Law and Justice
Vol. 7, No. 2, 2022, pp. 196-212
e-ISSN : 2549-8282
https://journals2.ums.ac.id/index.php/laj/article/view/1586

The Urgency Of Authentication And Protection Of Personal Data In Online Transactions

Mutimatun Ni'ami
Universitas Muhammadiyah Surakarta
mn272@ums.ac.id

DOI: 10.23917/laj.v7i2.1586

Submission Track:
Received:
February 2023

Final Revision:
February 2023

Available Online:
February 2023

Corresponding Author:
Mutimatun Ni'ami
mn272@ums.ac.id

ABSTRACT

Fraud in online trading is a crime that is difficult to enforce the law. Fraud can be committed by sellers by counterfeiting their products or by driving transactions outside of e-commerce. Meanwhile, fraud committed by buyers is carried out by falsifying identities and fake orders. The efforts have been made to threaten the perpetrators with criminal noose but have not reduced the number of frauds that occur. This research was conducted using normative research that looked at fraudulent behavior and related it to the legal provisions in the ITE Law and in the Personal Data Protection Law. The research found that the need for authentication as a marker for sellers and buyers when interacting on the internet so that fraud can be minimized because the identity of the perpetrator can be identified easily with the authentication method. So that the perpetrator's track record can be easily detected and this prevents the perpetrator from committing fraud.

***Keyword** : authentication, e-commerce, fraud*

INTRODUCTION

The rise of online trading lately is an exciting thing for the community. NielsenIQ noted that the number of online shopping consumers in Indonesia who use e-commerce will reach 32 million people in 2021. The number has shot up 88 percent compared to 2020, which was only 17 million people. Director of Nielsen Indonesia Rusdy Sumantri said the number of online shopping consumers increased because internet users in Indonesia rose 32 percent from 34 million to 45 million people so far this year.

In addition, government policies that limit people's mobility in controlling the spread of Covid-19 increase the number of consumers who shop online (CNN Indonesia, 2021b). Bank

Indonesia said that throughout 2021 economic and digital transactions will develop very significantly along with increasing public acceptance and preference for e-commerce and the value of trade transactions reaching Rp. 401 trillion (Elena, 2022).

The online transaction system makes it easier for business people to market and sell their products. The obstacle that originally appeared in the form of a place of business can be overcome with this e-commerce model because it does not require stalls to sell. Only by capitalizing on a smartphone and social media, anyone can shop and sell their products easily.

The ease that appears is usually accompanied by disadvantages on the other side. Product images that appear as a result of sophisticated camera shots sometimes deceive consumers. The condition of the product in the picture does not match the reality of the product. Likewise on the other side. Buyers can also commit acts of fraud by ordering using someone else's account or using someone else's credit card account. The absence of the meeting between sellers and buyers directly complicates the authentication process. Is the buyer a person who really intends to buy? Can the seller be trusted for his wares? This problem has not been resolved so far. . It has been proven that there are many frauds with e-commerce media. It is known that there were 1,253 data card breaches as of January 18, 2019, approximately $16 billion due to these frauds and crimes (Sukandar, 2019).

The Cekrekening.id website said that there were 115,756 cases of online fraud from e-commerce and online selling on social media in September 2021. Fraud via e-commerce is often carried out by inviting buyers to make transactions outside of e-commerce. The buyer is asked to pay for the goods that have been ordered, then the seller does not process the order and the seller will change the phone number so that he can escape responsibility (CNN Indonesia, 2021a).

Indonesia is the fastest growing e-commerce market in the world, with 74% of respondents having made a purchase online. This growth is also in line with the high number of frauds. On average, 25% of e-commerce actors have experienced criminal acts of fraud through various services. This was conveyed by Dev Dhiman, Managing Director, Southeast Asia and Emerging Markets, Experian Asia Pacific (Dwijayanto, 2018).

Therefore, research is needed to find out whether authentication can overcome the rampant fraud in online buying and selling and whether there is personal data protection for consumers in the Indonesian legal system.

RESEARCH METHODS

The type of this research is normative legal research. It uses literature studies originating from books, scientific works and writings of legal experts. This research focuses on the existing legal regulations in Indonesia in preventing fraud in e-commerce transactions (Wasito, 1997). While the research data used is secondary data obtained from literature related to theories and concepts of research objects, scientific writings of legal experts and scientific works through literature study (Sumardjono, 2014). The data analysis used is a qualitative analysis then presented in a descriptive analytical form. Qualitative analysis was carried out through categorization based on the problems studied and the data collected (Arikunto, 2018).

