Available online at https://journal.rescollacomm.com/index.php/ijeer/index

International Journal of Ethno-Sciences and Education Research

Vol. 3, No. 2, pp. 63-69, 2023

Dumpster Diving Threat in Personal Data Leakage Case in Indonesia

Sayid Muhammad Rifki Noval[1*], Soecipto[2], Ahmad Jamaludin[3], Erna listiawati[4]

[1,2,3,4] *Universitas Islam Nusantara, Bandung, Indonesia*

* *Corresponding author email :* smrn.uninus@gmail.com

Abstract

It is a big job for law enforcement to be able to deal with fraud crimes and data leaks that are increasing at this time. Social engineering attacks are considered one of the modes perpetrators use in carrying out their actions. If the current prevention efforts always link social engineering with phishing, an activity closely related to technological sophistication, it is necessary to know another form of social engineering that deserves attention, namely dumpster diving. A term that describes the activity of "scavenging" a target's trash in search of valuable information. Dumpster diving is often underestimated because some people think that if others do not use the waste disposed of, it will even have a threatening impact. The habit of throwing away records and documents without being destroyed makes it a target for perpetrators to collect information that will be used to attack their targets. Several countries have considered regulating the designation of waste that has the potential to be misused, including regarding the security of personal data. Therefore, this article aims to provide an alternative policy for the Indonesian government to consider issuing regulations that protect victims affected by losses due to the use of waste by perpetrators.

Keywords: Cyber Crime, Dumpster Diving, Social Engineering.

1. Introduction

As a country with a waste generation amount of 30 million tons/year (El-Gayar & Fritz, 2006), Indonesia certainly has a difficult task in managing it. Many studies have been conducted to elaborate on these problems, but it is worth acknowledging that most focus on recycling, quantity reduction, and health issues. Nevertheless, what if the study is done through legal perspectives. Generally, the involvement of the legal field takes place at the regulation level of landfill placement. We need to understand that other problems have been persisting and become more serious now, that is, regarding privacy and crimes due to the inspection of waste by other parties. Other parties might eventually take over various documents containing passwords and confidential information discarded by the government under the pretext of garbage. It is whether a person still has the right to ensure the confidentiality of information, especially regarding privacy contained in the goods that they have disposed of and about the rights of other people who think that they can take, check, and use all information they obtained through waste without the permission of the person who has disposed of it in the belief that someone's rights to the goods or information contained in the goods are lost after disposal. In Indonesia, the regulation of waste can be found in Law Number 18 of 2008 on Waste Management (Waste Management Law), which defines waste as the residue of human daily activities and/or solid natural processes and specific waste that, due to its nature, concentration, and/or volume requires special management. However, we should know that there are no explicit provisions governing the protection of the privacy of waste relating to the person who disposes of it. Waste seems to be useless, and the impact that occurs in the future does not need a permit or consideration of its use, so anyone can take it and use it, including information in it.

An interesting case occurred in Seattle in 2015 when a law was enacted requiring residents to put waste in different bins – one for yards and leftovers and one for recycling. If in an inspection, it is found that more than 10% of the waste bins contain inappropriate types of waste, the waste collection officer will label the waste bins red, and there will be a fine for the residents. The good intention to suppress the amount of waste led to protests by citizens who saw that their privacy rights had been violated. Citizens perceive that none is allowed to see the contents of their waste, not to mention assess and count the amount of waste (Al-Kassimi, 2021). It shows different interpretations of waste between citizens and the government, especially regarding privacy rights. Some people believe that even if it is a waste, there is a right attached to it, for instance, the privacy of whoever disposes of it. So, they do not allow anyone to check and assess it, considering that it may cause them losses in the future since it does not eliminate the possibility

that the waste contains confidential information. If they allow other people to check it, there is a potential for financial loss or other crimes.

