*Research Article*

# Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?

**Rahmi Ayunda**
**Faculty of Law, Universitas Internasional Batam, Indonesia**
**rahmi@uib.ac.id**

***ABSTRACT***

Internet is one of the media facilities that is not only used for communication, but is also used in the process of buying and selling or trading (e-commerce). Behind all the conveniences obtained, e-commerce also raises the issue of consumer concerns on the responsibility for personal data. This study aimed to examine and re-explain the urgency of protecting personal data of e-commerce consumers and focused on the challenges and legal certainty of protecting personal data of e-commerce consumers in Indonesia. The method used was a doctrinal research method. This study showed that the application of data in e-commerce provides many benefits. However, the challenge was the absence of binding laws to safeguard personal data submitted to e-commerce companies. Legal certainty for the protection of e-commerce consumers is currently contained in several laws and regulations. Therefore, it is necessary to improve the effectiveness in the implementation of personal data protection and to regulate the protection of personal data in a law. In Indonesia, the urgency of the ratification of the Personal Data Protection Bill may become a solution in providing legal certainty for the protection of e-commerce consumers on their personal data.

**Keywords: E-Commerce; Legal Certainty; Protection; Consumer.**

## A. INTRODUCTION

The development and advancement of increasingly sophisticated and modern technology appears in various systems in almost all lines. This causes the necessities of life to experience a significant increase (Tan, & Disemadi, 2021). Human needs are diverse, in line with the development of civilization, science, and technology (Amboro, & Christi, 2019). In meeting needs, humans continue to strive to optimize the satisfaction of their desires. This makes technology a significant aspect of meeting needs (Disemadi, 2021). Human need for the satisfaction of material goods which is in line with technological advances makes the internet a media facility that is not only used for communication, but also can be used for buying and selling process or trade (Nurfitri, Sudirman & Disemadi, 2022). This phenomenon is known as “online shopping”. With the synergy between trade and information technology, e-commerce is created. E-commerce is the use of the internet, websites, and applications for digital business transactions between companies and individuals (Barkatullah, & Djumadi, 2018). E-commerce can be an alternative choice in buying and selling goods or services online. Consumers do not need to spend a lot of energy, just by looking at the

website to make a purchase transaction (Rahayu, & Day, 2015).

E-commerce can be interpreted as an online commercial activity that focuses on the exchange of commodities (goods or services) electronically, on the internet in particular (Setyawan, & Wijaya, 2018). E-commerce is in high demand because e-*commerce* sellers (sellers) are not required to meet consumer or buyers directly (face to face) (Bagheri, Hassan, & Mansour, 2017). Transactions can be conducted through electronic mail (electronic email), telecopy, and others (Kumar, Belwal, & Raina, 2019). Payments are also made using internet intermediaries, which are considered more efficient (Fathur, 2020). However, behind all the conveniences obtained, e-commerce also raises the issue of consumer concerns about the responsibility for personal data that have been recorded and collected by e-commerce companies. The personal data are in the form of consumer identity such as names, passwords, debit and credit card numbers, conversations in e-mail, as well as information related to consumer requests. In this regard, consumers need to be legally protected from possible losses due to these business practices (Simanullang, 2017). In fact, law in Indonesia still does not provide certainty and protection for privacy and personal data to consumers, because Indonesia so far does not have a legal instrument that specifically accommodates people's needs to obtain stronger protection for privacy and personal data. The unpreparedness of Indonesian law in anticipating developments in information technology can have fatal consequences and even pose a threat to society. Data protection of legal instruments in modern times must meet at least three requirements: (1) the glue elements of individuals and economic communities; (2) having an international character; and (3) encouraging the community to become part of digital economy era society (Fathur, 2020).

Consumer protection law has received enough attention because it involves rules for the welfare of society as consumers (Ayunda, & Rusdianto, 2021). The government plays a role in regulating, supervising and controlling, so as to create a conducive system that is interconnected with one another (Disemadi, & Regent, 2021). Thus, the goal of the welfare of society at large can be achieved. Business is identical with the existence of consumers; this is part of the interaction in carrying out economic or business activities and is usually referred to as consumers, namely connoisseurs of products produced by business people or business actors (Paryadi, 2018). In social life, humans are never free from conflicts or disputes, regarding violations of consumer rights (Disemadi, & Regent, 2021). Moreover, in business activities it is necessary to have protection, especially consumer protection (Simanullang, 2017). Legal issues relating to consumer legal protection are increasingly concerning the event that a consumer conducts e-commerce transactions with merchants in one country or in different countries In buying and selling via the internet, fraud often occurs (Barkatullah, 2007). These frauds can occur involving the whereabouts of business actors, goods purchased,

prices of goods, payments by consumers, and protection of personal data (Anugerah, & Indriani, 2018).

Previous research was carried out by Hari Sutra Disemadi in 2021. The research examines the prospect of using *Artificial Intelligence* to protect consumers' personal data (Disemadi, 2021) Another similar study was conducted by Arfian Setiantoro, Fayreizha Destika Putri, Anisah Novitarani, Rinitami Njatrijani in 2018. This research shows that current legal instruments in Indonesia do not fully regulate legal protection for consumers in e-commerce transactions. The mechanisms of available dispute resolution are either through the courts or outside the courts. In the future, consumer protection must be preventive in nature, and synergy between regulations made by the government is needed so that there is more comprehensive legal protection for consumers (Setiantoro et.al, 2018). Furthermore, a study conducted by Sulasi Rongiyati in 2019 shows that the protection of e-commerce consumers cannot be carried out optimally because the regulation is still scattered in several laws that require implementation rules. Consumer protection provisions in Indonesia have not been able to cover e-commerce consumer protection thoroughly, especially if the parties have different jurisdictions (Rongiyati, 2019). In addition, Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula also conducted a study on the same issue in 2018. This research examines the changes and implications of general data protection regulations in the European Union for private data collection companies (Tikkinen-Piri, Rohunen, & Markkula, 2018). Lastly, there is an international published research by Kamal Halili Hassan which focuses on examining new legal challenges for Malaysia in the protection of personal data (Hassan, 2012).