RESULTS AND DISCUSSION

The shift and development of the role of the state has occurred as a result of the process of modernization and democratization of the state government system. State understanding has developed from a political state to a legal state and finally a welfare state. These three schools of thought all take advantage of the power of the state has as a determinant of the will of the people under its control. The welfare state emerged as an answer to the social inequality that occurs in the liberal economic system. In the understanding of the welfare state, the state has freis ermessen, namely the freedom to participate in all social, political and economic activities with the ultimate goal of creating the bestuurzorg general welfare.

In the past, the government had a centric role in managing its people. Trade is under government control in relation to permits, goods sold and places to sell. Even though it doesn't regulate totally, the rules that are made and law enforcement can be implemented easily considering that the government's control over its people is still large.

Over time, the modernization process reduced the government's authority to regulate its citizens. For example, in online trading (e-commerce), the government is no longer able to strictly regulate places to sell, including sellers, buyers and the entry of imported goods into Indonesia.

Through the internet, anyone can sell and sell their objects (goods) to be offered through stalls or websites that they have made themselves. Some laws are then very easy to violate. A small child can easily buy an e-cigarette or other items that should not be reserved for him. On the other hand, a teenager can easily sell his mother's jewelery that he stole from the wardrobe.

The government must force itself or be forced to change itself from the beginning as the ruler of the political state to become a legal state to finally become a welfare state. The welfare state is a form of democratic government which emphasizes that the state is responsible for the minimum welfare of the people, that the government must regulate the distribution of the country's wealth so that no people go hungry. Countries in this category contain elements of socialism, emphasizing welfare in the political and economic fields (R.M.A.B., 2006).

In the economic field, there are four functions of the state, namely as a guarantor (provider) of people's welfare, the state as a regulator, the state as an entrepreneur or running certain sectors through State-Owned Enterprises (Indonesian abbreviation is BUMN), and the state as the umpire to formulate fair standards regarding the economic sector including state companies (state corporation) (Farmer, 1973). The function of the state, as stated by Friedmann, shows that actually in the notion of a welfare state, the state may intervene in the economic sector.

Historically constitutional, it can be proven that the legal state of Indonesia adheres to the concept of a welfare state. The existence of economic democracy which is the characteristic of a welfare state is reflected in the Explanation of Article 33 of the 1945 Constitution which reads:

……. "The economy is based on economic democracy, prosperity for all people. Because of this, the branches of production which are important to the state and affect the livelihood of the many people must be controlled by the state. If it's not, the reins of production will fall into the hands of those in power and the people who are being oppressed by them. Only companies that do not control the lives of many people can be in the hands of one person. Earth and water and the natural wealth contained in the earth are the main points of people's prosperity. Therefore, it must be controlled by the state and used for the greatest prosperity of the people".

Indonesia's choice to understand the welfare state has become a firm determination. In addition to being a welfare state, Indonesia has also declared itself as a constitutional state. As a country that adheres to the concept of a welfare state, the state can use law as a means to regulate

and administer and guarantee the welfare of its people. Therefore, it is necessary to develop a national legal system that will be used to support the fulfillment of this responsibility.

Model of Fraud in E-Commerce Transactions

The Cekrekening.id website said that there were 115,756 cases of online fraud from e-commerce and online selling on social media in September 2021. Fraud via e-commerce is often carried out by inviting buyers to make transactions outside of e-commerce. The buyer is asked to pay for the goods that have been ordered, then the seller does not process the order and the seller will change the phone number so that he can escape responsibility (CNN Indonesia, 2021a).

Other fraud models appear in various forms, including:

1. Classic fraud

   This type of fraud takes advantage of other people's credit card data. The theft is done by carding. Indonesia ranks second in this model of fraud ("Indonesia Pelaku Kejahatan Carding Terbanyak Kedua Di Dunia," n.d.). The perpetrator committed a pattern of crime by using a smartphone. First, they sign in with fake accounts on Apple and Paypal. From these accounts, they can steal data in the form of credit card numbers and expiration dates (Rinanda, 2018). The perpetrator will resell the item so that the police don't find out. This carding crime has caused many online shopping sites to be blocked by the internet protocol, meaning that consumers from Indonesia are not allowed to shop on foreign online sites.

