International Journal of Applied Research and Sustainable Sciences (IJARSS)
Vol. 3 No. 2, 2025: 145 - 164

Protection Against Digital Crimes in E-Commerce Transactions

Marifah Marifah[1]*, Sami Ben Slama[2], Rofaat Ruyati[3], Muhammad Ribhi Safari[4]
[1*3]Master of Law Program, Sultan Adam School of Law, Indonesia
[2] King Abdul Aziz University, Jeddah, Kingdom of Saudi Arabia
[3-4]University of Lambung Mangkurat, Indonesia
Corresponding Author: Marifah Marifah marifah@stihsa.ac.id

A R T I C L E I N F O

Keywords: Regulation, Personal Data Protection, Sustainability, E-Commerce

Received : 13 December 2024
Revised : 14 January 2025
Accepted: 17 February 2025

A B S T R A C T

This study looks at the critical role that consumer data protection legislation play in ensuring the security of electronic transactions. Personal data protection has emerged as a critical concern in preserving public trust in the e-commerce industry. The purpose of this study is to understand the ratio legis of existing legal regulations in accommodating and addressing various forms of digital crimes such as hacking, malware dissemination, data theft, online fraud, and online gambling; to assess the feasibility of the Personal Data Protection Law in relation to technological advancements; and to thoroughly examine the legal measures regulating digital crimes for the security of personal data for e-commerce transaction users in the new Indonesian Penal Code (KUHP). This study uses a normative-empirical legal approach that combines legal framework analysis through case studies analyzed using qualitative analysis methods, referring to existing literature from both National and International databases, as well as case studies from several countries that illustrate the practical application of personal data protection regulations based on judicial considerations in the context of evaluating personal data protection policies.

Research results show that although Indonesia has the Law Number 27 of 2022 on Personal Data Protection (PDP Law), there are still issues in its implementation, law enforcement, and monitoring, particularly in the context of e-commerce transactions. Strengthening regulations and harmonizing policies with international standards are necessary to create a sustainable personal data protection system. Thus, an active role from the government is needed regarding strict enforcement mechanisms, enhancing digital literacy among businesses and consumers, and tighter supervision of user data collection and processing practices in e-commerce to ensure sustainable protection.

INTRODUCTION

Protecting personal information is guaranteed under the constitution. Article 28G, paragraph (1) of the 1945 Constitution of the Republic of Indonesia, guarantees the protection of personal data for Indonesian citizens. It states that everyone has the human right to personal, family, honor, dignity, and property protection under their control, as well as the right to feel secure and protected from threats and the fear of acting or not acting. As human rights, privacy rights are safeguarded by international legal accords. The right was maintained by the Constitutional Court as part of personal data protection in Decision Number 20/PUU-XIV/2016. The Constitutional Court Decision Number 5/PUU-VIII/2011 states that data protection and privacy are two different concepts. The right to personal data protection is a perspective of human rights and falls under the right to privacy, including information privacy and data privacy. According to the Indonesian Internet Service Providers Association (APJII, 2024), the number of internet users in Indonesia reached 221,563,479 in 2024, or 79.5% of the total population of 278,696,200 in 2023. This finding shows an increase in internet penetration of 1.4% from the previous period. According to APJII, this positive trend shows consistent improvement and significant growth over the past five (5) years. Indonesia's internet penetration has experienced rapid growth since 2018. It reached 64.8% in 2018, rising to 73.7% in 2020, 77.01% in 2022, and 78.19% in 2023. The protection of consumer personal data is very important in e-commerce to prevent information misuse and avoid security risks such as identity theft by irresponsible parties for unlawful purposes, such as fraud, spamming, and phishing attacks.

E-Commerce is one of the trade industries that does not require physical signatures and instead conducts transactions using technology or marketplace platforms such as websites, smartphone applications, and social media. The combination of information technology development and worldwide improvements increases commerce capacity via Electronic Commerce (E-Com) or Electronic Business (E-Bis). However, the expanding contacts and transactions in the e-commerce industry for business actors and consumers in Indonesia pose severe issues about the protection of consumer personal information, as customers are required to disclose personal information in order to transact on e-commerce platforms.

Various data breach risks in e-commerce, including credit card data theft and other personal information, make it important to understand techniques to reduce these potential risks and minimize the impact of data breaches on consumers and businesses (Yadav, M., & Suri, P. (2020).

Challenges in Protecting Personal Data in E-Commerce Transactions

1. Risk of Data Breach and Misuse: In e-commerce transactions, personal customer data such as names, addresses, credit card numbers, and payment information are frequently targets of cyber attacks. The possibility of data breaches influences the complexity of transactions and the use of multiple digital platforms or merchants. Hacking, malware, and security system mistakes can all lead to data breaches. Data usage by irresponsible parties also offers a risk, including fraud, identity theft, and unlawful marketing.

Data breaches can damage consumer trust and influence their purchasing behavior, thereby increasing potential risks for e-commerce companies (Acar, G., & Yalçınkaya, A. (2020).Data privacy breaches (including data leaks) can lead to the loss of customer loyalty and a decrease in trust in e-commerce platforms (Sharma, S., & Joshi, M. (2021).In addition to data loss, data breaches can significantly damage a company's reputation, ultimately leading to a decrease in the number of customers and revenue (Tritsini, E., & Papageorgiou, A. (2022).The importance of data encryption as a protective measure to reduce the risk of data breaches in e-commerce transactions (Wang, X., & Chen, L. (2022).