Based on the description above, this research will examine and re-explain the urgency of protecting personal data of e-commerce consumers. This study focuses on the challenges and legal certainty of protecting personal data of e-commerce consumers. The discussion of personal data protection in this article contains two main points. The first section will examine the challenges of protecting personal data of e-commerce consumers. The second part will review the urgency of protecting personal data of e-commerce consumers in Indonesia.

## B. RESEARCH METHODS

Research method is an effective way of seeking scientific truth. Meanwhile, research is defined as an attempt to analyze and construct methodologically, systematically and consistently. Research can be regarded as a means to strengthen, foster and develop human knowledge. So, this research method contains several aspects, one of which includes ways of thinking to achieve goals. The type of this research was descriptive research. This legal research was a doctrinal research or normative law using literature study or secondary data. The secondary data consist of primary and secondary legal materials. The legal materials were compiled systematically, studied and then a conclusion was drawn in relation to the problem under study.

## C. RESULTS AND DISCUSSION

### 1. The Challenges of Protecting Consumer Personal Data in E-Commerce

#### a. The Definition of Consumers in the Consumer Protection Act in Indonesia

The term consumer comes from and is translated from the word consumer (English-American) or consumer/consumer (Dutch). The literal meaning of the word consumer is (as opposed to producer), everyone who uses goods. The purpose of using these goods and services will determine which group of consumers the user belongs to. Likewise, the English-Indonesian Dictionary, gives the meaning of the word consumer as a user or consumer (Simanullang, 2017). Consumers (*consumers*) are literally defined as “people or business actors who buy certain goods or use certain services”; or "something or someone who uses a stock or number of goods". It also means "everyone who uses goods or services". Those definitions of the term ‘consumer’ shows that there is a difference between consumers as natural persons or natural persons and consumers as business actors or legal entities. This distinction is important to distinguish whether the consumer uses the goods for himself or for commercial purposes (sold, produced again) (Barkatullah, 2007).

Consumer protection arrangements in Indonesia are contained in Law Number 8 of 1999 concerning Consumer Protection (Consumer Protection Law). Article 1 number 1 emphasizes that "consumers are every person who uses goods and/or services available in the community, both for the benefit of themselves, their families, other people, and other living creatures and not for trade". Thus, the definition of consumers can be divided into three parts, namely consumers in the general sense, namely users, users and/or utilization of goods and/or services for certain purposes; intermediate consumers, namely users, users and/or utilization of goods and/services to be produced into other goods/services or to trade them for commercial purposes. These consumers are the same as business actors; and end consumers, namely users, users, and/or utilization of consumer goods and/or services to meet the needs of themselves, their families or households not to be re-traded (Simanullang, 2017).

From the description above, we can put forward the elements of the definition of a consumer. The subject referred to as a consumer means any person who has the status of a user of goods and/or services. The term 'person' here does not distinguish whether an individual person is commonly called a person or is also a legal entity (*rechtspersoon*). Therefore, the most appropriate thing is not to limit the definition of consumers to individuals, but consumers must also include business entities with a broader meaning than legal entities. Thus, consumers can be divided into two categories, namely personal consumers and organizational consumers. Personal consumers are individuals who buy goods and services for their own use, for household use, family members and friends. While the organizational consumer is a company, government agency or other for-profit or non-profit

institutions that buy goods, services and other equipment needed for the organization to run well.

**b. Utilization of Big Data in E-Commerce Activities**

The presence of the internet a few decades ago really has revolutionized the way the world works so fast. Information flows so fast even in real time. The speed of information makes time seem to be shortened, thus this world is like experiencing a time leap. On the one hand, technological developments are so amazing and bring tremendous benefits to the progress of human civilization. Types of work that previously required quite a lot of physicality now relatively can be replaced by automatic machines as if the presence of technology has been able to shift the position of human brain's ability in various sciences and human activities. Advances in technology are now truly recognized and felt to provide a lot of convenience and comfort for mankind (Pujianto, Mulyati, & Novaria, 2018). The world is now entering an era of digitalization, which is an era that emphasizes the *digital economy*.

There are several things that need to be considered in the era of digital economy, namely the issue of protecting the personal data of e-commerce consumers. In online activities, personal data is one of the essential things and is becoming increasingly important in all aspects of human life. Personal data is data relating to a person's characteristics, name, age, gender, education, occupation, address, and position in the family. In juridical, personal data according to the Government Regulation of the Republic of Indonesia Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions is certain personal data that is stored, maintained, and kept true and protected by confidentiality. Residents' personal data that must be protected includes the Family Card number, Population Identification Number, date/month/year of birth, information on physical and/or mental disability, NIK of biological mother, NIK of father, and several contents of important event records. It is very important to protect personal data related to residence such as the Population Identification Number, Identity Card and Family Card so that it is not easily exploited (Mahira, Yofita, & Azizah, 2020).

Some of the benefits of data in *e-commerce* include knowing consumer responses and behavior to the products issued, helping to make decisions more validly and accurately from the many structured data and information obtained, and helping to improve the company's image because it knows consumer desires and market trends through data. The application of data in *e-commerce* provides many benefits and advantages for business people with a large number of consumers. Companies can further develop the system and serve consumers better according to the data in the company. For the business industry such as *e-commerce companies,* the availability of abundant data recorded digitally will be very much needed for a company's decision making. This sea of data leads to one terminology, namely 'Big Data'. Big Data opens up opportunities as a business strategy and innovation in terms of processing, analyzing, and storing data with high and effective volume and speed (Latifah, Farahdiba, &

Kalbu, 2021). For industry circles or practitioners, Big Data has opened up opportunities to set business strategies and innovations in processing, analyzing and storing data with high volumes and levels of volatility as well as quickly and effectively. Therefore, those who are able to process and utilize the data available in large volumes, varied diversity, high complexity and high speed of data addition, can take great advantage (Pujianto, Mulyati, & Novaria, 2018).