The information obtained from waste is not only in the form of physical documents, but current technological developments have encouraged the collection of large data on electronic devices, such as smartphones, USBs, or even smart refrigerators that can collect personal information of someone from his/her list of goods purchased, to credit card data that is automatically used for purchasing these goods. It does not rule out the possibility that irresponsible people could have used these data after taking the item from the waste. They might recover the data even if the device has been formatted. Research conducted in 2018 on the Gulf Cooperation Council (GCC) Countries found that in 2015 there were 645 tons of electronic waste, including PCs, laptops, games consoles, and smartphones, whose data were vulnerable to being protected because there were no regulations that specifically regulated the privacy of the electronic waste data (Alghazo et al., 2018). Some assumed that if they found data contained on the Internet, whether personal information they saw on Facebook, blogs, or other sites, then they could use the data without permission since it is considered to be public and there are no absolute ownership rights to it, which is often equated with the principle of permissionless innovation used in data-driven technology infrastructures (Lu et al., 2015).

In the scope of the law, in particular telematic law, searching through the waste to obtain information is known as dumpster diving. One of the most famous examples of dumpster diving is done by Jerry Schneider in Southern California. Back in high school in 1968, Jerry came across documentation regarding Pacific Telephone's automated equipment ordering and delivery system, which he used to order equipment. Jerry collected thousands of dollars worth of telephone equipment and set up a creative systems company to sell them. Some of these devices were sold back to Pacific Telephone until Jerry was finally arrested in 1972 (Gregg et al., 2006).

Based on the phenomena explained earlier, this article aims to analyze the phenomenon of crime that occurs due to the use of information in garbage which is often known as dumpster diving. The study is carried out by first exploring several cases related to the use of waste in the process to finally provide an alternative view in formulating the concept of privacy protection and threats to social engineering attacks related to the use of waste by other parties.

2. Literature Review

The high number of cyber attacks resulting in data leaks as many as 90% due to social engineering attacks (Ghafir et al., 2018). Social engineering is a form of online, telephonic, or face-to-face techniques employed by social engineers designed to lure unsuspecting users into providing business confidential and personal identity information (Borkovich & Skovira, 2019). There are four types of social engineering: (1) Physical; (2) Social; (3) Technical; and (4) Socio-technical. Dumpster diving itself is included in the Physical type because the primary purpose of the attacker is to accumulate information about the victim from physical materials (Hijji & Alam, 2021).

Dumpster diving is a form of social engineering attack (Medlin et al., 2008) which describes the activity of "scavenging" the target's waste to find valuable information. Not many people know the amount of information that might be obtained through this way. Some people do not really think about what they throw away at home; credit card statement, medical prescription bottles, bank statement, work-related materials, etc. At work, employees need to be given an understanding that there are people who use waste to get information that is useful to them (Clarke et al., 2021).

This form of attack was increasingly popular during the 1980s, when security was not as good as it is today. The perpetrator of dumpster diving is initially conducted by individuals who have a curiosity about something. These people want to know more about how a product or technology works. They feel that the best way to find out is to dive into the source. The conventional way is to enter a company's office, by requesting sensitive information about a particular product; it is absolutely impossible. The only other way to access that information is to search through it in the trash. Initially, people who feel the need to arouse their curiosity by searching the trash cans are considered to be hackers or crackers. Hackers can be characterized as "people who enjoy using computers and exploring the information infrastructure and systems connected to them". Crackers on the other hand, are classified as "people who maliciously break into information systems and intentionally cause losses in doing so" (Sagar, 2022).

In 1982, Geraldo Rivera warned about electronic delinquents in computer hacking. Rivera unraveled his steps and revealed that it all started from a dumpster located behind an enterprise. This was where Rivera got all the information he needed to access the computer systems of a phone company. At that time, it was called garbology, a term that describes the abandonment of company waste and finding important information such as passwords and other important records written by someone. Trashing is a practice shared by hackers with private detectives, paparazzi, and scavengers who all rate trash as a valuable source of material, including information (Gehl & Lawson, 2022).

Someone who is used to dumpster diving will understand that what he is doing is not Someone who is used to dumpster diving, will understand that it is not fun, but it is a challenge. They are puzzle makers, so even if a document is torn apart, they will reassemble it because they suspect that it must have valuable information. Another consideration is that such activities have minor problems. Most people don't mind when their waste is picked up because it is commonly done by scavengers and the possibility of doing so is legal – as long as they do not trespass their territory.