2. The security threat's source: Emerging cyber threats, including more sophisticated phishing attacks, disguised malware, and threats from attacks on IoT systems, make it important to have various security solutions and technologies that can be used to protect systems from these threats (Rashid, U., & Iqbal, M. (2020). Various threats faced by IoT devices connected to e-commerce platforms, such as devices vulnerable to exploitation by hackers and malware, require various solutions to enhance IoT security and protect consumer data (Hassan, W., & Ali, S. (2022). Threats to personal data can come from various sources, including phishing attacks, malware, or even negligence in managing security systems by e-commerce operators, thus mitigation techniques that can be applied (Tian, Y., Liu, Y., & Sun, J. (2021). Threats to critical infrastructure that endanger the e-commerce sector and others, such as attacks on energy systems, transportation, and information systems, require measures to be taken to reduce cyber threats to that infrastructure (Zhao, Y., & Xu, X. (2020). Various threats faced by cloud computing platforms, such as access abuse, data breaches, and attacks on cloud infrastructure, necessitate solutions and mitigation measures that can be implemented to protect the cloud environment (Salloum, S. A., & Al-Sayyed, R. (2021).Various types of security threats, including ransomware, DDoS attacks, and intrusions carried out by hackers, impact business sustainability in the technology and e-commerce sectors (Agarwal, A., & Rathi, S. (2020). The impact of increasing ransomware and malware attacks on the e-commerce sector targets user and company data, as well as the latest technologies used to combat these threats (Zhang, Y., & Yang, Z. (2021). Advanced Persistent Threats (APTs), which are more sophisticated and harder to detect threats, often originate from state actors or organized groups. How APTs can attack e-commerce systems and the mitigation measures that companies must take (Hasan, H. R., & Ibrahim, M. (2021). Threats faced by e-commerce platforms, including common cyber attacks such as SQL injection, cross-site scripting (XSS), and attacks on network infrastructure. This requires security techniques and protocols that can be used to reduce its vulnerabilities (Kumar, A., & Singh, M. (2022). The challenges faced by SMEs (Small and Medium Enterprises) in implementing cybersecurity policies. Factors such as limited resources, lack of awareness about cyber threats, and difficulties in complying with regulations are the main obstacles in implementing effective security (Doherty, N. F., & Malone, J. (2020). The challenges in implementing security frameworks to protect critical infrastructure, such as energy systems, transportation, and healthcare services, still include

difficulties in aligning security policies and practices across various industrial sectors (Matsumoto, K., & Kikuchi, H. (2020).

The ease of transactions in the field of computer technology and telecommunications is vulnerable to attacks and high risks in the world of cyberspace, which undoubtedly necessitates legal regulations to govern all activities that occur within it and impose sanctions on parties that violate personal data regulations and cause harm to others, as well as how e-commerce actors must comply with data protection regulations to maintain consumer privacy and trust.

How may International regulations affect privacy and data security in e-commerce? How can organizations and the government address this issue by adopting more integrated and modern technology-based solutions?

The purpose of this study is to understand the ratio legis of existing legal regulations in accommodating and addressing various forms of digital crimes such as hacking, malware dissemination, data theft, online fraud, and online gambling; to assess the feasibility of the Personal Data Protection Law in relation to technological advancements; and to thoroughly examine the legal measures regulating digital crimes for the security of personal data for e-commerce transaction users in the new Indonesian Penal Code (KUHP).

LITERATURE REVIEW

1. Legal Protection

There are two sorts of legal protection based on their source: internal protection and external protection. Internal legal protection can be accomplished by the parties when their legal situations are relatively balanced, which means they have equal negotiating power, and the parties have the freedom to express their will in accordance with their interests under human rights. This serves as the foundation when the parties construct the agreement clauses, allowing legal protection to be tailored to the parties specific needs. External legal protection established by authorities through rules can protect the interests of the weaker party. Legislation must be balanced and unbiased.

The other party must likewise receive proportionately balanced legal protection as soon as possible. Because the party that was initially powerful may end up being the one who feels wronged after an agreement is reached. For instance, the creditor needs legal protection when the debtor abuses their rights. The parties are proportionately protected by the legal framework (Isnaeni, 2017). It is currently recognized that the legal protections afforded to consumers do not balance the interests of business owners and consumers. This is demonstrated by the fact that business actors have more economic factors than consumers, which frequently leads to injustice when customers and business actors disagree (Kristiyanti, Celina Tri Siwi, 2009).

2. Law Enforcement

Prayuti (2024), Legal and regulatory aspects, the Consumer Protection Law and the Electronic Information and Transactions Law (ITE Law), are very important for maintaining consumer security and trust in supporting law enforcement and justice for buying and selling transactions.The complexity of

collecting and validating digital evidence has become the main obstacle in effectively resolving these cases. Law Number 1 of 2024 on Information and Electronic Transactions strengthens consumer protection aspects in electronic transactions. Article 26B emphasizes the obligation of electronic system organizers to maintain the confidentiality, integrity, and availability of consumer personal data. This article also states that organizers who neglect to maintain the security of personal data may be subject to administrative and criminal sanctions, providing stronger protection for consumers.

As a result, the application of law and consumer protection in the digital sphere may undergo major changes (Rambe et al., 2023). Article 46 of the ITE Law recognizes the usefulness of electronic evidence in law enforcement. Another problem is ensuring that law enforcement agents understand how to properly use and present electronic evidence in court. Article 50 regulates international collaboration, which is acknowledged as an important component in the execution of the ITE Law. It is envisaged that by using a more comprehensive and coordinated strategy, Indonesian law enforcement will be able to better address the increasingly complex and sophisticated challenges of cybercrime.

METHODOLOGY

This study uses a normative-empirical legal approach that combines legal framework analysis through case studies analyzed using qualitative analysis methods, referring to existing literature from both National and International databases, as well as case studies from several countries that illustrate the practical application of personal data protection regulations based on judicial considerations in the context of evaluating personal data protection policies.

The use of the normative-empirical legal approach method in research refers to the manner or structure of writing the study findings. The creation of successful techniques for the prevention and resolution of digital crimes in e-commerce transactions necessitates a complete technological and legal approach. In addition, this study will evaluate the substantive justice of each item regulating digital crimes by determining if the existing restrictions are appropriate or require consistency.

RESEARCH RESULT AND DISCUSSION

1. International Regulations Governing Personal Data Protection in E-Commerce

The data protection system began in Europe due to a lack of a clear definition of privacy and personal life, as outlined in Article 8 of the European Convention. Germany was the first country to implement the Data Protection Act in 1970, followed by the United Kingdom and several other European countries, including Sweden, France, Switzerland, and Austria. A similar development occurred in the United States, with the Fair Credit Reporting Act of 1970, which also included data protection provisions.

The important advance in data protection law happened in 2016, when the European Union harmonized its data protection regulations under the EU General Data Protection Regulation (GDPR), which went into effect on May 25,

2018. This law covers how data controllers manage and store identifiable personal data, both within and outside of the European Union. The GDPR highlights the significance of the foundation for data processing. The GDPR also gives data subjects the right to access their personal information, request data deletion, and have their data treated fairly and transparently. Noncompliance with these laws can result in significant fines of up to 4% of annual income or €20 million, whichever is greater.