2. Triangulation fraud

   This type of fraud involves three parties: the fraudster, the unsuspecting legitimate buyer and the e-commerce store. Online listings are created by fraudster, often on eBay or Amazon, who offer high-demand items for very low prices. The store collects payment for the items it sells. The fraudster then uses other stolen credit card data and names collected in his online store's orders to purchase goods from the legitimate website and sends them to customers who purchase on his new online store.

   This type of fraud can usually be identified by the product it is targeted as well as some investigative work by finding unsuspecting buyers who can identify the online market as where the stolen goods were purchased.

3. Interception fraud

Fraudsters will create orders where billing and shipping match the address linked to the card. Their goal is to intercept the package in one of the following ways: asking a customer service representative to change the address on the order prior to shipping, or contacting the sender to reroute the package to an address where they can pick up the stolen item.

In cases where the fraudster resides close to the cardholder's billing address, physically wait near the address for the shipment to arrive and offer to sign for the package because the homeowner is not available.

4. Card testing fraud

This is the practice of testing the validity of credit card numbers, with a plan to use valid credentials on other websites to commit fraud. Fraudsters target websites that express different responses for each type of disapproval.

For example, when a card is declined for an incorrect expiration date, the response is different, so they know they just need to find out the expiration date. This is generally done by bots, and transaction attempts happen quickly, sequentially. Data on orders will often be identical, either all of the data or only part of the data, such as shipping addresses.

5. Account takeover fraud

This occurs when fraudsters obtain valid customer login credentials and utilize stored credit cards to purchase goods. Updates to the shipping address will usually occur shortly before purchase so fraudsters can retrieve stolen items.

6. Fraud through identity theft

In this case, the fraudster assumes someone else's identity, makes a credit card in the victim's name and goes shopping. This type of fraud is increasing rapidly as the number and scope of data breaches increases. It is also the most difficult to identify because the fraudsters behind identity theft are quite sophisticated.

7. Friendly fraud, also known as chargeback fraud

An online shopper will make a purchase, then issue a chargeback, claiming their card was stolen. Refunds usually occur after the item is shipped. This type of fraud has traditionally not been perpetrated by hard criminals but by consumers who are clearly aware of what they are doing.

The Authentication and application of digital data in an effort to minimize fraud rates.

Authentication is a method for confirming a user or users in a service, application, payment system or storage system, so that it is known with certainty that the user is a legitimate person and has access rights to certain information. Information or data used to perform authentication is usually confidential data that only the user knows. Therefore, when the data entered matches, the system assumes that the access request made is really being made by the legitimate user (Verihubs, 2022).

Digital identity is a collection of digital records containing the identity of a citizen. These records are kept in an institution that provides this system. The digital system facilitates the process of documenting citizens and collecting their important data. With a sophisticated authentication and security system, the digital identity system cannot be stolen, faked or lost like a manual identity system. The existence of a digital identity system allows the financial industry to verify and identify prospective customer data more quickly ("Sistem Identitas Digital Di Industri Finansial Dan 7 Fungsinya," 2018). This system can also be used to verify online shoppers when they want to make purchases.

With the existence of a digital identity system, this convoluted KYC (Know Your Customer) process can be made more concise. Because our data is stored in digital records, financial institutions can access our data quickly for all verification and identification purposes. It is not only that, digital records on identities can also be used to track financial history and transactions that have been carried out more easily to avoid money laundering.

In the European Union, starting in 2019, new policies emerged under the Payment Services Directive (PSD2) to reduce fraud and make transactions more secure for online businesses located in the European Economic Area (EEA). One of the parts of this policy (Strong Customer Authentication/SCA) requires all online businesses to implement a more in-depth authentication

process on transactions if the cardholder and bank are doing business in the European Economic Area

This is done in an effort to ensure that the customer is the legal owner of the card. If the SCA is not carried out, the bank is required to refuse to make the payment. In this SCA the identity of the guest will be thoroughly verified. In other words, the customer must prove that they are the legal owner of the card using two or three authentication methods by ensuring that the customer knows or has the password, PIN, phone number or fingerprint ("Apa Yang Dimaksud Dengan Autentikasi Pelanggan Yang Kuat," n.d.).