For a social engineers, dumpster diving has many advantages. He can get enough information to guide his attack on the target company, including memos, meeting agendas, letters, etc. which reveal the name, department, position,

phone number and project assignment. Waste can generate company organization charts, information about company structure, itineraries, and so on. All of those details may seem trivial to insiders, but they may be valuable information to attackers. One can even find all the reports that were discarded due to typos, passwords written on a piece of paper, a folder file full of documents in it, all of which can help one to attack the target (Clarke et al., 2021), including sensitive medical history data discarded in the trash (Khan, et al., 2014). Meanwhile, Siddiqi describes some documents that can be found include: (1) financial reports; (2) Access Codes; (3) Passwords; (4) Meeting Calendars; (5) Equipment Purchase Slip; (6) Phone Numbers;

(7) Network/application diagram; (8) Printed Email; (9) Printed Meeting Documents; (10) Employees and their designation; (11) Credit Card Receipts; (12) Employee Names (Ramjist et al., 2018). Another study conducted on 25 IT practitioners in New Zealand revealed that the impact of dumpster diving was from losing confidential information to funds (Janczewski & Fu, 2010).

Another vulnerability in social engineering attacks is the habit of someone who often disposes of documents in the form of financial statement bills that often reveal sensitive information such as account numbers, credit card numbers, etc. that are potentially used by the attacker to pretend to be victims to gain access to bank accounts or credit cards. Regarding the target companies, whether it is a company engaged in technology, law firm, and pharmaceutical; all have similar vulnerabilities. Application developer companies may dispose of valuable documents related to program code, law firms may create documents relating to specific cases, and pharmaceutical companies may have blueprints of the chemical composition of new drugs that have been under development and have not been marketed.

Not only documents, some people and enterprises frequently dispose of unused computers, laptops or flash drives. Most people think that it is difficult to utilize the data in the device because it has been corrupted or deleted. However, it should be noted that various equipment and software today can easily recover it. It is known that in order to ensure completely erased data, one needs to perform up to 7 stages of the process through a special program. The currently produced hard drive has a built-in program to safely erase data, namely secure erase. However, before it can be used, it is necessary to enable it on the motherboard BIOS because most systems disable this feature by default (Khan et al., 2014).

It becomes a problem if there is no sorting for someone who carries out waste collection activities with the aim of violating the law or other purposes, as stated by scavengers. Scavenger is a person who searches, picks up, takes, collects and looks for waste both individually and in groups, then sold the waste to the collector. Scavengers work to collect used items by crowding unloaded waste of trash trucks, some other scavengers travel around scavenging used items from waste piles (Lehtonen & Pyyhtinen, 2021). Scavengers are not prohibited, but there are limits that govern them. So far, the basis for scavenger and collector permits in Indonesia is regulated in Article 1 number 3 of the Regulation of the Minister of Home Affairs Number 27 of 2009 on Guidelines for Determination of Nuisance Ordinance in Regions. This regulation states that the granting of business/activity permits to private persons/entities in certain locations that may cause harm, loss and disturbance, excluding places/activities is determined by the Central Government or Regional Government. However, it should be noted that a scavenger cannot immediately pick up or scavenge waste because waste management has actually been carried out by the government from the Temporary Shelter (TPS) to the Final Processing Site (TPA). In several Regional Regulations, such as Article 40 of Samarinda Municipal Regulation Number 2 of 2011 on Waste Management, it is confirmed that scavengers are prohibited from dredging or scavenging waste at TPS, except at TPST/TPA. Similar regulation is also seen in Article 28 letter i of Jambi Regulation Number 5 of 2020 on Waste Management which prohibit dredging or scavenging waste at TPS, except by the waste officers.