Big Data is data collections that have a large capacity and a high diversity of data sources (Joestiwan, 2021). The concept of Big Data begins with data that has various forms, such as text, numbers, and symbols that are sourced from facts but have no meaning. The data obtained will be processed into information or the result of data processing both linguistically and mathematically. The term Big Data began to appear after 2005 introduced by O'Reilly Media. However, the actual use of data and the need to understand the data have existed since ancient times. Big Data was first mentioned in a scientific article entitled '*Application-controlled Demand Paging for Out-of-Core Visualization*' written by Michael Cox and David Ellsworth in 1997. The problems that arise regarding Big Data are stated in the formula "*Visualization provides an interesting challenge for computer systems: data sets are generally quite large, taxing the capacities of main memory, local disk, and even remote disk. We call this the problem of big data*". Big Data terminology is often associated with data science, data mining, and data processing. However, Big Data involves infrastructure and data mining or data processing techniques that are more sophisticated than before (Islah, 2018). The existence of data is becoming increasingly important as Big Data grows. Big Data is a method used by organizations, both state and private, to combine large digital data sets, then use statistics and other data mining techniques to extract the data to be presented in decision making. Big Data has three characteristics, namely the processing of large amounts of data, the use of high-speed processing computers, and the latest computing frameworks. The ability of Big Data is able to increase the effectiveness and large economic profits. That is because it can predict something in the future accurately in a fast and easy timeframe. However, beyond the advantages of using Big Data, there is something that needs to be sacrificed, namely the privacy of our data. Therefore, it is necessary to find common ground between the two. So that personal data remains protected, but economic development, especially through Big Data can still be carried out simultaneously.

Big Data refers to three characteristics referred to as 3V (*volume, variety, velocity*) and some add other V elements such as *veracity* and *value*. *Volume* or capacity is the size of data storage media that can be accommodated up to *zettabytes* IP (*internet protocol*)-based storage capacity. Furthermore, there is a *variety* or data variation that refers to the diversity of data types, while *velocity* is the speed of processing data generated from the source and is *real time*. Meanwhile, *veracity* and *value* are the truth and value associated with the uncertainty of the data

and the value of the benefits of the resulting information (Latifah, Farahdiba, & Kalbu, 2021). The reason Big Data is growing rapidly around the world is because Big Data has advantages in terms of quality and quantity of data compared to other data stores. These advantages also have an impact on the trade and business sectors, and have great potential in the future in business competition (Joestiwan, 2021).

The benefits obtained from the use of Big Data in the business sector, among others, are to know the responses from the community to the products issued by the company, then to build the image of a company towards its consumers, to assist companies in making the right decisions, and to guide them. Accurately based on the data collected, Big data helps business design based on customer behavior data when using their services and benchmarks for a market trend. Big Data also, in the business sector, especially e-commerce, contains data that consists of the combinations of products purchased, in what amount and at what price (Joestiwan, 2021). The opportunity and use of Big Data is very potential in various business and public sectors. The use of Big Data can be designed and implemented more effectively and precisely in order to achieve the target, simply by paying attention to the aspects of cyber security and network infrastructure. However, every advanced technology concept also has some loopholes in security threats. Therefore, the use of large data in Big Data systems also requires security from cyber-attacks so that the data will not be misused by irresponsible parties. Criminals can find loopholes in the developer's technology. Technology is the result of a product development of human logic. Through a different logical approach, many criminals take advantage of this loophole and use it as a doorway to collect data from an organization. Indonesia is considered to be on the list of countries most at risk for digital security (Latifah, Farahdiba, & Kalbu, 2021).

**c. The Challenge of Protecting the Personal Data of *E-Commerce***

In today's digital era, fast data rates are unavoidable. These data contain a collection of information of various kinds and from various places regardless of regional boundaries. Frequently in this data, there is information on the privacy of a person, corporation, or even government (Tikkinen-Piri, Rohunen & Markkula, 2018). This fast data rate is also often used by irresponsible people to harm a person or corporation. This kind of data is considered as valuable data because of the elements it contains (Bieker et.al, 2016). The rapid rate of data and information dissemination are unavoidable, so it is against this background that various countries are competing to formulate and ratify regulations that can overcome the threats caused by the rapid pace of information and data, including the European Union. In 2016, the European Union passed the General Data Protection Regulation (“GDPR”) as a regulation related to personal data that applies in all countries that are members of the European Union. The ratification of the GDPR and its implementation in all European Union countries are intended to harmonize

regulations related to personal data on the European continent.

The GDPR replaces the old European Union personal data regulation passed in 1995, the Data Protection Directive. GDPR is expected to provide more space for individuals to control their personal data. In the passage of regulations and regulations, there must be an underlying principle (Wachter, Mittelstadt, & Floridi, 2017). Principle is the truth that is the basis for thinking, acting, and so on. GDPR also includes the principles used in formulating and implementing rules or regulations related to the processing of personal data in Europe which are listed in Article 5. These principles are important to know so that the public can understand the importance and implementation of this GDPR (Shabani, & Borry, 2018).

**First,** Lawfulness, Fairness and Transparency. This principle explains that the processing and management of personal data must be carried out in a fair, legal and transparent manner. In the application of this principle, the GDPR has determined certain indicators that aim to achieve lawfulness, fairness, and transparency, namely: 1) The identity of the data controller or related third parties who will be involved in data processing; 2) The purpose of processing the relevant data; 3) Any and all recipients or categorization of data recipients; 4) Access rights to own personal data; 5) Contact details for data controller; and 6) Other relevant information that brings justice to the data subject. These indicators serve as the basis for the implementation of GDPR data processing. After the fulfillment of this indicator, a contract must be executed against the data subject as proof of agreement. The contents of the contract are required to protect data and provide legal obligations to data subjects to ensure the legal processing of data. A data processing contract can only be signed by a person who is over 13 years of age. **Second,** Purpose Limitation. Personal data collected must be processed according to its lawful purpose and not further processed in a manner that is inconsistent with that purpose. The delivery of goals must also be explicit in order to avoid multiple interpretations. **Third,** Data Minimization. The personal data collected must be adequate, relevant and limited according to the purpose for which it is processed. This minimization aims to prevent irrelevant data from being processed and hindering the achievement of data processing itself. **Fourth,** Accuracy. The accuracy in question is the accuracy of the data or the quality of the existing data. Existing personal data must be accurate and if necessary keep it updated from time to time. Data inaccuracies can hinder data processing. There are indicators of the obligation of data controllers regulated in the GDPR to ensure data accuracy, namely: 1) Frequency of inspection; 2) Quality of data criteria; 3) Completeness of data; 4) Data consistency; 5) Applicability; 6) Correct representation of the existing reality; 7) The suitability of the data to be used; and 8) Tolerance for inaccuracies. **Fifth,** Storage Limitation. This principle relates to the storage of personal data. Storage of personal data is required to be kept in a form that allows identification of data not to be carried out for