Another way that can be used in authentication is an electronic signature. When compared to wet ink signatures, electronic signatures are relatively more difficult to be falsified. This is because electronic signatures involve electronic certificates and data encryption technology. Both of these guarantee that the electronic signature cannot be changed.

Minimizing fraud and identity risks is the ability of electronic signatures to help secure online transactions. Every electronically signed digital document will be authenticated with a verified digital identity. To strengthen verification, the digital document signing process is equipped with biometric technology such as face recognition.

Electronic signature has a unique system. At first it will appear the unique hash of a document. Hash is a series of letters and numbers generated by the algorithm. There are no hash sets with the same letters and numeric combinations. Furthermore, the hash that appears will use the cryptographic method. This method uses a key pair system called a public key (for the recipient and sender of files) and a private key (for one-party use). One key is used to decrypt, then another key is used to encrypt.

In the cryptographic method, the method uses a public key infrastructure that engages the public key with an individual entity or organization. This engagement is established through registration and issuance of electronic certificates by a certificate authority (CA) such as VIDA.

The use of public key instruments is intended to facilitate the transfer of secure electronic information for various networks, especially those that require confirmation of the identity of the

parties involved in the communication as well as validating the information or messages being transferred.

Another reason is that implementing a digital identity system will bring more benefits in the future, especially for financial services. According to the Deloitte China research institute, there are seven advantages of implementing a digital identity system for the financial industry. These seven advantages are:

1. The risk profile adjustment for financial institutions
   Various financial institutions can create risk profiles of credit products for consumers through algorithms and data they get from consumer identities
2. Facilitate customers to conduct banking affairs overseas
   With a digital identity, consumers can easily access financial services abroad because a digital identity system can store consumer transaction history even if it is done in a different country.
3. Simplify e-commerce authentication and verification
   E-commerce service users can easily receive consumer data provided through financial institutions in accordance with consumer agreements
4. Digital tax filling uses a digital identity system
   Citizens can report taxes easily through financial institutions without having to collect asset data and fill out old forms.
5. Measuring the risk of electronic transactions
   The digital identity system allows financial service providers to know the financial history of their prospective users, so that service providers can determine the user's risk level more precisely
6. Identify each transaction actor
   A digital identity system that is identified with tax reporting information means the availability of complete information about the prospective customer's assets along with their history of ownership and its use

7. Linking individual identity with corporate identity

   Integrating personal identity with work history data will streamline the KYC process while minimizing the risk of fraud.

In item no. 3 states that the digital identity system facilitates the authentication and verification process in e-commerce. If this system has been successfully implemented in Indonesia, the online business market share in Indonesia will increase. The market share is not only in Indonesia but also in foreign markets, so it is hoped that our products will be able to compete with imported goods, the spirit of being the host in our own country will be realized as the e-commerce market share increases.

The Protection of Personal Data

Authentication is a process of validating or proving the identity of a user who wants to access a particular file, application or system. Authentication is developed further by asking for some personal information such as biometric fingerprints to ensure the security of the account from people who have the technical ability to break into system weaknesses. Authentication can guarantee that systems and data will be much safer from the hands of irresponsible people (Prayoga, 2023).

Personal data protection is regulated in the Personal Data Protection Act (PDP Law) and the ITE Law. In Article 26 paragraph (1) Law No. 19 of 2016 stipulates that the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned unless there are other provisions from the law. (Oktavira, 2022)

Personal Data Data consists of:

a. Specific Personal Data; And
b. General Personal Data.

Personal data that is general in nature includes: health data and information, biometric data, genetic data, crime records, child data, personal financial data and/or other data. Besides that, there is also general personal data, including: full name, gender, nationality, religion, marital status and personal data that are combined to identify a person.

In its development, especially after the amendment to the 1945 constitution, the right to privacy which includes the protection of personal data is recognized as a constitutional right of citizens. This is stated in Article 28G paragraph (1) of the 1945 Constitution which states "Every person has the right to protection of self, family, honor, dignity and property under his control and has the right to feel safe and protected from threats of fear to do or not do something that is a human right.