GDPR is extensive, governing practically all aspects of personal data processing. Furthermore, its implementation will have an impact not just on data controllers and processors headquartered in the European Union, but also on those who provide products or services to or monitor the behavior of European Union people. The GDPR is founded on data protection principles such as legality, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability. This rule applies to entities that process EU citizens' personal data, including third-party service providers and monitors of EU citizens' activities. GDPR replaces the Data Protection Act 1998 as a consequence of digital transformation. GDPR requires certain firms that meet the criteria to designate a Data Protection Officer. A DPO is essential if the organization processes sensitive data on a significant scale or regularly monitors individuals. In general, organizations, as data controllers, must manage data in line with these standards and establish the legal basis for data processing. Organizations must also have clear privacy policies. Risk reduction, effective human resource planning, and data security are critical for minimizing the risk of data breaches and ensuring GDPR compliance.

Compare the personal data protection regulations implemented in various regions of the world, focusing on the General Data Protection Regulation, California Consumer Privacy Act, and similar regulations in Asia and Latin America. The authors examine how e-commerce companies in each region manage compliance with regulations (López, C., & Pérez, J. (2022). The impact of personal data protection laws such as the General Data Protection Regulation and the California Consumer Privacy Act on e-commerce operations. The authors provide an analysis of the difficulties faced by companies in complying with these regulations, as well as the strategies used to ensure compliance (Liu, Y., & Zhang, H. (2022).Challenges in compliance with the General Data Protection Regulation, California Consumer Privacy Act by global e-commerce companies. The development of privacy and personal data security regulations in e-commerce across various countries, including the implementation of the General Data Protection Regulation, California Consumer Privacy Act, and similar laws (Zhao, S., & Liu, Y. (2023). Challenges and opportunities in compliance with personal data protection regulations, particularly the General Data Protection Regulation in the e-commerce sector. This study also discusses the efforts made by e-commerce companies in Europe and outside Europe to ensure compliance with regulations (Tung, H. T., & Nguyen, H. K. (2023).

The Italian Data Protection Authority for Child Protection further said that OpenAI did not provide an age verification system to prevent minors under 13 from viewing potentially inappropriate AI content. GDPR ensures stringent

protection of child data. Recital 38 Special Protection of Personal Data Children claim that they have the right to enhanced protection for their personal data. Because they may be less aware of the risks, implications, and safeguards involved, as well as their rights regarding the processing of their personal data. Special protection must be provided for the use of children's personal data for marketing purposes, personality profiling, or user profiling, as well as the gathering of personal data about children when they utilize services given directly to them. Consent from guardians or parents is not required for preventive services or counseling provided directly to children. Article 8 of the GDPR specifies the conditions for children's consent in respect to services given directly to them. Processing a kid's personal data is considered lawful if the youngster is at least 16 years old. If the kid is under the age of 16, the processing will be lawful only if the child's parent or guardian gives consent or authorizes it. GDPR allows member states to choose a lower age for this reason based on their national laws. With the condition that the lower age be no less than 13 years. GDPR also requires data controllers to make reasonable attempts to verify and get consent from the responsible person or the child's parent, while taking into account available technology.

2. The National Personal Data Protection Regulation

Personal data protection legislation vary by country, but all require e-commerce firms to maintain consumer data in a safe and transparent manner. The Indonesian personal data protection regulation mandates every institution that gathers personal data to manage it with care and only use it for legitimate purposes.

Provision Article 1 number 4 of Law Number 27 of 2022 on Personal Data Protection contains articles that impose obligations on Personal Data Controllers. The data controller according to the Personal Data Protection Law is any person, public body, or international organization that acts independently or jointly in determining the purposes and controlling the processing of Personal Data. The data controller here can be either the government or the private sector. From the government, for example, there is the Directorate General of Population and Civil Registration, Ministry of Home Affairs, which records the personal data of residents for the interests of the state or the public. Meanwhile, from the private sector, a marketplace can be one of the examples. Because, in order to use or access all of the services supplied, the public must supply personal information. According to Article 35 of the Personal Data Protection Law, Data Controllers must protect and ensure the security of the Personal Data they process by preparing and implementing operational technical measures to protect Personal Data from processing disruptions that violate statutory regulations, as well as determining the level of security for Personal Data by considering the nature and risks of the Personal Data that must be protected in the processing of Personal Data.

Article 39 of the Personal Data Protection Law states that:

(1) The Data Controller must prevent Personal Data from being accessed unlawfully;

(2) Prevention as referred to in paragraph (1) is carried out with a security system for Personal Data that is processed and or processes Personal Data in an electronic system reliably, safely, and responsibly.
(3) Prevention as referred to in paragraph (2) is carried out in accordance with the provisions of the laws and regulations.

Article 46
(1) In the event of a Personal Data Protection failure, the Personal Data Controller is required to provide written notification no later than 3 x 24 (three times twenty-four) hours to:
a. the Data Subject;
b. the institution;
(2) The written notification as referred to in paragraph (1) must at least contain: the Personal Data that has been disclosed; when and how the Personal Data was disclosed; and the efforts to handle and recover from the disclosure of Personal Data by the Personal Data Controller.

Article 65
(1) Every person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to them with the intent to benefit themselves or others, which may result in harm to the Data Subject.
(2) Everyone is prohibited by law from disclosing Personal Data that does not belong to them;
(3) Every person is prohibited from unlawfully using Personal Data that does not belong to them.

Article 66 states that every person is prohibited from creating false Personal Data or falsifying Personal Data with the intent to benefit themselves or others, which may result in harm to others.

Article 67
(1) Anyone who intentionally and unlawfully obtains or collects Personal Data that does not belong to them with the intent to benefit themselves or others, which may cause harm to the Personal Data Subject as referred to in Article 65 paragraph (1), shall be punished with imprisonment for a maximum of 5 (five) years and/or a fine of up to Rp5,000,000,000.00 (five billion rupiah).
(2) Any person who intentionally and unlawfully discloses Personal Data that does not belong to them as referred to in Article 65 paragraph (2) shall be punished with imprisonment for a maximum of 4 (four) years and/or a fine of up to Rp4,000,000,000.00 (four billion rupiah).
(3) Anyone who intentionally and unlawfully uses Personal Data that does not belong to them as referred to in Article 65 paragraph (3) shall be punished with imprisonment for a maximum of 5 (five) years and/or a fine of up to Rp5,000,000.00 (five billion rupiah).

Article 68 states that any person who intentionally creates false Personal Data or forges Personal Data with the intent to benefit themselves or others, which may result in harm to others as referred to in Article 66, shall be punished

with imprisonment for a maximum of 6 (six) years and/or a fine of up to Rp 5,000,000,000.00 (five billion rupiah).

Article 69 states that in addition to the penalties as referred to in Article 67 and Article 68, additional penalties may also be imposed in the form of confiscation of profits and/or assets obtained or derived from the crime and payment of compensation.