too long. Data that takes long time to process can become inaccurate data because it is not relevant to the current situation. Personal data may also be stored for a longer period of time insofar as it is kept for public, scientific, historical research or statistical purposes. **Sixth,** Integrity and Confidentiality. This principle is related to measuring and ensuring a level of security that is commensurate with the risk to the personal data concerned. All risks, possibilities, and the level of risk impact must be determined by security measures. Particular attention paid to the risks to personal data in the GDPR are: 1) Unintentional or unlawful destruction of data; 2) Data loss; 3) Unintentional or unlawful alteration of data; and Access to unauthorized personal data. **Seventh,** Accountability. The principle of accountability relates to the principle of responsibility of each party related to the processing of personal data. It sets the roles of each party of data processor. Data processing parties must demonstrate compliance with GDPR requirements. All parties must be proactive (have initiatives in data processing according to GDPR), maintain processed personal data, provide notices regarding personal data leaks, and provide updates regarding data processing carried out to data subjects.

All of the above principles aim to provide security for all data processing parties. Data processing is a complicated process because it relates to a person's personal information (Goddard, 2017), therefore GDPR exists as a legal umbrella that protects the rights of European citizens to be protected from data leakage in data processing. These principles need to be adhered to by all parties in order to create a healthy data processing climate without violations (Hoofnagle, Van der Sloot, & Borgesius, 2019).

Digital transformation is having a profound impact on our economy and society, changing the way consumers interacts with each other and online marketplaces (Belwal, Al Shibli, & Belwal, 2020). Consumer data, in this context, has become an important economic asset with a wide range of new and innovative business models, technologies and transactions. Digital Transformation has affected long-standing consumer policy issues, such as asymmetric information and inadequate irregularities, irresponsible business practices, consumer fraud, product security, cooperation between countries, dispute resolution and recovery, sustainable consumption and protection to consumers' vulnerable data. Currently, the increasing penetration of smartphone use in Indonesia has made it easier for consumers, but on the other hand it can also be a threat to conventional economic activities. For example, threats to e-commerce consumer data. Data security and privacy have become an important focus in recent times. Of course, this is bad news for the digital ecosystem that is developing, especially the services that have recently leaked tend to be from large technology companies. In terms of business scale and user coverage, the aspects of data security and privacy (ideally) are components that must exist in a digital product development process. Discussions regarding anticipatory steps from this issue became interesting, especially for the e-

commerce ecosystem in Indonesia, where most of the products are digital and involve users' personal data.

The security of personal data of *e-commerce* should be a guarantee given by the company to its consumers. When consumers feel that their personal data is securely protected by *e-commerce companies,* they will feel free to use the services provided by the company. However, when viewed from cases of data security threats that occur in *e-commerce*, leaked personal data results in the loss of comfort, security, and safety as consumers are no longer fully guaranteed. Therefore, the threat of personal data leakage directly poses a privacy threat to consumers who have provided their personal data to*e-commerce*. In today's era, privacy is considered increasingly important given the emergence of technology that is able to record and store new forms of personal information. This information can include fingerprints and faces. Privacy is a concept that upholds one's independence, authority and self-esteem by respecting the existence of personal space (Pujianto, Mulyati, & Novaria, 2018). However, personal information is not just a mobile number, home address but financial transaction data, location and uploaded photos or images. It is the state's obligation to protect its people, in the fourth paragraph of the opening of the 1945 Constitution of the Republic of Indonesia, it is clearly stated that the government of the Republic of Indonesia is obliged to protect the entire nation and in Law Number 29 of 1999 concerning Human Rights Article 29 paragraph (1) states that every person has the right to personal protection. Indeed, the provision does not explain what personal protection is, but it can be concluded that the protection of personal data also includes the right of a person to keep everything in him private or commonly referred to as self-protection from the right to privacy. Personal data is also something that must be protected because personal data includes the privacy rights of the Indonesian people themselves (Putri, & Fahrozi, 2021).

The challenges in implementing Big Data in Indonesia include: 1) the principle of sharing data. Security in sharing data is certainly vulnerable to cyber-attacks. Therefore, it is necessary to pay attention to the use of the data. Every year the available data will increase so that it is necessary to pay attention to the infrastructure, storage, confidentiality and security of the stored data; 2) government standardization. With the standardization of government data, it can be continued with data integration between agencies for efficiency and preventing redundancy. For example, to make a SIM or to register a system that requires validation of a person's residence number, the use of big data can be done by sharing existing data on the population system so that the data taken is centralized in one source; 3) data security. *Real time* security monitoring is always a challenge given the number of alerts generated by the device (Security). However, Big Data technology may also provide opportunities, in the sense that this technology does not allow for rapid processing and analysis of various types of data. Big data security is very important. If we want the system to be considered 'secure', Big Data must

meet data security requirements, including confidentiality which means a means to protect data from unauthorized disclosure, *integrity* which implies actions taken to protect data from being modified improperly or without permission, and availability, which means the ability of the system to prevent and recover hardware or hardware and software or software failures that may cause the database system or database to not be available properly and efficiently; and 4) HR competence. In utilizing Big Data, governments, organizations, and companies must have competent human resources or HR in the field of data analytics with high programming skills, and the ability to have creativity and innovation in the development of information technology. So that in implementing Big Data, when an unwanted cyber-attack occurs, the Information Technology HR team is able to analyze and solve problems that arise quickly and effectively (Nugroho et.al, 2019). Thus, every sophisticated technological concept has some gaps. Utilization of Big Data also has some forms of privacy and security concerns. For this reason, how companies optimize their data and keep security threats away is a challenge for using Big Data for*e-commerce companies.* This is a complex process and must have clear governance for each company. *E-commerce companies* must improve data security systems and make the level of security vulnerabilities that can be hacked stay in a low percentage. The level of implementation of security systems using Big Data technology should continue to be developed by companies that use this technology.

