



The Responsibility of the Online Marketplace to Protect Consumer Data Privacy in E-commerce Transactions

Firman Freaddy Busroh ¹, Fatria Khairo ², Putri Difa Zhafirah ³

¹ Doctor, Law Study Program, Sekolah Tinggi Ilmu Hukum Sumpah Pemuda, Palembang, Indonesia

² Doctor, Law Study Program, Sekolah Tinggi Ilmu Hukum Sumpah Pemuda, Palembang, Indonesia

³ Undergraduate Student, Law Sekolah Tinggi Ilmu Hukum Sumpah Pemuda, Palembang, Indonesia

* **Corresponding Author:** argiaglobal@gmail.com

Citation: Busroh, F. F., Khairo, F., & Zhafirah, P. D. (2024). The responsibility of the online marketplace to protect consumer data privacy in e-commerce transactions. *China and WTO Review*, 10(1), 61-68. <https://doi.org/10.52152/cwr.2024.10.1.05>

ARTICLE INFO

Received: 13 Jul 2024

Accepted: 24 Oct 2024

ABSTRACT

Currently, the business world cannot be separated from digital transactions. Internet users continue to increase, and e-commerce transactions also increase. Almost all companies, both small and large companies, trade using the Internet network. The development of the Internet has taken over the conventional business world to become all digital. Even e-commerce transactions do not only use money transfer payments between banks but also through digital payment platforms. This is why consumers do not realize that providing privacy data is easy for companies through the marketplace. For this reason, there are many cases of misuse of personal data that occur. The marketplace must be responsible for protecting personal consumer data. The research method used in writing the paper uses a qualitative descriptive approach. The research with this method is intended to collect essential and detailed information, identify problems, make comparisons or evaluations. The result of this research is to make laws and regulations governing the security of consumer data in the online market. Assisting the government in making laws and regulations regarding consumer data in the online market, so that consumers feel safe for electronic transactions.

Keywords: Online Marketplace, Consumer Privacy Data, E-commerce.

INTRODUCTION

A large number of Internet users in Indonesia shows a significant market potential that will affect the emergence of various new business opportunities. On the other hand, several things need to be considered in online shopping activities, namely, the issue of protecting personal data and online consumers. In online activities, personal data is one of the essential things, especially concerning payment methods, marketing, and offers.

E-commerce companies offer and market their goods depending on what is known as ad-targeting. Ad-targeting is an activity by industry and businesses to sell a product or service by targeting potential consumers. The background of ad-targeting is the existence of technology that provides convenience and accuracy in promotion and marketing at low costs.

Online shopping activities have become a separate phenomenon in Indonesia. Data and reports compiled by the Wall Street Journal and We are social show a significant increase in online activities. This cannot be separated from the number of active Internet users who use mobile Internet to carry out their online activities (Kemp, 2015).

With the technology used, there are potential problems in using consumers' data, including tracking online transactions where there are shopping preferences, shopping locations, and communication data to a consumer's address.

The technology is called cookies; these devices can record our search activities, and the result is ad targeting that matches the results of previous online searches of consumers. Intervention practices on privacy and

interference with personal data are certainly some of the big problems that arise, especially with the increasing use of information and communication technologies such as cookies in ad-targeting (Kurbalija, 2016).

This situation indeed results in the vulnerability of the protection of the right to privacy of each online consumer. In various countries, issues related to privacy and regulations regarding privacy have begun to develop as an integral part of the social development of their society.

Experience in several democratic countries shows that positive law and jurisprudence existed long before privacy became integral to the international human rights law regime. Recently, the UN Human Rights Council has adopted Resolution 68/167 on protecting the right to privacy in the digital age. One of its clauses asserts that everyone has the same ownership when offline and must also be protected online, including the right to privacy. In Indonesia itself, the issue of the importance of protecting the right to privacy has strengthened along with the increasing number of cellular phone and Internet users in recent years (Tim Privacy International & ELSAM, 2015).