Based on those provisions, the marketplace has an obligation to secure personal data. However, if there is a data breach, the marketplace, as the data controller, is required to notify consumers whose information has been compromised by an irresponsible party. In addition, the marketplace may face administrative measures such as a written warning, temporary suspension of Personal Data processing activities, erasure or destruction of Personal Data, and/or administrative fines.

As specified in Article 57 of the Personal Data Protection Law. Meanwhile, the terms of Government Regulation 71 of 2019 governing Electronic System Organizers may be subject to consequences such as written warnings, administrative fines, temporary suspension, access termination, and/or removal from the list. In the event of a breach of consumer personal data, the consumer may register a complaint with the Minister over the failure to maintain the confidentiality of personal information. This article is connected to Article 26 letter b, which provides that data owners have the right to register a complaint with the Minister about a failure to secure their personal data. Furthermore, consumers as the aggrieved party can launch a legal complaint against the marketplace on the grounds. In terms of negligence, Article 1366 of the Civil Code specifies that every person is liable not only for damages produced by their actions, but also for losses caused by negligence or carelessness. Article 1366 of the Civil Code states that a person can be held legally liable not only for damages produced by their own conduct, but also for negligence that causes harm to others. According to Article 64 of the Personal Data Protection Law, disputes can be resolved by arbitration, courts, or alternative dispute resolution institutions that follow applicable procedural law and statutory regulations, and are supported by sufficient evidence.

3. **Responsibility for Personal Data Management by Business Actors**

How should businesses and operators maintain personal data in accordance with data protection and privacy regulations?

According to the Personal Data Protection regulation, e-commerce companies must seek customer consent before collecting personal data, inform them of the purpose of data collection, and give consumers the ability to access and erase their data. Businesses must also have proper security measures to prevent data leaks. The responsibility of data controllers, as defined in Article 4 of the Personal Data Protection Law, defines the obligations of parties who manage personal data, such as businesses or institutions. They must keep the stored data secure, be responsible for its usage, and not spread it without the owner's consent. If there is a data breach, the data manager must notify the appropriate authorities or risk legal consequences, such as hefty fines or criminal

charges. Another rule requires the data owner to provide explicit consent before their data is collected and handled by the company. This means that organizations can no longer access or use user data without their knowledge or permission.

The obligations of e-commerce operators in Indonesia in managing personal data based on the newly enacted Personal Data Protection Law and identifying the main obligations related to the collection, use, and deletion of customer personal data as well as compliance with existing regulations (Kurniawan, A. S., & Pratama, I. A. (2022). The obligations that business operators have in managing consumer personal data in accordance with the regulations in force in Indonesia, including the PDP Law and other regulations. The challenges faced by business operators in the e-commerce sector in complying with these regulations (Rahman, A., & Santosa, P. (2022). The obligation of business actors to manage personal data in accordance with the Personal Data Protection Law (UU PDP) in Indonesia. Analysis of the challenges and implementation of personal data management obligations by digital platforms in Indonesia (Putri, R. A., & Setiawan, D. (2023).The obligation of business actors in implementing personal data protection policies on e-commerce platforms in Indonesia. Analysis of the implementation of policies under the PDP Law and the challenges faced by business actors in managing personal data (Budi, A. R., & Suhartono, T. (2023). The obligations of business operators in managing personal data in the digital market. How businesses must fulfill personal data management obligations through policies and procedures that ensure compliance with regulations such as GDPR and CCPA (Harrison, P., & Fitzgerald, J. (2022). The obligations of businesses in managing personal data according to the General Data Protection Regulation in Europe and the California Consumer Privacy Act in the United States. The main obligations of companies in terms of transparency, consent, and consumer data protection (Smith, A. L., & Tang, X. (2022). The obligations that businesses have in managing personal data in the e-commerce sector, with a focus on global data protection policies, including GDPR and other international standards, as well as the challenges of implementing these policies in various countries (Tao, Z., & Liu, L. (2022). The obligations of businesses in managing personal data, particularly in the context of GDPR regulations and other regulations in Europe. Challenges in complying with personal data management obligations, such as data collection, storage, and deletion, as well as the implementation of appropriate privacy policies (Mikkonen, T., & Laukkanen, T. (2023). The role of data controllers in managing personal data in the context of e-commerce and the obligation to protect personal data, including notification obligations, access rights, and data deletion in various global personal data regulations (Wang, Y., & Zhang, R. (2023).

In Case 1:

Facebook (Meta) violated GDPR in 2018. In 2018, the European Commission fined Facebook (now Meta) €110 million for failing to properly inform users about the data merger between Facebook and WhatsApp. This case demonstrates how infractions of data protection legislation, such as the General Data Protection Regulation (GDPR) for the European Union, can result in harsh penalties. Meta

was chastised for failing to warn consumers that their data will be used more extensively following the acquisition of WhatsApp, which violated GDPR regulations requiring transparency and user control over their personal data.

In Case 2:
Facial recognition: Italian SA fines Clearview AI EUR 20 million
Background information

Final decision date: February 10, 2022 Cross-border case or national case: national case, Article 3(2) applies Controller: Clearview AI Inc. Legal References: Principles related to the processing of personal data (Article 5(1)(a)(b)(e)); Lawfulness of processing (Article 6); Processing of special categories of personal data (Article 9); Transparent information, communication, and modalities for the exercise of data subjects' rights (Article 12); Information to be provided when personal data is collected from the data subject (Article 13); Information to be provided when personal data has not been obtained from the data subject (Article 14); Right of access by the data subject (Article 15); Representative of the controller not established in the Union (Article 27). Decision: SA Italia imposed a fine of EUR 20 million, enforced a ban on further collection and processing, ordered the deletion of data, including biometric data, processed by the Company's facial recognition system related to individuals in the territory of Italy, and the appointment of a representative in the European Union territory. Keywords: Web Scraping, Image Database, Facial Recognition, Biometric Data, AI System, Geolocation, Jurisdiction under EU Law, Representative in the EU.

Summary of Decision
Origin of the Case

SA Italia initiated a lawsuit on its own initiative after receiving press reports about multiple concerns with Clearview AI Inc's facial recognition technologies. Furthermore, in 2021, Garante got four complaints and two cautions from two groups operating in the fields of privacy protection and individual fundamental rights against Clearview.

Main Findings

SA Italia conducted investigations and assessments that revealed various infractions by Clearview AI Inc. The company's personal data, including biometric and geolocation information, was handled unlawfully and without the necessary legal basis because the US-based company's legitimate interests do not qualify. Furthermore, the corporation breached several important aspects of the GDPR, such as transparency and purpose limitation.