Privacy is crucial for human life. With privacy, each individual can maintain his identity within the boundaries of social life. The role of privacy in people's social lives is to be able to regulate information entering and leaving the network and data collection in the community. Therefore, with the guarantee of privacy by *e-commerce*, consumers can feel safe and comfortable when using the services of *e-commerce.* Privacy in Big Data includes identity protection, *equality*, security, and *trust*. The existence of the division of privacy in Big Data can make it easier for consumers to demand privacy protection in the form of personal data to *e-commerce* companies. First, the presence of identity protection in Big Data can prevent the emergence of recommendations based on the analysis of individual behavior and preferences that can limit the space for consumers to move. Second, equality includes restrictions on collection, algorithmic transparency and accountability, and restrictions on the use of analytics to sort and treat people differently. Third, security is the existence of a guarantee against the transfer and manipulation of consumer personal data by *e-commerce* or irresponsible outside parties. Fourth, *trust* is the reciprocity that consumers give to *e-commerce* when they feel there is a guarantee of security for privacy and personal data that has been given to the company (Latifah, Farahdiba, & Kalbu, 2021). Seeing the importance of privacy in the form of personal data, *e-commerce* must ensure that sensitive information stored or collected will not be misused by the people who have been given the responsibility to analyze and report it. However, the

emergence of various cases of personal data breaches by irresponsible parties is also due to weak regulations to protect consumers' personal data. The absence of binding laws to protect privacy can make consumers even more worried about personal data being handed over to *e-commerce companies.* In Indonesia, the absence of specific regulations governing the protection of personal data makes this a major challenge in protecting consumer personal data.

**2. Legal Certainty for the Protection of Personal Data of E-Commerce Consumers in Indonesia**

As Indonesian Government aims in the fourth paragraph of the Preamble to the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945), the Government has an obligation to protect the constitutional rights of Indonesian citizens to improve general welfare, participate in educating the entire nation's life, and participate in carrying out world order based on social justice according to the 5th precept of Pancasila as the nation's ideology. So, if there is a data leak that can result in losses for e-commerce users themselves, there must be government accountability to the perpetrators and accountability from e-commerce owners to their consumers. However, Indonesia itself regarding regulations regarding consumer protection against e-commerce data leakage has not given much more attention. There is no law that specifically regulates it (Putri, & Fahrozi, 2021). Regulations regarding the protection of personal data have not yet been ratified. Currently, Indonesia, in handling cases of data leakage that occurs in e-commerce, still adheres to Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 (UU ITE) as well as Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP No. 71/2019).

The protection of personal data has long been recognized as the foundation of the protection of a person's right to privacy. The protection of the right to privacy itself has been explained above which is contained in the provisions of Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. Strictly in the article, it says that everyone has the right to self-protection, meaning that privacy owned by a person should be able to be protected because it is a human right of every person. The statement in Article 28G paragraph 1 of the 1945 Constitution of the Republic of Indonesia is actually the basis for Article 26 of the ITE Law which requires that the use of personal data in electronic media must first seek approval from the data owner. In this regard, every electronic system operator that uses or utilizes a person's personal data must comply with the approval of the owner of the data. The content of the articles aforementioned can be interpreted that any activity such as dissemination or collection of personal data is a violation of privacy because the right to privacy is to determine whether to provide personal data or not.

Articles in the 1945 Constitution of the Republic of Indonesia as well as in the ITE Law have not egulated in detail regarding the actual scope of protected personal data which should include what

and what is regulated regarding personal data and the most important thing is the process of proving what is legally alleged for the theft of personal data or leakage of personal data (Sahetapy, 2021).

The Consumer Protection Law also regulates e-commerce consumer protection. Article 1 point 1 of the Consumer Protection Law emphasizes "consumer protection is all efforts that guarantee legal certainty to provide protection to consumers". The Consumer Protection Law has not been able to protect consumers in e-commerce transactions because the provisions contained in the Consumer Protection Law have not accommodated consumer rights in e-commerce transactions, especially the protection of personal data. This is because e-commerce has its own characteristics compared to conventional transactions. These characteristics are that sellers and buyers do not meet, the media used is the internet, transactions can occur across the juridical boundaries of a country, goods traded can be in the form of goods/services or digital products such as software (Natalia, 2017). However, because there is no lex specialis regulation regarding a person's personal data, a legal framework is needed to protect the existence of a person's Big Data which is completely transparent in this digital world (Joestiwan, 2021). This is supported by many cases of personal data breaches due to the lack of public awareness in protecting their personal data. It is important that according to Article 4 of the Consumer Protection Law, consumers have the right to security in consuming goods and/or services that their personal data is not sold or used without their consent. In line with this, the use of social media in Indonesia has increased sharply. When it comes to using electronic system platforms such as fintech, transportation online and of course e-commerce, in general, users also do not fully understand the privacy policy and terms and conditions of service of each of these applications, especially those related to the use of personal data itself (Joestiwan, 2021).