In its report, The Wall Street Journal stated that the development of online activities was supported by access to Internet network infrastructure. Several cases that have emerged, especially those related to the leakage of someone's data, which have resulted in fraudulent actions, have strengthened the discourse on the urgency of enhancing the protection of the right to privacy. In everyday facts, the absence of a mechanism for protecting privacy, especially personal data, impacts consumers' offerings and various products, ranging from property, insurance, and loan facilities to credit cards. On the other hand, consumers have never submitted their personal data to the producers concerned regarding their preferences for a product or service.

ISSUE

1. How are online consumer privacy settings in the online marketplace system?
2. How to protect the privacy and personal data in the online marketplace system?

METHODOLOGY

The research method used in writing the paper uses a qualitative descriptive approach. The research with this method is intended to collect essential and detailed information, identify problems, make comparisons or evaluations, and determine what other people do in dealing with the same problem and learn from their experiences to set plans and decisions in the future. Thus, qualitative descriptive research only describes responses to a situation, event, or phenomenon, so no explanation is needed between causality and hypothesis testing.

DISCUSSION

In the application of commercial business, the buying and selling process in e-commerce is very different from the conventional system, where all functions, from finding information about the goods or services needed and placing orders to payments, can be made electronically through the media. This indicates that literacy in digital technology in Indonesian society is quite good. This is supported by Internet penetration which has reached many areas in Indonesia.

Based on the Survey Results Report issued by the Indonesian Internet Service Providers Association (APJII) in 2018, with the title Penetration and Profile of Internet Users in Indonesia (APJII, 2018), it is stated that Internet user penetration reaches 171.17 million people from the total population of Indonesia which ranges from around 264.16 million people. This means that technological advances have touched approximately 64.8% of Internet users in Indonesia without discriminating against users regarding gender and age (APJII, 2018).

For Internet penetration per region of all Internet users in Indonesia, it can be seen that Sumatra Island has a penetration rate of 21.6% of users, Java Island reaches 55.7% of users, Kalimantan Island reaches 6.6% of users, Sulawesi and Papua Islands reach 10.9% of users. The islands of Bali and Nusa Tenggara reached 5.2% of users. So it can be concluded that the penetration of inter-island Internet users in Indonesia is still dominant.

According to the Scientific Journal of Business Orations with the title Utilization of E-Commerce in the Business World (Irmawati, 2011), Electronic Commerce, commonly referred to as e-commerce, is the process of buying and selling or exchanging products. Or services or in the form of information through Internet network media and computer equipment. E-commerce is one part of e-business, where the coverage area of e-business is much wider, not only covering commerce or trade but also including collaboration with business partners, banking sectors such as services to customers, and the fintech industry (financial technology), the tourism

industry, job vacancies, and insurance.

In the Scientific Journal of Business Orations, with the title Utilization of E-Commerce in the Business World (Irmawati, 2011), it is also mentioned the classification of forms of e-commerce itself, including:

1. Business to Business (B2B), which has characteristics such as trading partners, data exchange, as well as the most commonly used models such as peer-to-peer, where processing intelligence can be distributed across both businesses.

2. Business to Consumer, which has characteristics such as the services provided are only general in nature based on the website, and services are provided based on requests for customer needs in the form of products and services using a systematic system.

3. Trading collaborative.

4. Consumer to Consumer, where someone sells products or services to customers directly.

5. Consumer to Business, where customers provide a list of needs for a particular product or service, and service providers compete healthily to provide the best service, both in the form of products and services to customers.

6. Intra organizational trade.

7. Government to Citizen (Government to Citizen technology system e-commerce reliable).

8. Mobile Commerce, where the process is carried out in wireless communication lines, such as the use of cell phones in accessing the Internet and transacting, is then called m-commerce.

In a Proposed Design Report, Principles, and Policy Recommendations: Big Data, Artificial Intelligence, Blockchain, and Financial Technology in Indonesia (Ramadhan & Putri, 2018) addressed to the Directorate General of Informatics Applications of the Ministry of Communications and Information Technology (KOMINFO), the concept of big data consists of several characteristics, namely volume, variety, and velocity.