Decision

SA Italia imposed a fine of EUR 20 million. In addition, SA Italia: SA Italia issued a fine of EUR 20 million. SA Italia will:

1) Prohibit web scraping of images and metadata related to individuals in Italy, as well as further processing of standard and biometric data handled by the Company through facial recognition systems.

2) Regularly delete data, including biometric data, processed by facial recognition systems related to individuals in the territory of Italy, is subject to the obligation to promptly respond to requests for the exercise of rights based on Articles 15 to 22 of the Regulation that may have been received from data subjects in accordance with Article 12 (3) of the Regulation;
3) Ordering the Company to appoint a representative in the European Union area. (EDPB, 2022)

In Case 3:

Elon Musk brings Microsoft into his latest lawsuit against OpenAI

Elon Musk, a tech tycoon, has increased his lawsuit against OpenAI. He also filed federal antitrust and other allegations, and named Microsoft, OpenAI's major financial sponsor, as a defendant. Quoted from Reuters. Elon Musk's complaint, filed on Thursday, November 14, 2024, in federal court in Oakland, California, alleges that Microsoft and OpenAI are illegally attempting to monopolize the generative artificial intelligence industry and remove competitors. According to the extended case, OpenAI and Microsoft violated antitrust rules by requiring investment opportunities in exchange for pledges not to work with the company's competitors. It was suggested that the company's exclusive license deal is a merger that does not require regulatory permission. (Tempo, 2024)

Elon Musk asks the federal court to prohibit OpenAI from seeking profit

Elon Musk has petitioned a federal court to prevent the American artificial intelligence company OpenAI from becoming a solely profit-driven enterprise. According to CNBC International, Elon Musk is now establishing his own artificial intelligence business, xAI. Shivon Zilis, the lawyer for Musk, filed a preliminary ruling against OpenAI. The verdict also prohibits OpenAI from allegedly asking its investors not to support competitors such as xAI and others. The most recent court documents reflect an increase in the legal dispute between Musk, OpenAI, and its CEO Sam Altman, as well as other parties and supporters who have previously been involved, such as tech billionaire Reid Hoffman and Microsoft. Musk initially sued OpenAI in San Francisco state court in March 2024, but then withdrew the action and re-filed it in federal court six months later. Musk's lawyers stated in their case that OpenAI had broken federal racketeering laws, or RICO.

In mid-November, they expanded the complaint to include charges that Microsoft and OpenAI had broken antitrust laws. The reason for this is that OpenAI purportedly requested that investors refrain from investing in competitive companies, including Musk's most recent startup, xAI. OpenAI has emerged as one of the most successful startups in recent years. ChatGPT has also grown in popularity, helping to pique major companies' interest in AI. OpenAI began as a non-profit organization in 2015 before transitioning to a limited-profit model firm in 2019, with the non-profit OpenAI controlling its profit-seeking subsidiaries. The company is in the process of being converted into a traditional profit-seeking company, which may make it more appealing to investors. The restructuring plan will also allow. (CNBC Indonesia, 2024)

In Case 4:

The Italian Privacy Authority imposed fines for ChatGPT violations

On Friday, December 20, 2024, the Italian Data Protection Authority (*Garante Per la Protezione Dei Dati Personali*) fined OpenAI OpCo, LLC 15 million Euros, which is equivalent to more than IDR 252 billion. The fine was levied because the corporation failed to comply with GDPR in the management of ChatGPT. Garante further stated that ChatGPT failed to protect children while operating the AI-powered digital platform. The ruling's concerns included infractions such as insufficient legal grounds for data processing, failure to comply with user data transparency principles, and inadequate age verification.

The sanction was levied following an investigation that began in March 2023 and was based on the European Data Protection Board's Opinion of December 28, 2024. OpenAI was also directed to launch a six-month campaign promoting data privacy and ChatGPT user rights. "OpenAI Fined by Italian Privacy Watchdog for ChatGPT Violations". According to an inquiry report by the Italian government, OpenAI exploited personal data from ChatGPT users in Italy to train the chatbot's algorithm. OpenAI received a fine for the infractions committed by ChatGPT.

This case joins a string of litigation against OpenAI, which runs the generative AI system ChatGPT, including copyright claims in the United States. ChatGPT is now being investigated and is drawing the attention of regulators in the United States and Europe. According to Newsweek, the probe began last year in response to complaints that OpenAI processed personal data without proper legal grounds and did not meet transparency criteria. However, an OpenAI spokeswoman noted that the business has been working to collaborate with privacy authorities since the Garante ordered the suspension of ChatGPT services in Italy in 2023. This fine is unreasonable, being roughly 20 times the revenue earned in Italy throughout the relevant period. OpenAI reiterates its commitment to continue working with worldwide authorities to develop AI that respects personal rights.

Appeal Level

Facing this sanction, OpenAI intends to challenge the penalties imposed on it.This phenomenon should act as a warning to all generative AI developers worldwide. According to Euro News, "Italy's privacy watchdog fines OpenAI €15 million after probe into ChatGPT data collection," in an email statement, OpenAI labeled the judgment "disproportionate" and announced an appeal. A representative for OpenAI stated that the amount was approximately 20 times the company's revenue in Italy the same year. In its statement, OpenAI also offered to collaborate on the application of beneficial AI that respects privacy rights. (Kompas, 2024).

3. The Importance of Compliance and Law Enforcement:

Legal protection is the implementation of the function of law to achieve social order, which leads to certainty and impacts public order. Article 28D paragraph (1) states that "Everyone has the right to recognition, guarantee, protection, and legal certainty that is fair, as well as equal treatment before the

law." The law can function and play a role through the assistance of legislation, court rulings, or a combination of both.The formation of legislation is the most rational and quickest way compared to other methods of legal development such as jurisprudence and customary law (Mochtar Kusumaatmadja dan B. Arief Sidharta, 2013).

Ministerial Regulation Number 20 of 2016 on Personal Data Protection also governs the procedures for resolving disputes, as described in Articles 29–33. Its regulations allow consumers to make a complaint with the Ministry of Communication and Information about a failure to protect personal data. Consumers must make a complaint with the Ministry of Communication and Information within 30 days of becoming aware of the failure to secure their personal data. Consumers must include supporting evidence in their reports. If the complaint is received by the Ministry of Communication and Information, the Personal Data Dispute Resolution Agency shall answer within 14 working days.