The provisions described above explain that there is no full prohibition for scavengers to scavenge waste. The definition of scavenger is different from criminal who from the start has a certain intention in scavenging garbage, especially in obtaining important information, while the scavengers do it to resale trash and earn money. In the Regional Regulation that has been mentioned previously, it is also confirmed that there are restrictions related to the activity of dredging or scavenging waste, especially in terms of location, which is not allowed to take waste from a TPS, but allowed in the Final Processing Site with certain conditions, such as Batam Government's effort to collect data on scavengers (Ferza et al., 2019). Therefore, the next discussion will be directed by the waste collection and scavenging activities carried out by people with a specific purpose, especially the perpetrators of crime.

3. Material and Methods

This study uses descriptive qualitative with a statutory, comparative, and conceptual approach. The primary legal material used in this study includes Law Number 27 of 2022 on Personal Data Protection (UU PDP). The secondary legal material used in this study included books, journals, and related articles.

4. Results and Discussion

The main reference to the dumpster diving case will generally lead to an event in 1988, when the United States Supreme Court tried the California v. Greenwood case. William Greenwood, a suspected drug dealer, whose trash had been examined by a janitor at the request of Laguna Beach California police officers. After waste inspection by the police, the evidence related to drug abuse was found. After this discovery, a warrant was issued to allow a search of

Greenwood's residence. This search resulted in findings of evidence related to drug abuse. Greenwood was arrested on drug charges. In the California Supreme Court proceedings, it was stated that, "inhumane waste inspections violate the Fourth Amandment. Furthermore, the court concluded, "the probable cause for the search of Greenwood's residence would not exist without the evidence obtained from the examination of illegal waste, and therefore, all evidence seized from the residence should be stopped and all charges against Greenwood dropped. The United States Supreme Court finally overturned the California Supreme Court's decision by a vote of 6-2. The Panel of Judges of the United States Supreme Court believed that one should not expect any privacy in the waste left for collection. The Panel stated, "it is an open secret that plastic waste bags left or placed on the side of public street are easily accessible to animals, children, scavengers, scouts, and other members of the public." Furthermore it is stated, "What is consciously exposed to the public, even in his own home or office, is not the subject of protection of the Fourth Amandment".

The events above are often used as a basis for the freedom to take anything including the information contained in the goods, so that privacy seems to be contradictory and not even present in a waste. A study was written by Ronald B. Standler regarding Privacy, especially the view of Privacy of Garbage. In his writing, Standler agrees that under certain conditions and certain parties, the police for instance, are allowed to conduct searches and even inspections without a warrant and utilize the information they found to later be used for the sake of law enforcement. However, for the general public, those who are without interest and have certain intentions, it needs to be expressly prohibited because the principle of privacy is attached to the waste, considering that in the waste pile, it is possible to (Khan & Samadder, 2014):

a. Empty prescription medicine bottles, which are always labelled with the individual's name and may be labeled with the name and dosage of the drug, so that someone who searches the trash may infer the individual's medical condition. Particularly in the case of sexually-transmitted diseases or psychiatric disorder, disclosure of the individual's medical condition could cause embarrassment.
b. Credit card receipts, which have the person's name and credit card data; someone who searches the trash could use these data to order merchandise by telephone.
c. Letter that contain confidential information on financial, political, religious, family, or romantic topics.
d. Empty containers of alcoholic beverages, which could be embrassing in a town with a substantial number of people who disapprove of alcohol for religious or moral reasons.
e. Empty boxes for condoms, birth control pill packages, empty containers of spermicide, and other contraceptive materials that could be embarrassing, but are legal to possess and use.
f. Telephone invoice, with a list of all long-distance number called, with the date and duration of the call.
g. Paper indicating membership in political or religious groups.

