Privieet Social Sciences Journal

P-ISSN: 2798-866X & E-ISSN: 2798-6314

available at http: www.privietlab.org

Privieet Social Sciences Journal, 2022, 2(2), 11-14

Analysis of E-Commerce data breach and theft

Rodiatun Adawiyah[1], Muhammad Arif Prasetyo[1], Hanuring Ayu[2], Raymond Septiyan[1], Steven Leonardy[1], Michael Calvin[1]

[1]Fakultas Hukum Universitas Prima Indonesia, [2]Universitas Islam Batik
*Corresponding Author: rodiatunadawiah@unprimdn.ac.id

Received: 21 June 2022 **Accepted:** 10 September 2022 **DOI:** https://doi.org/10.55942/pssj.v2i2.168

ABSTRACT
The development in the field of E-commerce is something that is very important for our country today. E-commerce is not only advancing the country in the field of electronics, but this development can also be felt in other fields such as: Economics, and also the field of Education. However, it is not the only benefit that we can feel from these developments. There are things that can be very detrimental to us if we are not careful enough in the development of this E-commerce technology. Oneaofatheamostaimportant thingsato watch outafor is the breach of individual data/identity leakage that can be carried out by irresponsible parties in the E-commerce sector. Even though there are already articles of the ITE Law Article 32 Paragraphs 1, 2, and 3 which regulate the theft of personal data, the crime of theft still occurs in Indonesia. We can see examples of this crime from several similar crime cases, such as: The case of data leakage of 91 million accounts on Tokopedia in May 2020 and the case of data leakage of Cermati and Lazada involving 2.9 million accounts at the end of 2020.

Keywords: E-commerce; Development; Data/Identity leakage; ITE Law

1. INTRODUCTION

Modern technology which is developing more rapidly has led to people's dependence on technology in their daily needs. Especially during the current Covid-19 pandemic, almost everyone carries out activities at home such as: working, studying, and transacting via the internet network. The use of this technology is certainly very beneficial for the community, especially in the fields of economy and education, matters relating to science can be easily accessed so that we can receive important information related to the world of science. Meanwhile, in the world of economy, promotions and advertisements that can improve the welfare of the community can be carried out quickly and without limitations of place or time and can reach both national and international levels of the population. We can see this from how many E-commerce companies have been established in the last few years in Indonesia, such as: Tokopedia, Grab, Gojek, etc.

E-commerce itself can be interpreted as a business activity involving consumers (consumers), manufacturers (manufactures), service providers, and intermediary traders (intermediaries) using a computer network (computer network), namely the internet. However, in connection with the emergence of these E-commerce companies, of course, violations related to E-commerce field are increasingly prevalent in the wider community. Violations that often occur are violations of customer data theft at these E-commerce companies, then the data will be traded on the DarkWeb (Illegal Sites). In general, the stolen data is data regarding the personal identity of these E-commerce customers.

Self-identity in the Big Indonesian Dictionary (KBBI) can be interpreted as special characteristics or a person's identity. In addition, identity can also be interpreted as a very important marker for everyone. So identity theft can be interpreted as an act where a person or group of people uses another person's personal information such as: name, address, telephone number, SIM number or other identity without the consent of the person concerned. Matters relating to the leakage of individual identities, of course, already have special sanctions for violators/ perpetrators, as stipulated in Article 32 of the Indonesian Constitution No. 11 of 2008 concerning Information and Electronic Transactions, according to our analysis, can be interpreted as anyone who steals, adds or changes the data of a person or the public is a crime of data theft.

However, there are still many elements/actors who still commit this E-commerce violation even though many sanctions have been imposed. Therefore, it is very important for the community to know the impacts and consequences that can be generated along with the rapid development of today's technology. In this case, it is not only profits that can be generated but can also bring enormous losses if not addressed immediately. In this study, we will explain various types of violations and thefts of E-commerce data (identity) in Indonesia along with examples of data theft violations that have occurred in Indonesia in recent years.

2. METHODOLOGY

The type of research used in our research is normative research, which means that our research is carried out by examining library materials using existing secondary data. We take a normative approach with the aim of approaching it in terms of the applicable laws and regulations. We do this data collection technique by means of a literature study, namely reviewing and also reviewing articles, journals, legal research results, official state documents such as laws, government regulations, ministerial regulations, and literature related to research problems that we will use as sources. reference. Our case analysis was carried out using qualitative descriptive analysis, namely a collection of data which was then made in a narrative manner and analyzed with the existing problems. The results of the analysis are then presented in the form of a narrative without any manipulation process. So, this type of research is processed to obtain data as it is.