This type of consumer personal data protection is outlined in the Minister of Communication and Information Regulation Number 20 of 2016 about Personal Data Protection and Law Number 27 of 2022 regarding Personal Data Protection. The government has the authority to regulate electronic system providers and examine certification of electronic system viability. It also underlines that each electronic system provider must develop internal regulations to improve the protection of consumer personal data. Article 52 of Law 8 of 1999 on Consumer Protection. To address the complexities of the lengthy and formal court procedure, the UUPK offers out-of-court dispute resolution (non-litigation) via conciliation, mediation, and arbitration (Susanti Agung Nugroho. 2008). Thus, the Marketplace is liable for data breaches and may face administrative sanctions if it violates the provisions of Law Number 27 of 2022 on Personal Data Protection (Erna Priliasari, 2023).

Article 31 of Law Number 1 of 2024, which amends Law Number 11 of 2008 on Information and Electronic Transactions, regulates the responsibilities of electronic system organizers (PSE) in protecting personal data. PSE are responsible for ensuring that electronic transactions are conducted safely and securely. Other articles in Law Number 1 of 2024 related to personal data protection include Article 16A, which stipulates that the protection of children's rights is a priority for PSE over commercial interests.

Article 16A

1) Electronic System Organizers are required to provide protection for children who use or access the Electronic System.
2) The protection referred to in paragraph (1) includes protection of children's rights as stipulated in the legislation regarding the use of products, services, and features developed and organized by Electronic System Organizers.
3) In providing products, services, and features for children, Electronic System Organizers are required to implement technology and operational technical

steps to provide protection as referred to in paragraph (1) from the development stage to the operation stage of the Electronic System.

4) In providing protection as referred to in paragraph (1), the Electronic System Organizer is obliged to provide:
    a. Information regarding the minimum age limit for children who can use the product or service;
    b. Child user verification mechanism; and
    c. Mechanisms for reporting abuse of products, services, and features that violate or potentially violate children's rights.
5) Further provisions regarding the protection as referred to in paragraphs (1) to (4) shall be regulated by Government Regulation.

Article 16B

(1) Violations of the provisions as referred to in Article 16A are subject to administrative sanctions.
(2) Administrative sanctions as referred to in paragraph (1) may include:
A. Written Reprimand;
B. Administrative Fine;
C. Temporary Suspension; and/or
D. Access Termination.

Article 45 regulates stricter criminal sanctions for parties who misuse electronic information.

The ITE Law enhanced the assurance of consumer protection in all electronic transaction activities. This regulation corresponds with the principles of consumer protection outlined in Law Number 8 of 1999 concerning Consumer Protection, emphasizing the importance of protecting consumer rights in transactions, utilizing technological conveniences with a focus on comprehensive data privacy provisions, where Article 26B of the ITE Law regulates the obligations of electronic system organizers to maintain the confidentiality, integrity, and availability of consumer personal data. This article affirms that organizers who neglect the security of personal data can be subject to administrative and criminal sanctions, providing stronger protection for consumers. If interpreted broadly, personal data protection has actually been regulated in the ITE Law. The subsequent articles in the ITE Law are Articles 30-33 and Article 35, which fall under Chapter VII regarding Prohibited Acts.

Meanwhile, in the New Criminal Code, namely Law Number 1 of 2023, Fifth Part on Informatics and Electronic Crimes regarding types of cybercrime or electronic crime or internet-based crime (International Cybercrime as criminal activities involving the internet, computer systems, or computer technology, also based on the ITE Law), includes:

1) Illegal Access (Article 332);
2) Cyber attacks on the information systems and infrastructure of the state, government, and society (Article 333);
3) Cyber attacks on finance, banking, government (Articles 334 and 335).

The threat of severe sanctions for violations of that article aims to maintain the security and integrity of Indonesia's electronic systems and information.

The Brain Chiper ransomware group caused a data breach at the Temporary National Data Center (PDNS) on Thursday, June 20, 2024. The ransomware assault encrypted data at 282 ministries/agencies and demanded a payment of 8 million USD (131 billion IDR) to unlock it. This is not the first data leak in Indonesia (Quoted from various media sources):

1. Indi Home Data Breach (2022) Indi Home, a Telkom Indonesia-owned internet service provider, reported a data breach in August 2022, affecting millions of consumers. The disclosed information includes browser history, population identification numbers (NIKs), and other personal details.
2. KPU Data Breach (2022). In September 2022, hacker Bjorka claimed to have accessed 105 million voter records from the General Election Commission's (KPU) website. The disclosed information contains full names, population identification numbers (NIK), and voter addresses.
3. Data Breach at Bank Syariah Indonesia (2023). In December 2023, Bank Syariah Indonesia (BSI) suffered a data breach that affected millions of clients. The disclosed data contains full names, account numbers, and other sensitive information.
4. Data breaches at Carousell, MyPertamina, PeduliLindungi, Lazada, and Mobile Legends (2022). In November 2022, the Ministry of Communication and Information Technology (Kominfo) revealed five fresh data breaches within a month. The disclosed material contains full names, email addresses, and other personal information.
5. Data breach in the Temporary National Data Center (2024) The ransomware organization Brain Chiper compromised data at the Temporary National Data Center (PDNS) on Thursday, June 20, 2024. The ransomware attack purportedly encrypts data in 282 ministries and departments. It is not yet known what information has been disclosed.

This section allows you to describe your research findings academically. You may not enter figures related to your statistical tests here; instead, you should explain those numbers here. You should structure your discussion with academic support for your studies and a good explanation according to the specific area you are investigating.

CONCLUSIONS AND RECOMMENDATIONS

Reflecting on the aforementioned cases, the issue in Law Enforcement and Personal Data Protection Regulations, which will continue to change and encounter implementation challenges, particularly in cross-border transactions. Differences in laws between countries can make it more difficult to police privacy infractions and data exploitation. Not all e-commerce platforms adhere to strong data security standards; user personal data can be exploited or even sold without authorization by other parties, and vulnerable systems can become targets for hackers seeking to steal customer information.

The lack of encryption, two-factor authentication, or proper security standards raises the danger of assaults like phishing, ransomware, and more sophisticated malware that can target e-commerce platforms and customers.

Cybercriminals frequently use system flaws or human ignorance to get access to sensitive information. Many e-commerce enterprises have failed to completely comply with data privacy rules such as the GDPR in Europe and the Personal Data privacy Law in Indonesia.

The application of the ITE Law in e-commerce regulation must not only be effective in dealing with technological obstacles, but also assure substantive justice for all parties concerned. This inconsistency could create legal loopholes that can be exploited for customer data exploitation.The Indonesian government should promptly harmonize personal data protection policies and immediately establish implementing regulations for Law Number 1 of 2024 and Law Number 27 of 2022 in the form of Government Regulations regarding child protection provisions, including personal data, and supervisory bodies both on social media and digital platforms in general.