This view needs to be considered due to the great impact of the use of information obtained from waste. As happened in the 1975 incident, when a journalist from The National Enquirer named Jay Gourley unloaded the trash bins of a member of the United States Secretary of State and National Security Advisor, Henry Alfred Kissinger. From the waste, Gourley then released information including the work schedule of the agents in charge of Kissinger's residence, confidential documents related to secret service activities, documents on the number of arms and ammunition carried by the secret service, and other information (Cooper, 2008; Siddiqi, et al., 2022). In the study conducted in 2018, in 5 hospitals in Canada throughout 2014 to 2016, it was found that out of 591.6 Kg of waste that was recycled, there were 2687 documents included in personal identifiable information (PII) and 1042 were high sensitivity data. In the analysis, these data contain the risk of privacy violation because they do not only contain PII, but also personal health information (PHI) which has actually been protected through The Personal Health Information Protection Act of Ontario (Rombach & Bitsch, 2015). It is not appropriate if in the end the solution offered for individuals to maintain privacy in their waste is to use a document shredder because in some cases the perpetrators even attempt to reconstruct the shredded paper, while other solutions that often offer waste incineration. However, it is also not an easy task to do since it can violate the provisions as stipulated in Article 29 paragraph (1) item g of the Waste Management Law in Indonesia which states that everyone is prohibited from burning waste that is not in accordance with the technical requirements of waste management.

The act of utilizing waste with the aim of violating the law can be carried out in various ways, not only directly scavenging the waste. However, in its development, a company might even purchase waste of other companies by utilizing company cleaners as happened in 2020. Microsoft's competitor, Oracle, has admitted to spying on Microsoft and its partners by digging through their company waste. Oracle is thought to be the actor who pay someone known to have bribed the janitor to get the garbage thrown away by Microsoft's partner company, the Association for Competitive Technology (ACT). A woman who identified herself as Blanca Lopes offered $700 in cash to a janitor for ACT's garbage paperwork. Oracle acknowledged that it hired a detective from Investigative Group International (IGI) to obtain information about the opposition to antitrust lawsuits directed at Microsoft. Oracle CEO, Larry Ellison, is a supporter of the antitrust lawsuit and regularly provides documents to the government to assist with the investigation process. Oracle benefited from the lawsuit and its stock rose by about 4%, making Ellison the richest man in the world at the time (Listokin & Schizer, 2012; El-Gayar & Fritz, 2006).

The debate over privacy and trash cans came back in 2015, when protests were filed by David McMurray over the evacuation and inspection by police officers in Minnesota. The police officers conducted a waste check without a warrant in 2012, after suspected drug use by McMurray. On that basis, McMurray's lawyers assessed that police actions had violated the U.S. constitution, which was also corroborated by the opinions of Judges David Lillehaug and Alan Page who viewed that household trash contained private information, so that there was privacy that needed to be protected.

Unlike the previous case, there was a contradiction that occurred in a motel in Mexico. This similar case related to drug making the police investigation to check waste without a warrant illegal. It was initiated by reports of other motel room neighbor who smelled strong scents, until finally the police conducted a waste check and found the waste associated with the production of drugs. Based on the 4th Amendment of New Mexico Constitution Article II Section 10, the court ruled that garbage has a strong privacy protection value, so any attempt to inspect it requires an official warrant (Cooper, 2008).

From the various events and cases that have been discussed, the author assesses if the general view on waste that has occurred so far, needs to be accompanied by other understandings of the potential for problems or major impacts if it is not supported by privacy protection. Since it is not only about personal data breaches, a person may feel embarrassed because of his/her personal information. However, in this current development, legal violations and financial losses may arise due to the use of information from waste by an individual or organization. In 2020, two perpetrators broke into three regional bank accounts were caught by the South Sumatra Regional Police. The perpetrators used the receipt left at the ATM trash can. If the amount of balance stated is large, the perpetrator will immediately take it. After that, the perpetrator will forge the victim's identity, in the form of ID cards and savings books belonging to the victim until finally they withdraws money to the teller at the bank by saying that they do not bring their cards. This action was first carried out in 2018 at BPD Lampung worth IDR 70 million, then Bank Sultra in Kendari worth IDR 120 Million, and finally Bank Sumsel Babel worth IDR 116 Million. It is known that the perpetrator obtained the victim's data from the voter website owned by the Election Commission (KPU).