For the characteristics of volume, big data literally means big data or a lot. Today, the world has entered the Zettabyte era where-based communication traffic Internet protocol has increased rapidly in the last three years. The second characteristic is variety; here, it is stated that data variation refers to various kinds of data variations and types. Sources of data variation are dominated by the activity of using search engines on the Internet, social media, and M2M connections in the form of IoT. While the third characteristic of big data is velocity, where big data is not only indicated by the amount of data generated but also by the speed of data production, which also takes place in real time.

From the description of the characteristics that have been mentioned, it is realized that the role of big data in e-commerce is very much needed. The first characteristic is related to the volume of data, which is increasing daily. The number of customers increasing daily will require bigger data storage. The second characteristic is that the exponential data variation will also increase along with the volume of incoming data. This is because the data recorded in storage is not only about personal data but also includes image data, sound, and even electronic data, such as the history of the conversation. The volume of incoming data and data variations are very varied, and data access speed becomes the most needed thing and should be the main concern in big data business networks e-commerce.

Cholissodin and Riyandani (2016) explain that Big data consists of several parts, namely Data Device, Data Collector, Data Aggregator, and Data User/Buyer. In addition, it also explains the role of the concept of analytics which is the beginning or the beginning of an understanding of how to explore or investigate in the depth of a data object. The results from analytics usually do not cause much confusion because the context is a clear description of meaning. The development of analytics itself started with DSS (Decision Support System) and then developed into BI (Business Intelligence).

Definition of Online Marketplace System

Classical economic law theory has given signs regarding how trading systems and mechanisms are carried out, where if there is a demand (Supply), there is always a supply (Demand), even if things happen in e-commerce, which is needed by consumers. Service providers in e-commerce see an opportunity that privacy data from online consumers makes it easy to find out and sell products as desired precisely and effortlessly, even though this has clearly violated the privacy rights of online consumers themselves.

The definition of an online marketplace system, according to Albert J. Marcella Jr. and Carol Stucki, is the collection and use of personal information for marketing purposes. In these terms, it can be seen that the definition is related to the Online Marketplace System as a way of collecting personal data online for business

purposes. In addition to violating consumer privacy rights, it is also a form of ignoring the principles of trust built between consumers and e-commerce service providers by providers of online marketplace system platforms (Marcella Jr & Stucki, 2003).

Furthermore, the cookie used for online marketplace system platform to collect various kinds of one's product search preferences is used as a knowledge base and interest from potential buyers and knowledge for online marketplace system platform which advertisements are suitable to be marketed persistently to prospective the right buyer, this can be known through actions taken by prospective buyers such as repeated access to a site; interaction; keywords; product content searched online; etc., at least that's what Rosemary Jane describes to define an online marketplace system.

Online marketplace system, according to GBFNiblett's view, also affirms the same understanding, which in its meaning is mentioned as the use of online media access to enter things that are not desired from the privacy rights of individuals whose privacy policy in the Online Marketplace System (Niblett, 1992).

By definition, Anup K. Gosh describes the Privacy Policy as "... as a comprehensive description of a Web site's practices which is located in one place on the site and may be easily accessed. Every organization involved in electronic commerce transactions has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information" (Ghosh, 2012).

The privacy policy is a complete description that states the responsibilities and implementation of these provisions in order to protect the privacy rights of an individual who has disclosed his private data in e-commerce activities. Privacy policy in every transaction of e-commerce can be accessed easily, this is because these provisions are very important in e-commerce as a code of conduct that is respected by the parties.

Settings Privacy Policy in the Online Marketplace System according to Positive Indonesian Law

Indonesia generally has legal regulations governing privacy policy in the online marketplace system, which is contained in Law Number 11 of 2008 concerning Information and Electronic Transactions (Law Number 18 of 2008 concerning ITE) and Government Regulation Number 28 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP Number 28 of 2012 concerning PSTE). One of the lead sectors of the Government of Indonesia that handles e-commerce is the Ministry of Communication and Information (KEMENKOMINFO) of the two legal regulations, the Ministry of Communication and Information has a registration and data collection program for e-commerce through a series of profiling and report database processes. This is to prevent consumers from being scammed by irresponsible people.