REFERENCES

Acar, G., & Yalçınkaya, A. (2020). The Impact of Data Breaches on Consumer Trust in E-Commerce Platforms: A Quantitative Study. *Computers in Human Behavior*, Volume 112, 106452. DOI: 10.1016/j.chb.2020.106452

Agarwal, A., & Rathi, S. (2020). A Study on Cybersecurity Threats and Their Impact on Business Organizations. *Computers, Materials & Continua,* Volume 64, Issue 3, pp. 1181-1194.DOI: 10.32604/cmc.2020.011742

Bianchi, L., & Romano, M. (2022). *The Role of Legal Enforcement in Ensuring Data Privacy Compliance in E-Commerce: An Analysis of Global Trends. Journal of Internet Law,* Volume 26, Issue 4, pp. 59-78. DOI: 10.1080/0141907X.2022.2077652

Budi, A. R., & Suhartono, T. (2023). *Penerapan Kebijakan Perlindungan Data Pribadi oleh Pelaku Usaha E-Commerce di Indonesia. Jurnal Ilmiah Teknologi Informasi, Volume 11, Issue 1, pp. 45-58.*

Doherty, N. F., & Malone, J. (2020). Security Challenges in Implementing Cybersecurity in Small and Medium Enterprises (SMEs): A Case Study Approach. *Computers & Security,*Volume 92, 101717. DOI:10.1016/j.cose.2020.101717

Erna Priliasari. Perlindungan Data Pribadi Konsumen dalam Transaksi E Commerce. Rechts Vinding: Media Pembinaan Hukum Nasional. Volume 12, Nomor 2, Agustus 2023

Harrison, P., & Fitzgerald, J. (2022). *Data Privacy Management for Businesses: Legal Requirements and Practical Considerations in the Digital Marketplace. Journal of Privacy and Security, Volume 17, Issue 4, pp. 255-270.* DOI: 10.1016/j.jpriv.2022.07.003

Harrison, P., & Clarke, L. (2023). *Data Protection Compliance and Enforcement: The Role of Regulatory Authorities in E-Commerce. Journal of Cyber Law and Ethics,Volume 30, Issue 1, pp. 45-62.* DOI: 10.1080/1094192X.2023.2018650

Hasan, H. R., & Ibrahim, M. (2021). Advanced Persistent Threats (APTs): Risks and Solutions for Cybersecurity in E-Commerce. *Cybersecurity,* Volume 7, Article 17. DOI: 10.1186/s42400-021-00117-0

Hassan, W., & Ali, S. (2022). A Review of Threats to Cybersecurity in the Internet of Things (IoT) Ecosystem and Countermeasures. *Journal of Internet Services and Applications,* Volume 13, Article 8. DOI: 10.1186/s13174-022-00109-4

Kumar, A., & Singh, M. (2022). A Survey on Cybersecurity Threats, Vulnerabilities, and Countermeasures in E-Commerce Platforms. *Journal of Information Security,* Volume 13, Issue 4, pp. 156–171. DOI: 10.1016/j.jis.2022.03.005

Kurniawan, A. S., & Pratama, I. A. (2022). *Tanggung Jawab Pelaku Usaha dalam Pengelolaan Data Pribadi di E-Commerce Indonesia. Jurnal Teknologi dan Sistem Informasi, Volume 14, Issue 4, pp. 175-189.*

Kurniawan, A. S., & Pratama, I. A. (2023). *Kepatuhan terhadap Regulasi Perlindungan Data Pribadi dan Penegakan Hukum di Indonesia: Perspektif Hukum dan Praktek di E-Commerce. Jurnal Administrasi Bisnis, Volume 15, Issue 1, pp. 65-79.*

Liu, Y., & Zhang, H. (2022). Data Privacy Laws and Their Impact E Commerce: Compliance Challenges and Strategies. *Journal Business Research,* Volume 138, pp. 195-209. DOI: 10.1016/j.jbusres.2021.09.056

López, C., & Pérez, J. (2022). The Role of Data Protection Laws in E-Commerce: A Comparative Study of GDPR, CCPA, and Other Regional Frameworks. *Journal of Global Information Technology Management, Volume 25, Issue 2, pp. 124–143.* DOI: 10.1080/1097198X.2022.2044513

Matsumoto, K., & Kikuchi, H. (2020). Challenges in Implementing Cybersecurity Frameworks for Critical Infrastructure Protection: A Comparative Study. *International Journal of Critical Infrastructure Protection,* Volume 31, 100374. DOI: 10.1016/j.ijcip.2020.100374

Mikkonen, T., & Laukkanen, T. (2023). *Obligations of Businesses in Personal Data Management: Challenges and Legal Compliance in the Digital Age. Journal of Business Research, Volume 154, pp. 314-324.*DOI:10.1016/j.jbusres.2022.11.054

Prayuti, Y. (2024). Dinamika perlindungan hukum konsumen di era digital: Analisis hukum terhadap praktik e-commerce dan perlindungan data konsumen di Indonesia. *Jurnal Interpretasi Hukum*, 5(1), 903–913. https://doi.org/10.55637/juinhum.5.1.8482.903-913

Putri, R. A., & Setiawan, D. (2023). *Kewajiban Pengelolaan Data Pribadi dalam E-Commerce: Studi Kasus pada Platform Digital di Indonesia. Jurnal Hukum dan Pembangunan, Volume 55, Issue 2, pp. 105-119.*

Rahman, A., & Santosa, P. (2022). *Regulasi dan Kewajiban Pengelolaan Data Pribadi oleh Pelaku Usaha: Perspektif Hukum dan Praktik di Indonesia. Jurnal Ilmu Hukum, Volume 16, Issue 3, pp. 105-118.*

Rambe, R. F. A., & dkk. (2023). Penerapan UU ITE (Informasi dan Transaksi Elektronik) dan UU Perlindungan Konsumen pada kasus jual beli jasa review palsu. *Journal on Education,* 6(1), 10030–10040.