Protection of personal data in the PDP Law must pay attention to several principles, namely:

1. The principle of protection means that the processing of personal data is carried out by providing protection so that it is not misused.
2. The principle of legal certainty that any processing of Personal Data is carried out on a legal basis so as to obtain legal recognition within and outside the Court.
3. The principle of public interest is that in enforcing Data Protection it is necessary. Paying attention to the public interest or the wider community.
4. The principle of expediency is that the regulation on Personal Data Protection is beneficial to the national interest, particularly in realizing the ideals of general welfare
5. The precautionary principle is that the parties involved in the processing and monitoring of Personal Data must pay attention to all aspects that have the potential to cause harm.
6. The principle of balance is an effort to protect Personal Data to balance between the rights of Personal Data on the one hand and the legitimate rights of the state based on the public interest.
7. The principle of accountability is that all parties involved must act responsibly.
8. The principle of confidentiality is that Personal Data is protected from unauthorized parties and/or from unauthorized processing of Personal Data.

Data protection itself in general terms refers to protective practices and binding rules that are enforced to protect personal information and ensure that the data subject remains in control of his information. The data owner must be able to decide whether or not to share some information, who has access for how long for what reasons and can modify some of this information.

Data protection laws must apply to automated data and automated data processing, as well as structured formats for storing manual data (filing systems). This means that the law must cover all data processing on computers, phones, IoT devices, as well as paper records. It also reaches out to public (government) and private institutions. Meanwhile for individuals, it is widely accepted that processing for individual or household needs is exempt from the enactment of the law. In general, data protection law also considers that data moves cross borders, which often creates jurisdictional problems, including the possibility of conflicts with applicable national laws.

Article 20 of the PDP Law states that the processing of personal data requires written or recorded approval from the Personal Data Subject which is submitted electronically or non-electronically. Without such approval, the processing is declared null and void by law. The use of personal data in an electronic media must obtain approval from the data owner. Violation of these provisions may result in a lawsuit being filed for losses incurred. Protection of personal data includes protection from unauthorized use, protection by electronic system operators, and protection from illegal access and interference.

Any personal information containing Family card number, National Identity Number (ID card number), date/month/year of birth, information about physical and/or mental disabilities, biological mother's NIN, father's NIN, and some contents of Important Event records available on the internet as per Article 84 The Adminduk Law is part of a personal data that must be protected.

Minister of Communication and Informatics Regulation No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems (PM 20/2016) which has been in effect since December 2016, protection of personal data includes protection against the acquisition, collection, processing, analysis, storage, appearance, announcement, transmission, dissemination and destruction of data personal.

According to PM 20/2016, an electronic system that can be used in the process of protecting personal data is an electronic system that has been certified and has internal regulations regarding

the protection of personal data that must pay attention to aspects of the application of technology, human resources, methods, and costs.

The owner of personal data, according to PM 20/2016, has the right to keep his data confidential; has the right to file a complaint in the context of resolving personal data disputes; has the right to get access to obtain historical personal data; and has the right to request the destruction of certain personal data belonging to him in the electronic system.

This personal data is requested if we use the internet in connection with, for example, e-commerce transactions. Personal data provided may only be used for purposes approved by the data owner. If illegal manipulation occurs, leaks or fails to be protected by Electronic System Operators (both government or private certified) then based on Article 15 paragraph (2) PP STE

> *"If there is a failure in the protection of personal data that is managed, the Electronic System Operator must notify in writing to the Owner of Personal Data"*

This article does not explain the definition of failure in question. In general, these failures can be categorized into 2 (two). First, procedural failures in confidentiality and security in data processing. Second, system failure from the aspect of reliability and security aspects of the system used, and aspects of the operation of the Electronic System as it should (see Explanation of Article 15 paragraph [1] of the ITE Law).

The occurrence of system failure can be caused by internal factors and external factors. One of the external factors that often occurs is the existence of cybercrime. Judging from the type of activity, cybercrime can be in the form of hacking, cracking, phishing, identity theft, etc. The impact of losses that arise include personal data leakage, data manipulation, privacy violations, system damage, etc. Every operation of an electronic system must notify in writing to the Personal Data Owner if there is a failure to protect the confidentiality of personal data. The information that must be submitted includes:

- reasons or causes for failure to protect confidential personal data can be done electronically,

- it must be ensured that it has been received by the Personal Data Owner if the failure creates a potential loss for the person concerned,
- written notification sent to the Personal Data Owner no later than 14 (fourteen) days after the failure is known,

In the event of cracking (entering other people's systems) which can result in loss, change or leakage of data that is confidential or personal data, the PDP Law provides legal protection for the security of electronic data from illegal access.