In the future, the projection of privacy data protection through the privacy policy in online marketplace systems will continue to improve because two legal regulations specifically regulate privacy rights, namely the Draft Ministerial Regulation on Personal Data Protection which is a mandate from PP No. 82 of 2012 and the Draft Law -Law on the Protection of Personal Data, these two legal regulations are encouraged by the government to answer the needs of the community related to the protection of consumer privacy. The purpose of these legal regulations is to encourage standard clauses that are often served to potential consumers on e-commerce applications to be fair and open to be agreed upon by both parties.

The actual conditions in e-commerce show that consumers are the weak parties in each of these transactions, meaning that technical rules related to the code of conduct of e-commerce are expected to be able to protect consumer interests through the per-consent of the privacy policy that applies in every e-commerce to be agreed upon by both parties so that the online marketplace system platform does not easily collect data for profit-oriented.

In this context, the state is just and fair in being the "middle party" and being the party that controls the privacy policy service provider e-commerce/seller with the consumer regarding privacy data that is carried out online. So that in this context, the standard clause of the privacy policy, which has many shortcomings, can be corrected immediately so that the rights of consumers are not violated.

Settings Privacy Policy in the Online Marketplace System in Several Countries

In several countries, especially in member countries of the European Union and the United States, where established conditions for e-commerce mechanism privacy policy in the online marketplace system have been set forth in various legal regulations, both in terms of international law, regional level (such as EU Directive) as well as in national legislation.

In European Union, general arrangements regarding e-commerce in the European Union are set forth in the Europe Union Directive on Electronic Commerce¹⁵ (EU Directive on E-Commerce), which regulates the relationship of the parties in e-commerce (Business to Business, B2B), including which legal mechanisms are

related, which is used by the parties in the event of a legal issue being applied, including which jurisdiction and court are authorized to adjudicate in e-commerce disputes.

Article 3 (1) of the EU Directive on E-Commerce regulates the interpretation of this rule in any area where it can be applied, namely:

1. The rules in the relevant international private law are applied in every e-commerce transaction.
2. This rule regarding private international law is related to the relevant IPL Rules of the country's establishment of the information society service provider (ISSP), which is applied in e-commerce transactions.
3. These rules are only centered on legal substance, so international private law cannot be applied/prohibited if it has been strictly regulated in the national legal mechanisms of the parties.

In relation to international legal regulations regarding the protection of privacy rights in e-commerce, the Organization for Economic Cooperation and Development (OECD), which is an inter-governmental organization consisting of 29 member countries from the European Union, United States, Australia, and New Zealand have made multilateral agreements related to the protection of privacy data in e-commerce in the context global marketplace. Where in the recommendation provides an obligation for state parties to make national regulations with specific principles regarding the protection of privacy and individual freedom relating to online consumer privacy data recorded in cookies so that they are not misused; this is a legal formulation that is universal and applies to the states parties.

At the European Union level, there are legal regulations at the regional level that regulate the protection of privacy data in e-commerce activities, such as the EU Directive on the protection of Consumers in Respect of Distance Contracts, the legal regulations that regulate: consumer protection from contract terms unfair trade, sales and guarantees for the period of a sale, it relates to how the harmonization and renewal of laws between member states of the European Union for consumer contracts both goods and services.

It was adopted in 1995 European Union Data Protection Directive (EU Data Protection Directive), which provides provisions regarding the protection of privacy data for the European Union (EU), in addition to those relating to the prohibition of the free flow of information between member countries. EU was also developed for the conduct of business and e-commerce.

More specifically, the privacy policy in the online marketplace system in the European Union is regulated in Article 7 EU Directive on E-Commerce. It is regulated more specifically in Article 5(3) of the Privacy and Electronic Communication Directive 2002 (PECD). In the online marketplace system, which has had a significant impact on the violation of the privacy data of online consumers conducting e-commerce transactions, there needs to be an effort to ban this technology in all e-commerce that is mandatory to comply with.