The case above illustrates personal information is vulnerable to be used by others who get it from the waste pile. Many people are negligent when throwing away ATM receipts or even throwing away package wraps which still contain all their full personal information on it. Therefore, it is expected that the existing regulations can be considered as a preliminary solution to ensnare the perpetrators of dumpster diving in the future. Legally, the Waste Management Law regulates the management of waste that is against the law as contained in Article 40 which states that:

"Waste management that is unlawful and intentionally conducts waste management activities without regard to norms, standards, procedures or criteria that can result in public health disturbances, security disturbances, environmental pollution, and/or environmental destruction is threatened with imprisonment for a minimum of 4 (four) years and a maximum of 10 (ten) years and a fine of at least IDR 100, 000,000.00 (one hundred million rupiah) and at most IDR 5, 000,000,000, (five billion rupiah)."

There is no further explanation regarding Article 40, but the phrase "resulting in security disturbances" can be interpreted as a result of the use of waste against someone who disposes of it, and there is protection against it. In this regard, if there is personal data obtained from waste, the provisions stipulated in Law Number 27 of 2022 on Personal Data Protection (PDP Law) can be considered. Article 4 paragraph (2) of PDP Law describes personal data including:

(1) health data and information; (2) biometric data; (3) genetic data; (4) criminal records; (5) child data; (6) personal financial data; and/or (7) other data in accordance with statutory provisions. Although it is regulated, it needs to be acknowledged that it is difficult to charge someone who collects information from waste in the form of paper shreds and contains email passwords, a list of company associates' names and even other data that is actually valuable if it is linked to business interests. Because such data can potentially result in losses not only to individuals but corporations. Thus, another determination that can be considered for further use is Article 65 paragraph (1) of the PDP Law which states, "Everyone is prohibited from unlawfully obtaining or collecting personal data that does not belong to him/her with the intention of benefiting himself/herself or others that may result in the loss of personal data subjects", with the threat of imprisonment stipulated in Article 67 paragraph (1) for a maximum of 5 (five) years and/or amend the fine of IDR 5,000,000,000, (five billion rupiah). However, it will be repeated if the provisions of this article continue to use the phrase "personal data" as stipulated in Article 4 paragraph (2), so that further understanding is needed to show the major impact caused by other data as stipulated in Article 4 paragraph (2) if it is misused by unauthorized persons, as stipulated in Article 67 paragraph (3) of the PDP Law which regulates the prohibition of the use of personal data that does not belong to them. If, it is known that the act of taking waste by stealing, because it is within the area of the house or office building, it can consider Article 362 of the Criminal Code concerning theft, Article 167 of the Criminal Code concerning entering people's yards without permission, or even Article 480 of the Criminal Code on detention.

It is necessary to admit, if some of the provisions above are not strong enough to be able to charge the perpetrators of dumpster diving because it is difficult to ascertain one's intentions in scavenging waste, until it proves the use of such information for unlawful purposes. Although it is trash, if its use can cause harm to its owner, the law should provide protection against it. The problem of obtaining information through waste and objects that have been disposed of should be separated between the physical objects that may become the ownership of other parties, but the information contained in it remains inherent and becomes the privacy rights of the owner. Therefore, the use of

information obtained through waste without rights should be specifically regulated with sanctions. The description above is expected to become a consideration for future studies on dumpster diving, so that it triggers the establishment of regulations that provide legal certainty and legal protection for individual from the use of information obtained from waste that has been disposed of.

In conclusion, a description that can be considered in the use of waste for unlawful purposes can be analogous as follows:

"If a homeowner leaves the house key while on vacation to the security officer, does the security officer who officially obtained the key and under his control have the right to enter the house at any time and make use of the house, or if someone found a house key belonging to another person, does he has the right to enter the house under the pretext of the control of the house key?"

5. Conclusion

This issue should be a common concern that the trivial view of waste that has been going on so far can potentially harm someone in the future. The perpetrators of dumpster diving are a serious threat due to the lack of regulations that can charge them, as well as the low awareness of people in disposing of waste containing personal information. The Waste Management Law, the Personal Data Protection Act, and the Criminal Code cannot provide full protection for victims, due to the absence of specific rules containing the principle of privacy protection for someone in their waste.

Acknowledgments

Thank you to the Ministry of Education, Culture, Research and Technology of the Republic of Indonesia for funding the research team of the author through the Higher Education Basic Research Grant Program (PDUPT) for the 2022 period, until finally making it the material for writing this paper.