Article 65 of the PDP Law in conjunction with Article 67 of the PDP Law is regulated as follows:

1. Any person who deliberately and unlawfully obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or another person which can result in loss of Personal Data Subjects as referred to in Article 65 paragraph (1) shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000.00 (five billion rupiah).

2. Any person who intentionally and unlawfully discloses personal data that does not belong to him as referred to in Article 65 paragraph (2) shall be subject to imprisonment for a maximum of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000.00 (four billion rupiah).

3. Any person who intentionally and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 paragraph (3) shall be subject to imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah)

In the event of cracking (entering other people's systems) which can result in loss, change or leakage of data that is confidential or personal data, the PDP Law provides legal protection for the security of electronic data from illegal access. Any act against the law by accessing an electronic system with the aim of obtaining Electronic Information/Documents by violating the security system is considered a criminal offense according to Article 65 of the PDP Law in conjunction with Article 67 of the PDP Law is regulated as follows:

1. Whosoever who intentionally and against the law obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or another person which

can result in loss of Personal Data Subjects as referred to in Article 65 paragraph (1) shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000.00 (five billion rupiah).

2. Whosoever who intentionally and against the law discloses personal data that does not belong to him as referred to in Article 65 paragraph (2) shall be subject to imprisonment for a maximum of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000.00 (four billion rupiah).
3. Whosoever who intentionally and against the law uses Personal Data that does not belong to him as referred to in Article 65 paragraph (3) shall be subject to imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah).

The existence of the PDP Law can increase consumer confidence, because it requires data managers and processors to be transparent about the management of personal data. In addition, the PDP Law also encourages the growth of innovation in business management because it can trigger competition for innovation between companies in proving the company's capacity to manage data security (Rizkinaswara, 2020).

CONCLUSION

Digital identity is a collection of digital records containing the identity of a citizen. These records are kept in an institution that provides this system. The digital system facilitates the process of documenting citizens and collecting their important data. With a sophisticated authentication and security system, the digital identity system cannot be stolen, falsified or lost like a manual identity system. The existence of a digital identity system allows the financial industry to verify and identify prospective customer data more quickly. This system can also be used to verify online shoppers when they want to make purchases.

Based on the discussion above, it can be concluded again that sociologically, the online buying and selling system has changed the culture of society. These changes are clearly visible in terms of:

a. The Identity of seller and buyer

In offline sales, there is no need to know the identities of the parties to the transaction. It is enough to show a desire to buy and make payments, then the transfer of goods will occur and the buying and selling process will be completed. Even if the parties know each other's name, place of residence and other identities, then this is due to the growing kinship between them. Known as *tuna sathak bathi sanak*, when kinship has been established, big profits are no longer the main goal, having more siblings is a separate fortune which is believed to bring blessings.

In contrast to buying and selling online, it is easy not to meet face to face and make transactions at long distances. However, complete identity and details are required in an effort to minimize fraud or deception.

a. Disclosure of information in online buying and selling raises concerns about the possibility of this data being used for crime. The parallel relationship between sellers and buyers is just a physical relationship without involving emotional elements to look after and help each other. It is very different from the offline transaction process which creates familiarity and emotional connection between the parties as a feature of Indonesian society which is communal.

REFERENCES

Apa yang dimaksud dengan Autentikasi Pelanggan yang Kuat. (n.d.). Retrieved January 28, 2023, from https://partner.booking.com/id/bantuan/kebijakan-pembayaran/pembayaran-tamu/apa-yang-dimaksud-dengan-autentikasi-pelanggan-yang-kuat

Arikunto, S. (2018). *Prosedur Penelitian Suatu Pendekatan*. Jakarta: Rineka Cipta.

CNN Indonesia. (2021a). Kominfo Catat Kasus Penipuan Online Terbanyak: Jualan Online. Retrieved January 27, 2023, from https://www.cnnindonesia.com/teknologi/20211015085350-185-708099/kominfo-catat-kasus-penipuan-online-terbanyak-jualan-online.