Rashid, U., & Iqbal, M. (2020). Emerging Cybersecurity Threats: A Review of Recent Attacks and Security Solutions. *Computers & Security,* Volume 92, 101725. DOI: 10.1016/j.cose.2020.101725

Salloum, S. A., & Al-Sayyed, R. (2021). Emerging Threats and Security Challenges in Cloud Computing Environments: A Systematic Review. *Journal of Cloud Computing: Advances, Systems and Applications,* Volume 10, Article 35. DOI: 10.1186/s13677-021-00243-2

Sharma, R., & Patel, R. (2020). Security Challenges in Smart Cities: A Review of Current Solutions and Gaps. *Journal of Ambient Intelligence and Humanized Computing,* Volume 11, Issue 7, pp. 2819–2831. DOI: 10.1007/s12652-020-02082-1

Sharma, S., & Joshi, M. (2021). Understanding the Impact of Data Privacy Violations on Customer Loyalty in E-Commerce. *Journal of Retailing and Consumer Services*, Volume 61, 102587.DOI: 10.1016/j.jretconser.2021.102587

Smith, A. L., & Tang, X. (2022). *The Legal Obligations of Businesses Regarding Personal Data Protection: A Comparative Analysis of GDPR and CCPA. Journal of Cybersecurity and Privacy, Volume 5, Issue 2, pp. 45–60.* DOI: 10.3390/jcp5020045

Smith, A. L., & Green, T. (2023). *The Importance of Legal Compliance and Enforcement in Personal Data Protection: A Global Perspective on GDPR and Beyond. Journal of Business Ethics, Volume 182, Issue 2, pp. 459-474.* DOI: 10.1007/s10551-022-05201-2

Tao, Z., & Liu, L. (2022). *Business Obligations in the Management of Personal Data in E-Commerce: An Analysis of Global Compliance Practices. International Journal of Information Management, Volume 63, 102456.* DOI: 10.1016/j.ijinfomgt.2021.102456

Tian, Y., Liu, Y., & Sun, J. (2021). Cybersecurity Threats in E-Commerce: A Survey and New Challenges. *Journal of Information Security and Applications*, Volume 58, 102701. DOI: 10.1016/j.jisa.2020.102701

Tritsini, E., & Papageorgiou, A. (2022). Data Breaches and Their Impact on Organizational Reputation: Evidence from the E-Commerce Sector. *Journal of Business Research*, Volume 146, pp. 1029–1041. DOI: 10.1016/j.jbusres.2022.02.028

Tung, H. T., & Nguyen, H. K. (2023). Data Protection Regulations and Compliance in E-Commerce: The Case of GDPR and Beyond. *Computers, Materials & Continua,* Volume 70, Issue 6, pp. 5193–5213. DOI: 10.32604/ cmc.2023.020532

Wang, X., & Chen, L. (2022).The Role of Data Encryption in Protecting E-Commerce Transactions from Data Breaches. *Computers & Security*, Volume 107, 102272. DOI: 10.1016/j.cose.2021.102272

Wang, Y., & Zhang, R. (2023). *Corporate Responsibilities in Personal Data Protection and*

Management: Examining the Role of Data Controllers. Journal of Global Information Technology Management, Volume 26, Issue 1, pp. 36-51. DOI: 10.1080/1097198X.2022.2128465

Yadav, M., & Suri, P. (2020). Cybersecurity in E-Commerce: A Critical Review of The Risks of Data Breaches. *Journal of Information Security and Applications*, Volume 54, 102560. DOI: 10.1016/j.jisa.2020.102560

Zhang, Y., & Yang, Z. (2021). Impact of Ransomware and Malware on the Cybersecurity Landscape: A Review of Recent Attacks and Countermeasures. *Computers & Security*, Volume 99, 102035. DOI: 10.1016/j.cose.2020.102035

Zhao, Y., & Xu, X. (2020). An Investigation into the Recent Cyber Threats to Critical Infrastructure and Mitigation Techniques. *International Journal of Critical Infrastructure Protection,* Volume 29, 100343. DOI: 10.1016/j.ijcip.2020.100343

Zhou, J., & Zhang, X. (2021). Challenges in the Implementation of Security Policies in Large-Scale Distributed Systems: A Survey and Recommendations. *Computers, Materials & Continua,* Volume 68, Issue 3, pp. 2341-2360. DOI: 10.32604/cmc.2021.013343

Zhao, L., & Chen, J. (2023). *Regulatory Compliance and Enforcement in Personal Data Protection: Challenges and Strategies for E-Commerce. Information Systems Journal, Volume 33, Issue 1, pp. 93–112.* DOI: 10.1111/isj.12399

Zhao, S., & Liu, Y. (2023). Privacy and Security Regulations in E-Commerce: A Global Perspective. *Information Systems Frontiers,* Volume 25, Issue 4, pp. 971–987. DOI: 10.1007/s10796-022-10287-9

Isnaeni. Moch, Seberkas Diaroma Hukum Kontrak (Surabaya: PT Revka Petra Media, 2017), hlm. 159

Kristiyanti, Celina Tri Siwi. 2009, Hukum Perlindungan Konsumen. (Jakarta, Sinar Grafika, 2009), hal. 25

Mochtar Kusumaatmadja dan B. Arief Sidharta, Pengantar Ilmu Hukum Suatu Pengenalan Pertama Ruang Lingkup Berlakunya Ilmu Hukum, Bandung: PT. Alumni, 2013, hal.50

Mahran, Z. A., & Sebyar, M. H. (2023). Pengaruh Peraturan Menteri Perdagangan (PERMENDAG) Nomor 31 Tahun 2023 terhadap perkembangan e-commerce di Indonesia. *Hakim,* 1(4), 51–67.

Susanti Agung Nugroho. 2008. Proses Penyelesaian Sengketa Konsumen Ditinjau dari Hukum Acara Serta Kendala Implementasinya, Kencana. Jakarta. hal 13

https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en , diakses pada tanggal 24 November 2024, Pukul 14.04 Wita

https://www.cnbcindonesia.com/tech/20241201190314-37-592508/elon-musk-minta-pengadilan-federal-larang-openai-cari-cuan, diakses pada tanggal 02 Desember 2024, Pukul 12.02 Wita

https://www.kompas.com/tren/read/2024/12/25/101036165/pelanggaran-chatgpt-dan-denda-otoritasprivasiitalia?amp=1&page=2&_gl=1*kh0jru*_ga*MTY4NTMwMDUzMi4xNjE0Njc0NjI0*_ga_77DJNQ0227*MTczNTkxNzkyNy4xLjEuMTczNTkxNzkyNy4wLjAuMA.., diakses pada tanggal 26 Desember 2024, Pukul 12.21 Wita

https://www.medcom.id/teknologi/news-teknologi/8koPDdWK-kasus-kebocoran-data-pribadi-di-indonesia-10-kejadian-terbesar-yang-perlu-diketahui