References

Alghazo, J., Ouda, O. K., & Hassan, A. E. (2018). E-waste environmental and information security threat: GCC countries vulnerabilities. *Euro-Mediterranean Journal for Environmental Integration*, *3*, 1-10.

Al-Kassimi, K. (2021). De-Historicizing (Mainstream) Ottoman Historiography on Tanzimat and Tahdith: Jus Gentium and Pax Britannica Violate Osmanli Sovereignty in Arabia. *Histories*, *1*(4), 218-255.

Borkovich, D. J., & Skovira, R. J. (2019). Cybersecurity Inertia And Social Engineering: Who's Worse, Employees Or Hackers?. *Issues in Information Systems*, *20*(3).

Clarke, L., Arnett, S., Bukhari, W., Khalilidehkordi, E., Jimenez Sanchez, S., O'Gorman, C., ... & Broadley, S. A. (2021). MRI patterns distinguish AQP4 antibody positive neuromyelitis optica spectrum disorder from multiple sclerosis. *Frontiers in neurology*, *12*, 722237.

Cooper, A. S. (2008). Showdown at Doha: The secret oil deal that helped sink the Shah of Iran. *The Middle East Journal*, *62*(4), 567-591.

El-Gayar, O., & Fritz, B. D. (2006). Environmental management information systems (EMIS) for sustainable development: a conceptual overview. *Communications of the Association for Information Systems*, *17*(1), 34.

El-Gayar, O., & Fritz, B. D. (2006). Environmental management information systems (EMIS) for sustainable development: a conceptual overview. *Communications of the Association for Information Systems*, *17*(1), 34.

Ferza, R., Hamudy, M. I. A., & Rifki, M. S. (2019). Public Private Partnership of Waste Management in West Java. *BISNIS & BIROKRASI: Jurnal Ilmu Administrasi dan Organisasi*, *26*(2), 4.

Gehl, R. W., & Lawson, S. T. (2022). *Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulativ e Communication*. MIT Press.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., ... & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*, *74*, 4986-5002.

Gregg, M., Watkins, S., Mays, G., Ries, C., Bandes, R. M., & Franklin, B. (2006). *Hack the stack: Using snort and ethereal to master the 8 layers of an insecure network*. Elsevier.

Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. *Ieee Access*, *9*, 7152-7169.

Janczewski, L. J., & Fu, L. (2010, October). Social engineering-based attacks: Model and new zealand perspective. In *Proceedings of the international multiconference on computer science and information technology* (pp. 847-853). IEEE.

Khan, D., & Samadder, S. R. (2014). Municipal solid waste management using Geographical Information System aided methods: A mini review. *Waste management & research*, *32*(11), 1049-1062.

Lehtonen, T. K., & Pyyhtinen, O. (2021). Living on the margins: dumpster diving for food as a critical practice. *Distinktion: Journal of Social Theory*, *22*(3), 441-463.

Listokin, Y., & Schizer, D. M. (2012). I like to pay taxes: Taxpayer support for government spending and the efficiency of the tax system. *Tax L. Rev.*, *66*, 179.

Lu, W., Chen, X., Peng, Y., & Shen, L. (2015). Benchmarking construction waste management performance using big data. *Resources, Conservation and Recycling*, *105*, 49-58.

Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the vulnerability of US hospitals to social engineering attacks: how many of your employees would share their password?. *International Journal of Information Security and Privacy (IJISP)*, *2*(3), 71-83.

Ramjist, J. K., Coburn, N., Urbach, D. R., Govindarajan, A., Armstrong, K. A., Scott, A. L., & Baxter, N. N. (2018). Disposal of paper records containing personal information in hospitals. *JAMA*, *319*(11), 1162-1163.

Rombach, M., & Bitsch, V. (2015). Food movements in Germany: Slow food, food sharing, and dumpster diving. *International Food and Agribusiness Management Review*, *18*(1030-2016-83042), 1-24.

Sagar, R. (Ed.). (2022). *The Progressive Maharaja: Sir Madhava Rao's Hints on the Art and Science of Government*. Oxford University Press.

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, *12*(12), 6042.