CNN Indonesia, U. (2021b). Konsumen Belanja Online RI Melonjak 88 Persen pada 2021. Retrieved January 27, 2023, from https://www.cnnindonesia.com/ekonomi/20211229141536-92-740093/konsumen-belanja-online-ri-melonjak-88-persen-pada-2021

Dwijayanto, A. (2018). Experian: Sekitar 25% konsumen pernah mengalami penipuan online. Retrieved January 28, 2023, from https://industri.kontan.co.id/news/experian-sekitar-25-konsumen-pernah-mengalami-penipuan-online

Elena, M. (2022). BI Catat Nilai Transaksi E-Commerce Tembus Rp401 Triliun pada 2021. Retrieved January 28, 2023, from https://ekonomi.bisnis.com/read/20220127/9/1494047/bi-catat-nilai-transaksi-e-commerce-tembus-rp401-triliun-pada-2021

Farmer, J. A. (1973). The State and the Rule of Law in a Mixed Economy. By Wolfgang Friedmann,

formerly Professor of International Law at Columbia University. [London: Stevens & Sons. 1971. vii, 101 and (Index) 3 pp. £2”00 net.] - Government Enterprise. Edited by Friedmann. *The Cambridge Law Journal*, *32*(1), 168–171. https://doi.org/10.1017/S0008197300090437

Indonesia Pelaku Kejahatan Carding Terbanyak Kedua di Dunia. (n.d.). Retrieved January 27, 2023, from http://news.rakyatku.com/read/135627/2019/01/15/indonesia-pelaku-kejahatan-carding-terbanyak-kedua-di-dunia

Jamin Perlindungan Data Pribadi, Kominfo Beri Sanksi Terhadap Penyalahgunaan oleh Pihak Ketiga, (2020 Juli,7), https://www.kominfo.go.id/content/detail/12865/siaran-pers-no-85hmkominfo042018-tentang-jamin-perlindungan-data-pribadi-kominfo-beri-sanksi-terhadap-penyalahgunaan-oleh-pihak-ketiga/0/siaran_pers diakses 25 januari 2023

Jumlah Pembeli Online Indonesia Capai 119 Persen Dari Populasi,(2018. September 27), https://ekonomi.kompas.com/read/2018/09/07/164100326/jumlah-pembeli-online-indonesia-capai-119-persen-dari-populasi diakses 28 Januari 2023

Oktavira, B. A. (2022). Jerat Hukum Pelaku Cracking Menurut UU PDP dan UU ITE. Retrieved January 25, 2023, from https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-icracking-i-menurut-uu-pdp-dan-uu-ite-lt4f235fec78736

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Prayoga, J. (2023). Autentikasi: Cara Kerja dan Pentingnya untuk Keamanan Data. Retrieved from https://gudangssl.id/blog/autentikasi-adalah/

R.M.A.B., K. (2006). Negara Kesejahteraan dan Jaminan Sosial. *Jurnal Konstitusi*, 160.

Rinanda, H. M. (2018). Pelaku Spamming dan Carding Dibekuk Bobol Kartu Kredit Rp 500 Juta. Retrieved January 25, 2023, from https://news.detik.com/berita-jawa-timur/d-3927140/pelaku-spamming-dan-carding-dibekuk-bobol-kartu-kredit-rp-500-juta

Rizkinaswara, L. (2020). Dirjen Aptika: UU PDP akan Beri Keuntungan bagi Sektor Bisnis. Retrieved January 25, 2023, from https://aptika.kominfo.go.id/2020/10/dirjen-aptika-uu-pdp-akan-beri-keuntungan-bagi-sektor-bisnis/

Roscoe Pound, (2012), Contemporary Juriscdic Theory, dalam Bernard L Tanya, Teori Hukum, Genta Publishing

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan

Sistem Identitas Digital di Industri Finansial dan 7 Fungsinya. (2018). Retrieved January 28, 2023, from https://blog.privy.id/case-study/7-kegunaan-sistem-identitas-digital/

Sukandar, C. A. (2019). Waspada! 7 Jenis Skema Penipuan E-commerce, Anda Harus Tahu. Retrieved January 28, 2023, from https://www.wartaekonomi.co.id/read210607/waspada-7-jenis-skema-penipuan-e-commerce-anda-harus-tahu.html

Sumardjono, M. S. (2014). *Metodologi Penelitian Ilmu Hukum*. Yogyakarta: Gadjah Mada Press.

Verihubs. (2022). Mengenal Pengertian, Cara Kerja, dan Manfaat Autentikasi dalam Sistem Perusahaan. Retrieved January 25, 2023, from https://verihubs.com/blog/autentikasi-adalah-2/

Wasito, H. (1997). *Pengantar Metodologi Penelitian Buku Panduan Mahasiswa*. Jakarta: PT. Gramedia Pustaka Utama.