All e-commerce including companies that produce products that will be marketed in e-commerce, as well as banking companies that produce credit cards for consumers in the European Union, are required to make clear provisions and be adhered to by the parties through a privacy policy that in accordance with the standards of the EU Directive .privacy policy must be honest and contain comprehensive information, both about the purpose and process of online data processing so that the privacy rights of online consumers are not violated in the e-commerce activities.²¹

Apart from being applicable at the EU regional level, various regulations relating to the privacy policy in the online marketplace system are also applied in the national legal provisions of several countries in the European Union; not all European Union countries will be discussed in this discussion, and the discussion is devoted to countries that have been established in making privacy policies in online marketplace system, these countries are France, Germany, the United Kingdom.

The French state, had a long-standing legal regulation in 1978 relating to data processing, data files, and individual liberties (relative it le Informatique, aux fichiers et aux liberties); legal regulation then some changes adjusted the provisions in the EU Directive.

Article 1 of the Law states, "Computers must be at the service of each citizen. Their development must occur in the framework of international cooperation. It must cause no damage or loss to either human identity, human rights, right of privacy, or to public and individual liberties". The legal regulations implicitly state that the French government guarantees the use of computer technology, especially the Internet, in accordance with international legal mechanisms (both applicable at the regional level of the European Union and internationally) and without violating human rights, privacy rights, and individual freedoms.

Mainland England, the United Kingdom consisting of England, Wales, and Ireland have legal regulations relating to data privacy; this is stated in The Data Protection Act 1998, which contains provisions regarding

personal information in national legal regulations regulated under English law. It can be summarized that the right to privacy in the aspect of e-commerce regulates:

1. A fair and legal process (including matters relating to sensitive online consumer information).
2. Processes and specific objectives of privacy data management.
3. Circumstances, relevance, and things that are not allowed related to the management of privacy data.
4. Data can be collected regarding the suitability of the purpose for which the data is collected/not for profit.
5. Respect the rights of each individual with regard to personal data information and search preferences in e-commerce activities.
6. Protect against unauthorized access to personal data.
7. Can accept the consequences of arrangements outside the legal jurisdiction determined by the European Union as long as they do not conflict with the rules in the United Kingdom regarding the protection of privacy data.

Similar to countries in the European Union, the arrangements regarding the protection of privacy data in the United States are discussed in detail, where the approach used by the United States government prevents specific violations of privacy and sensitive data; this applies both in countries -States and federal states.

Regarding the protection of consumer privacy data, it is regulated by the Federal Trade Commission Act 2010 (FTC Act 2010), which is reported in "Protecting Consumer Privacy in an Era of Rapid Change; A Proposed Framework for Business and Policymaker."

The FTC Act 2010 can be seen as related to the framework of the relationship between electronic transactions from e-commerce and online consumers, namely:

1. Implement and establish privacy data protection principles in every business practice.
2. Provide ample space for consumers to respect the protection of their private data, including in the context of exploiting the commercial interests of the privacy data itself.
3. Do the practice of using private data more transparent so that no party's rights are infringed.
4. Take steps to educate consumers regarding the practice of using private data for commercial purposes with the choices available.
5. In law enforcement for violators of the 2010 FTC Act, the American government has agencies for consumer protection, namely: (i) the US Department of Commerce, the White House/sub-section of the US Presidency (National Strategy of Trusted Identities in Cyberspace Initiative) in collaboration with the other civil society to promote privacy, security, and protection of sensitive data in online transactions.

Benefits of Setting Privacy Policy

Benefits achieved in setting privacy policy in e-commerce if it is carried out and adhered to properly by both parties, namely:

1. Increase the sense of security and trust between online consumers and e-commerce providers.
2. Protection of privacy rights for online consumers in e-commerce activities carried out.
3. Creating a healthy business competition climate in every electronic transaction activity.
4. There is an appropriate legal solution, as agreed in the privacy policy, if online consumers violate their privacy rights in the future.

Violations of Privacy Policy in the Online Marketplace System in Indonesia

Regarding the violation of privacy rights experienced by consumers in the online marketplace system, preventive/precautionary steps are needed from consumers to include their private data, including hobbies and tendencies, because when this has been tabulated by the company, then the consumer's own right to privacy is violated. So far, the majority of public complaints reported to the directorate of e-business, Ministry of Communication and Informatics, relate to the incompatibility of the goods ordered with the goods received; for cases related to the right to privacy, there have been no reports of complaints.