The right to privacy through data protection is a key element for individual freedom and dignity (Bagheri & Hassan, 2016). Data protection is a driving force for the realization of political, spiritual, religious freedom and even sexual activities. The right to self-determination, freedom of expression and privacy are rights that are important to make us human (Hisbulloh, 2021). Regulations regarding the protection of personal data are very much needed by citizens because without realizing it, personal data can be involved in online crimes committed by parties who have no legal ties and are not responsible. This urgency becomes an urgent agenda that must be considered by Indonesian legislators so that there will be no more violations of privacy rights while at the same time introducing and notifying them as part of human rights that must be protected. As an initial stage, the House of Representatives of the Republic of Indonesia (DPR RI) is currently discussing the Draft Personal Data Protection Law (Personal Data Protection Bill) at the legislative table. This draft acquired its position on the legislative table after being put on the agenda in the 2018 National. Legislative Program was made because the protection of personal data in Indonesia is considered

to be lacking in providing security and guarantees of confidentiality in the field of information and communication technology (Stevani, & Sudirman, 2021), as well as meeting the public's need for their rights as mandated in Article 28G of the 1945 Constitution of the Republic of Indonesia. Article 1 of the Personal Data Protection Bill states "personal data is any data about a person either identified and/or can be identified separately or combined with other information either directly or indirectly through the electronic and/or non-electronic system".

In contrast to the UK, regulations on personal data protection that apply is Data Protection Act 1998. Data Protection Act is a successor to the Data Protection Act 1984. UK also established an implementing agency that has the task of supervising users of personal data, namely The Data Protection Commissioner. The provisions of Data Protection Act 1998 are made to prevent the processing of data if it is deemed to be harmful to the interests of obtaining information. This means that the data obtained should not be stored for too long and should only be used as long as necessary. This regulation is very strong on the protection of personal data, so that if personal data is transferred to another place, strict sanctions will be imposed with the exception that the recipient of the personal data can guarantee similar data protection (Sahetapy, 2021).

Returning to the discussion of the Personal Data Protection Bill, the reason for the presence of the Personal Data Protection Bill is to reduce the overlapping provisions regarding the protection of personal data, so this bill is a standard for protecting personal data in general, whether partially or completely processed both electronically and manually, where each sector can apply personal data protection according to the characteristics of the sector concerned, including the provisions on personal data that have been regulated in professional provisions (Nurmalasari, 2021). The basis of the formulation of norms and implementation in the protection of personal data is based on the principle of protection, the principle of legal certainty, the principle of public interest, the principle of expediency, the principle of prudence, the principle of balance, and the principle of responsibility.

Following the Responsive Legal Theory, it is necessary to have personal data protection in a transition period. Based on this theory, the law must be sensitive to the transitional situation around it, so responsive law is not only required to be an open system, but also must rely on the primacy of purpose, namely the social goals it wants to achieve and the consequences arising from the operation of the law (Utomo, 2020). Responsive law is a model or theory initiated by Nonet-Selznick in the midst of a scathing Neo-Marxist critique of liberal legalism. As is well known, liberal legalism presupposes law as an independent institution with an objective, impartial, and completely autonomous system of rules and procedures. The icon of liberal legalism is legal autonomy. The most obvious form of autonomy is the rule of law. With its autonomous character, it is believed that the law can control repression and maintain its own integrity. For a responsive legal order, the law is a social institution. Therefore, law is

seen as more than just a system of regulations, but also how the law carries out social functions in and for the community. Seeing law as a social institution means seeing the law in a broad framework, which involves various processes and forces in society (Sulaiman, 2014).

Based on the Academic Paper of the Personal Data Protection Bill, the regulation of personal data protection in this bill aims, among others, to protect and guarantee the basic rights of citizens related to personal self-protection, to guarantee the public to receive services from the government, corporations, business actors, and other organizations/institutions, encourage the growth of the digital economy and the information and communication technology industry, and support the improvement of the competitiveness of the domestic industry. Therefore, the ratification of this bill into a law is considered urgent. Not only as an effort to protect the personal data of e-commerce consumers, but also as an effort to protect the public's personal data in general.

There is a relevant principle in Academic Paper of the Personal Data Protection Bill, which says that "parties related to issues regarding data processing, data dissemination, management and monitoring of personal data must act responsibly". Responsible means in accordance with the principles of personal data management and the principle of consumer protection responsibility. Of course, the material content in the Personal Data Protection Bill is in accordance with the principle of consumer protection, because consumers in this modern era have made it easier to use the help of e-commerce applications (Putri, & Fahrozi, 2021). Most of them have to register their personal data as proof of user of the ecommerce itself, of course this personal registration will cause concern for consumers that their personal data will be used or even traded without their consent.

## D. CONCLUSION

The application of data in e-commerce provides many benefits and advantages for business people with a large number of consumers. Companies can further develop the system and serve consumers better according to the data in the company. Privacy is crucial for human life. With privacy, each individual can maintain his identity within the boundaries of social life. The absence of binding laws to protect privacy can make consumers even more worried about personal data being handed over to e-commerce companies. In Indonesia, the absence of specific regulations governing the protection of personal data makes the protection of personal data of e-commerce consumers a major challenge. Legal certainty for the protection of personal data of e-commerce consumers is currently contained in several laws and regulations. Efforts to increase effectiveness in the implementation of personal data protection require regulations regarding the protection of personal data in a law. In Indonesia, the ratification of the Personal Data Protection Bill can be regarded as a solution to protect e-commerce consumers from personal data leakage, in which registration for the use of e-commerce requires filling in data pertaining to

personal data, which we will often encounter on the internet. The similarity and conformity of the content in the Personal Data Protection Bill with the principle of consumer protection provides added value and I firmly believe that this Personal Data Protection Bill needs to be ratified in order to become a solution for consumers who feel aggrieved. Because every consumer has the right to get compensation or compensation, as well as in the material content of the Personal Data Protection Bill, it says that data holders have the right to get compensation for losses resulting from violations of their rights. Holders of personal data here include consumers. Adequate protection of privacy regarding personal data will be able to give public confidence to provide personal data and/or information, for the greater interest of the community without being misused or violating consumers' personal rights.

