. https://www.jstor.org/stable/43950155.

Journal, HIPAA. *Healthcare Data Breach Statistics*, 2022. https://www.hipaajournal.com/healthcare-data-breach-statistics/.

Kaspersky. "What Is Data Theft and How to Prevent It." Accessed October 2, 2022. https://www.kaspersky.com/resource-center/threats/data-theft.

Kominfo. "Rapat Paripurna DPR Sahkan RUU PDP." Last modified 2022. Accessed October 16, 2022. https://aptika.kominfo.go.id/2022/09/rapat-paripurna-dpr-sahkan-ruu-pdp/.

Koyame-Marsh, Rita O., and John L. Marsh. "Data Breaches and Identity Theft: Costs and Responses." *IOSR Journal of Economics and Finance (IOSR-JEF)* 5, no. 6 (2014): 36–45. www.iosrjournals.org.

———. "Data Breaches and Identity Theft: Costs and Responses." *IOSR Journal of Economics and Finance (IOSR-JEF)* 5, no. 6 (2014): 36–45.

Langbroek, Philip, Kees van den Bos, Marc Simon Thomas, Michael Milo, and Wibo van Rossum. "Methodology of Legal Research: Challenges and Opportunities." *Utrecht Law Review* 13, no. 3 (2017): 1–8.

Law Insider. "Medical Reports Definition." Last modified 2022. Accessed October 4, 2022. https://www.lawinsider.com/dictionary/medical-reports.

M.D., Pradeep. "Legal Research- Descriptive Analysis on Doctrinal Methodology." *International Journal of Management, Technology, and Social Sciences* 4, no. 2 (2019): 95–103.

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier. "Data Privacy: Effects on Customer and Firm Performance." *Journal of Marketing* 81, no. 1 (2017): 36–58.

Martin, Nik. "Indonesia's Jakarta Hit by Major Power Blackout." Last modified 2019. Accessed October 2, 2019. https://www.dw.com/en/indonesias-jakarta-hit-by-major-power-blackout/a-49884728.

Della Mea, Vincenzo. "What Is E-Health (2): The Death of Telemedicine?" *Journal of Medical Internet Research* 3, no. 2 (2001): 6–7.

Media Infokes. "Penggunaan Aplikasi Kesehatan Digital Di Indonesia, Hanya 10% Dari Total Penduduk." Last modified 2019. Accessed October 4, 2022. https://media-infokes.com/2019/08/22/penggunaan-aplikasi-kesehatan-digital-di-indonesia-hanya-10-dari-total-penduduk/.

Mitchell, John. "Increasing the Cost-Effectiveness of Telemedicine by Embracing e-Health." *Sage Joulnals* 6, no. 1 (2000). https://journals.sagepub.com/doi/10.1258/1357633001934500.

Norton. "Why Hackers Love Public Wi-Fi." Last modified 2019. Accessed October 12, 2022. https://us.norton.com/blog/wifi/why-hackers-love-public-wifi#.

Okereafor, Kenneth, and Oluwasegun Adelaiye. "Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era." *International Journal of Recent Engineering Research and Development (IJRERD)* 05, no. 07 (2020): 61–72. www.ijrerd.com.

Ollmann, Gunter. *The Phishing Guide*. *IBM*, 2007. https://www.scribd.com/document/219802442/The-Phishing-Guide-Understanding-Preventing-Phishing-Attacks-IBM-Internet-Security-Systems.

Peretti, K. K. "Data Breaches: What the Underground World of Carding Reveals." *Santa Clara Computer & High Tech* 25, no. 2 (2008): 375–413.

Rahman, Rizal, Nazura Abdul Manap, and Sohaib Mukhtar. "Hacking in Cyberspace Identity Theft: A Comparative Analysis of Malaysia, United Kingdom, and Iran." *Baltica* 23, no. 11 (2020): 67–86. https://www.researchgate.net/publication/347935764.

Robertson, Geoffrey, and Andrew Nicol. *Media Law*. Fifth Edit. London, UK: Penguin Books, n.d.

Salahdine, Fatima, and Naima Kaabouch. "Social Engineering Attacks: A Survey." *Future Internet* 11, no. 4 (2019).

Saputra, Andi. "Jual Database Nasabah Perbankan, Warga Tangsel Dibui 9 Bulan." *Detik News*. Last modified 2019. Accessed October 2, 2022. https://news.detik.com/berita/d-4588549/jual-database-nasabah-perbankan-warga-tangsel-dibui-9-bulan.

Shankar, Nithya Mohammed, Zareef. "Surviving Data Breaches: A Multiple Case Study Analysis." *Journal of Comparative International Management* 23, no. 1 (2020): 35–54.

Soekanto, Soerjono. *Pengantar Penelitian HUkum*. Jakarta: UI Press, 1986.

Source Defense. "What Is Data Theft?" Last modified 2022. Accessed October 3, 2022. https://sourcedefense.com/glossary/what-is-data-theft/.

———. "What Is Data Theft?"

Statista. "EHealth - Indonesia." Last modified 2022. Accessed March 26, 2023. https://www.statista.com/outlook/dmo/digital-health/ehealth/indonesia.

Sudibyo, Agus. *Jagad Digital*. Jakarta: Kepustakaan Populer Gramedia, 2019.

Trautman, L. J., and P Ormerod. "Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach." *American University Law Review* 66 (2017): 1231–1291.

usa.gov. "Identity Theft." Last modified 2022. Accessed October 3, 2022. https://www.usa.gov/identity-theft.

verizon.com. "2022 Data Breach Investigations Report." Last modified 2022. Accessed October 4, 2022. https://www.verizon.com/business/resources/reports/dbir/.

Virmani, Charu, Neha Kaushik, Mohak, Vishnu Mathur, and Sanskar Saxena. "Analysis of Cyber Attacks and Security Intelligence: Identity Theft." *Indian Journal of Science and Technology* 13, no. 25 (2020): 2529–2536.

Walker, Clive, and David Wall. *The Internet, Law and Society*. UK: Person Education Limited, 2000.

White, Jamie. "Yahoo Announces 500 Million Users Impacted by Data Breach." *2021*. Last modified 2021. Accessed October 4, 2022. https://lifelock.norton.com/learn/data-breaches/company-data-breach.

WHO. "EHealth." Last modified 2022. http://www.emro.who.int/health-topics/ehealth/.

Decree of the Minister of Health Number 192/MENKES/SK/VI/2012 Regarding Roadmap of Strengthening Action Plan Indonesian Health Information System, n.d.

Decree of the Minister of Health of the Republic of Indonesia No. 374/MENKES/SK/V/2009 Concerning the National Health System (NHS), n.d.

Regulation of the Minister of Communication and Informatics No. 20 of 2016 Concerning Protection of Personal Data in Electronic Systems, n.d.

Regulation of the Minister of Health, No 18 of 2022 Concerning Implementation of One Data in the Health Sector Through the Health Information System., n.d.

The Law Number. 27 of 2022 on Personal Data Protection, n.d.

The Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 on Information and Electronic Transactions, n.d.

The Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 Concerning Medical Records, n.d.