CONCLUSION

In order to protect privacy rights so as not to be violated by e-commerce providers or online marketplace system providers, it is possible for legal remedies to be accessed by online consumers regulated by international legal mechanisms.

The mechanism for resolving disputes related to e-commerce (Online Dispute Resolution, ODR) is more specific regarding violations of private data, which is a combination of settlement between IT and alternative dispute resolution. Pablo Cortez stated that the mechanism for resolving disputes related to e-commerce (Online Dispute Resolution, ODR) is more specific regarding the violation of private data, which is a combination of IT and alternative dispute resolution; Pablo Cortez stated that the dispute resolution method could be fulfilled with IT provisions or in this context which is a customer in dispute resolution e-commerce, this includes neutral pointers, identity development processes, listening to oral input from the parties, discussions to binding decisions. ODR tries to synergize between settlements outside the judiciary and approaches that are in accordance with IT rules, and legal remedies are developments that are rife today.

Legal remedies that online consumers can take regarding privacy data violations can be seen from two processes. Namely, the adjudication process (litigation and arbitration) and the consensus process (mediation and negotiation), UNCTAD in the E-Commerce and Development Report 2003 provides an overview of the elements; In addition, related to the law available for victims of a violation of privacy rights following Indonesian legal regulations based on Law Number 18 of 2008 concerning ITE and Government Regulation Number 28 of 2012 regarding PSTE, they can file a civil lawsuit for damages, meaning that the legal mechanism for demanding compensation from online users to e-commerce has only recently become available, a tool for seeking civil compensation is available. Even though this privacy data violation is broad and not limited to purely civil matters, it is necessary to have more specific legal regulations and expand legal remedies for consumers whose privacy rights are violated.

REFERENCES

- APJII. (2018). Penetrasi & Profil Perilaku Pengguna Internet Indonesia. Retrieved from <https://www.apjii.or.id/>
- Cholissodin, I., & Riyandani, E. (2016). *Analisis big data (Teori & Aplikasi)*. Retrieved from https://www.researchgate.net/profile/Imam-Cholissodin/publication/325381687_Buku_Analisis_Big_Data/links/5b0928cfa6fdcc8c25309f9e/Buku-Analisis-Big-Data.pdf
- Ghosh, A. K. (Ed.). (2012). *E-commerce security and privacy* (Vol. 2). Boston, MA: Springer.
- Irmawati, D. (2011). Pemanfaatan e-commerce dalam dunia bisnis. *Jurnal Ilmiah Orasi Bisnis*, 6, 95-112.
- Kemp, S. (2015). *Digital, social mobile worldwide in 2015*. Retrieved from <https://wearesocial.com/us/blog/2015/01/digital-social-mobile-worldwide-2015/>
- Kurbalija, J. (2016). *An introduction to Internet governance*. Geneva, Switzerland: Diplo Foundation.
- Marcella Jr, A. J., & Stucki, C. (2003). *Privacy handbook: Guidelines, exposures, policy implementation, and international issues*. Hoboken, NJ: John Wiley & Sons.
- Niblett, G. B. F. (1992). *Digital information and the privacy problem*. Paris, France: OECD.
- Ramadhan, H. A., & Putri, D. A. (2018). *Big data, kecerdasan buatan, blockchain, dan teknologi finansial di Indonesia*. Retrieved from <https://aptika.kominfo.go.id/wp-content/uploads/2018/12/Kajian-Kominfo-CIPG-compressed.pdf>
- Tim Privacy International., & ELSAM. (2015). *Privasi 101: Panduan memahami privasi, perlindungan data dan surveilans komunikasi*. Jakarta, Indonesia: Lembaga Studi dan Advokasi Masyarakat (Perkumpulan ELSAM).

ETHICAL DECLARATION

Conflict of interest: No declaration required. **Financing:** No reporting required. **Peer review:** Double anonymous peer review.