## REFERENCES

### JOURNALS

Amboro, Yudhi Priyo., & Christi, Agustina. (2019). Prospek Pengaturan Cryptocurrency sebagai Mata Uang Virtual di Indonesia (Studi Perbandingan Hukum Jepang Dan Singapura). *Journal of Judicial Review*, Vol. 21,(No.2),pp.14-40. http://dx.doi.org/10.37253/jjr.v21i2.665

Anugerah, Dian Purnama., & Indriani, Masitoh. (2018). Data Protection in Financial Technology Services (A Study in Indonesian Legal Perspective). *Sriwijaya Law Review*, Vol.2,No.(1),pp.82-92. http://dx.doi.org/10.28946/slrev.Vol2.Iss1.112.pp82-92

Ayunda, Rahmi., & Rusdianto. (2021). Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence dalam Aktifitas Perbankan di Indonesia. *Jurnal Komunikasi Hukum (JKH)*, Vol.7, (No.2), pp.663-677. http://dx.doi.org/10.23887/jkh.v7i2.37995

Barkatullah, Abdul H. (2007). Urgensi Perlindungan Hak-Hak Konsumen Dalam Transaksi Di E-Commerce. *Jurnal Hukum Ius Quia Iustum*, Vol.14, (No.2), pp.247-270. https://doi.org/10.20885/iustum.vol14.iss2.art8

Bagheri, Parviz., Hassan, Kamal Halili., & Mansour, Mehdi Shabannia. (2017). Parties' legal capacity in electronic commerce transactions. *European Journal of Law and Economics,* Vol.44,(Vol.3),pp.503-515. https://link.springer.com/article/10.1007/s10657-012-9372-x

Bagheri, Parviz., & Hassan, Kamal Halili. (2016). Data Privacy in electronic commerce: Analysing legal provisions in Iran. *Journal of Internet Banking and Commerce,* Vol.21, (No.1),p.147. https://www.icommercecentral.com/open-access/data-privacy-in-electronic-commerce-analysing-legal-provisions-in-iran.php?aid=67480

Barkatullah, Abdul Halim., & Djumadi. (2018). Does self-regulation provide legal protection and security to e-commerce consumers?. *Electronic Commerce Research and*

*Applications*,Vol.30,pp.94-101. https://doi.org/10.1016/j.elerap.2018.05.008

Belwal, Rakesh., Al Shibli, Rahima., & Belwal, Shweta. (2020). Consumer protection and electronic commerce in the Sultanate of Oman. *Journal of Information, Communication and Ethics in Society,* Vol.19, (No.1), pp. 38-60. https://doi.org/10.1108/JICES-09-2019-0110

Bieker, Felix., Friedewald, Michael., Hansen, Marit., Obersteller, Hannah., & Rost, Martin. (2016). A process for data protection impact assessment under the european general data protection regulation. In *Annual Privacy Forum*, Vol. 9857, pp. 21-37. https://doi.org/10.1007/978-3-319-44760-5_2

Disemadi, Hari S. (2021). Fenomena Predatory Lending: Suatu Kajian Penyelenggaraan Bisnis Fintech P2P Lending selama Pandemi COVID-19 di Indonesia.*Pandecta Research Law Journal*,Vol.16,(No.1),pp.55-67. https://doi.org/10.15294/pandecta.v16i1.26860

Disemadi, Hari S. (2021). Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia. *Jurnal Wawasan Yuridika*, Vol.5, (No.2),pp.177-199. http://dx.doi.org/10.25072/jwy.v5i2.460

Disemadi, Hari Sutra., & Regent. (2021). Urgensi Suatu Regulasi yang Komprehensif Tentang Fintech Berbasis Pinjaman Online Sebagai Upaya Perlindungan Konsumen di Indonesia. *Jurnal Komunikasi Hukum (JKH)*, Vol.*7*,(No.2),pp.605-618. http://dx.doi.org/10.23887/jkh.v7i2.37991

Fathur, M. (2020). Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen. In*National Conference on Law Studies (NCOLS)*,Vol.2,(No.1),pp.43-60. https://conference.upnvj.ac.id/index.php/ncols/article/view/1345

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, Vol.59,(No.6),pp.703-705. https://dx.doi.org/10.2501/IJMR-2017-050

Hassan, Kamal H. (2012). Personal data protection in employment: New legal challenges for Malaysia. *Computer Law & Security Review*, Vol.28,(No.6),pp.696-703. https://doi.org/10.1016/j.clsr.2012.07.006

Hisbulloh, Moh H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi.*Jurnal Hukum*, Vol. *37*,(No. 2), pp. 119-133. http://dx.doi.org/10.26532/jh.v37i2.16272

Hoofnagle, Chris Jay., Van der Sloot, Bart., & Borgesius, Frederik Zuiderveen. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*,Vol.28,(No.1),pp.65-98. https://doi.org/10.1080/13600834.2019.1573501

Islah, K. (2018). Peluang Dan Tantangan Pemanfaatan Teknologi Big Data Untuk Mengintegrasikan Pelayanan Publik Pemerintah.*Jurnal Reformasi Administrasi:*

*Jurnal Ilmiah untuk Mewujudkan Masyarakat Madani*,Vol.5,(No.2),pp.130-138. https://doi.org/10.31334/reformasi.v5i2.272

Joestiwan, Michael W. (2021). Perlindungan Privasi Konsumen Terhadap Pemanfaatan Big Data.*Informatika*, Vol. 9, (No. 11), pp. 916-927. https://ojs.unud.ac.id/index.php/Kerthanegara/article/view/73375

Kumar, Sanjeev., Belwal, Rakesh., & Raina, Kartikeya. (2019). Decision-making styles of young Indian consumers in the context of online shopping. *International Journal of Internet Marketing and Advertising,* Vol.13, (No.3),pp.253-270. https://www.inderscienceonline.com/doi/abs/10.1504/IJIMA.2019.102568

Mahira, Dararida Fandra., Yofita, Eemilda., & Azizah, Lisa Nur. (2020). Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept. *Jurnal Legislatif*, Vol.3, (No.2), pp.287-302. https://doi.org/10.20956/jl.v3i2.10472

Natalia, H. (2017). Perlindungan Hukum Terhadap Konsumen Dalam Transaksi E-Commerce. *Melayunesia Law*, Vol.1,(No.1), pp.111-126. http://dx.doi.org/10.30652/mnl.v1i1.4497

Nurfitri, Nisa., Sudirman, Lu., & Disemadi, Hari Sutra. (2022). TikTok Phenomenon: Exoneration Clause VS. Personal Data Protection. *Jurnal Pendidikan Kewarganegaraan Undiksha*, Vol.10,(No.1),pp.441-453. https://doi.org/10.23887/jpku.v10i1.46478

Nugroho, Fendy Prasetyo., Abdullah, Robi Wariyanto., Wulandari, Sri., & Hanafi. (2019). Keamanan Big Data di Era Digital di Indonesia.*Jurnal Informa: Jurnal Penelitian dan Pengabdian Masyarakat*, Vol.5,(No.1), pp. 28-34. https://doi.org/10.46808/informa.v5i1.65

Nurmalasari. (2021). Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum. *Syntax Idea*, Vol.3*,* (No.8), pp.1947-1966.https://doi.org/10.36418/syntax-idea.v6i8.1414

Paryadi, D. (2018). Pengawasan E Commerce Dalam Undang-Undang Perdagangan Dan Undang-Undang Perlindungan Konsumen. *Jurnal Hukum & Pembangunan*, Vol.48, (No.3), pp. 651-669. http://dx.doi.org/10.21143/jhp.vol48.no3.1750

Pujianto, Agung., Mulyati, Awin., & Novaria, Rachmawati. (2018). Pemanfaatan Big Data Dan Perlindungan Privasi Konsumen Di Era Ekonomi Digital.*Majalah Ilmiah Bijak*, Vol.15, (No.2),pp.127-137. https://doi.org/10.31334/bijak.v15i2.201

Putri, Deanne Destriani Firmansyah., & Fahrozi, Muhammad Helmi. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka. Com). *Borneo Law Review*, Vol. 5*,* (No. 1), pp. 46-68. https://doi.org/10.35334/bolrev.v5i1.2014

Rahayu, Rita., & Day, John. (2015). Determinant factors of e-commerce adoption by SMEs in developing country: evidence from Indonesia.

*Procedia-social and behavioral sciences*, No. 195,pp.142-150. https://doi.org/10.1016/j.sbspro.2015.06.423

Rongiyati, S. (2019). Pelindungan Konsumen Dalam Transaksi Dagang Melalui Sistem Elektronik. *NegaraHukum*,Vol.10,(No.1),pp.1-25. https://doi.org/10.22212/jnh.v10i1.1223

Sahetapy, Wilma L. (2021). Perlindungan Data Pribadi Anak Dalam E-Commerce Di Masa Pandemi Covid-19. *Jurnal Hukum Bisnis Bonum Commune*,Vol.4,(No.2),pp.214-225. https://doi.org/10.30996/hukum%20bisnis%20bon.v4i2.5319

Setiantoro, Arfian., Putri, Fayreizha Destika., Novitarani, Anisah., & Njatrijani, Rinitami. (2018). Urgensi Perlindungan Hukum Konsumen Dan Penyelesaian Sengketa E-Commerce Di Era Masyarakat Ekonomi Asean. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, Vol. 7, (No. 1), pp.1-17.http://dx.doi.org/10.33331/rechtsvinding.v7i1.220

Setyawan, Aalfis., & Wijaya, Bella. (2018). Perlindungan Konsumen dalam Transaksi E-Commerce Ditinjau dari Undang-Undang Perlindungan Konsumen.*Journal of Judicial Review*,Vol.19,(No.2),pp.46-70. https://journal.uib.ac.id/index.php/jjr/article/view/290

Shabani, Mahsa., & Borry, Pascal. (2018). Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European Journal of Human Genetics*, Vol.26,(No.2),pp.149-156. https://doi.org/10.1038/s41431-017-0045-7

Simanullang, Heldya N. (2017). Perlindungan Hukum Terhadap Konsumen Dalam Transaksi E-Commerce. *Melayunesia Law*, Vol. 1, (No. 1), pp.111-126. http://dx.doi.org/10.30652/mnl.v1i1.4497

Stevani, Winnie., & Sudirman, Lu. (2021). Urgensi Perlindungan Data Pengguna Financial Technology terhadap Aksi Kejahatan Online di Indonesia.*Journal of Judicial Review*, Vol. 23, (No.2),pp.197-216. http://dx.doi.org/10.37253/jjr.v23i2.5028

Sulaiman. (2014). Hukum Responsif: Hukum Sebagai Institusi Sosial Melayani Kebutuhan Sosial Dalam Masa Transisi. *Jurnal Hukum Samudera Keadilan*, Vol. 9, (No. 2), pp. 199-205. https://repository.unimal.ac.id/1744/

Tan, Kendry., & Disemadi, Hari Sutra. (2021). Urgency of Electronic Wallet Regulation in Indonesia. *Nagari Law Review*, Vol.5*,* (No.1), pp.1-14. https://doi.org/10.25077/nalrev.v.5.i.1.p.1-14.2021

Tikkinen-Piri, Christina., Rohunen, Anna., & Markkula, Jouni. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, Vol.34,(No.1),pp.134-153. https://doi.org/10.1016/j.clsr.2017.05.015

Utomo, P. (2020). Omnibus Law: Dalam Perspektif Hukum Responsif.*Nurani Hukum: Jurnal Ilmu*

*Hukum*,Vol.2,(No.1),pp.33-41. http://dx.doi.org/10.51825/nhk.v2i1.8168

Wachter, Sandra., Mittelstadt, Brent., & Floridi, Luciano. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, Vol.7,(No.2),pp.76-99. https://dx.doi/org/10.1093/idpl/ipx005

**ONLINE SOURCE**

Latifah, May., Farahdiba, Rachel., & Kalbu, Ratu Mutiara. (2021). Ancaman Keamanan dan Privasi Konsumen dalam Kebocoran Big Data E-Commerce. Retrieved from https://www.balairungpress.com/2021/05/ancaman-keamanan-dan-privasi-konsumen-dalam-kebocoran-big-data-e-commerce/