3. RESULT AND DISCUSSION

Appropriate legal sanctions for perpetrators who steal E-commerce customer data in Indonesia.

Misuse of personal data is a criminal act such as theft, fraud, and other criminal acts that meet both objective and subjective elements. If these elements are fulfilled, then administrative sanctions, criminal sanctions and civil witnesses are still not enough to fully review this criminal system because this system is a perfect system. In Indonesia, there have been many acts of data theft that have disturbed citizens, but the most feared mode of crime from this crime is the mode of breaking into the cracking method. Cracking itself is a burglary process by damaging electronic systems. In addition to having destructive properties, cracking can also forcibly hijack someone's personal data or accounts. Which can cause very, very large losses than other data theft modes. Therefore, the above mode can be charged with Article 26 paragraph (1) of Law 19/2016 which reads:

"Every person intentionally and without rights or against the law intercepts or intercepts Electronic Information and/or Electronic Documents in a certain Computer and/or Electronic System belonging to another person."

Because the meaning of personal data above is not enough, I will explain further with the meaning of personal data in Article 84 paragraph (1) of Law 24/2013, namely:

"Personal data of residents containing information about physical or mental disabilities, fingerprints, irises, signatures, and other data elements that constitute a person's disgrace must be kept confidential."

We should know that all personal data of residents must be stored and protected by the state because it is a very important asset for residents. Furthermore, Cracking can also be included in Article 30 paragraph (3) of the ITE Law, which reads:

"Anyone who knowingly and without rights or unlawfully accesses a Computer or Electronic System in any way violates, breaks through, exceeds, or breaks the security system."

Depending on what he did, Cracker in prison for a maximum of 8 years or a fine of Rp. 800 million. And the act of Cracking can also be interpreted as Anyone who intentionally violates the law in any way to change, add, reduce, transmit, damage, remove, transfer, hide electronic information and Electronic Documents belonging to other people / the public in accordance with Article 32 of the ITE Law. Permenkominfo 20/2016 also contains administrative sanctions for anyone who commits a criminal act of data theft. The administrative sanctions are:

a) Written warning
b) Oral Warning
c) Temporary suspension of activities
d) Announcement of sites in the network.

The above violations will be subject to penalties as referred to in Article 48 of the ITE Law as follows:

1) Any person who fulfills the elements as referred to in Article 32 paragraph (1) shall be punished with imprisonment for a maximum of 8 years or a fine of a maximum of Rp. 2 billion.
2) Any person who fulfills the elements as referred to in Article 32 paragraph (2) shall be sentenced to a maximum imprisonment of 9 years or a maximum fine of Rp. 3 billion.
3) Any person who fulfills the elements as referred to in Article 32 paragraph (3) shall be sentenced to a maximum imprisonment of 10 years or a maximum fine of Rp. 5 Billion.

Ways to prevent data theft

In discussing ways to prevent data theft in e-commerce, we need to know that these data thefts can be carried out by perpetrators in various ways from the breadth of today's internet networks. Some of these methods are even unexpected by E-commerce service users, therefore you need extra attention when you use internet access.

Here are some ways to prevent E-commerce data theft for internet users, namely:

i. Installing “Anti-Virus” on the device used to access the Internet

Some cases of e-commerce data theft that we often hear about usually start from the planting of viruses from the perpetrators on our devices which are then carried out to hack or access our devices illegally. Usually the victims of this method tend to ignore or forget to install the "Anti-virus" service which ultimately makes their devices very vulnerable to attacks from the perpetrators of the data theft.

ii. Create a complex password

The next method of prevention is to create a complex password. With this method, we can prevent irresponsible parties from entering/accessing our website and social media which can be used to steal our personal data.

iii. Updating the device software used to access the internet

The method of updating software can be said to be the most powerful method in preventing hacking by parties who want to steal your personal data. It is said that because by updating your software you can increase the level of resistance of your device's system to the highest level so that it is very difficult to be hacked by external devices that do not have the same level.

iv. Stop opening advertisements on the internet

As explained in the 1st method, our devices can be attacked by viruses planted by hackers. Usually, these viruses are very often found in advertisements on the internet that often appear when you open a web page. Therefore, it is very important to avoid these types of ads that keep appearing even after closing the ad.

v. Don't install apps from untrustworthy sources

Hacking through this application is indeed a problem that is most often experienced by someone when downloading an application that comes from an untrusted source because the application is not paid compared to other sources. However, this unpaid application can sometimes lead to the entry of hacker systems that already exist in the application so that it can make it easier for personal data theft to be carried out successfully. Therefore, it is not recommended to download applications from untrusted sources.

Those are some ways to prevent data theft. It looks trivial, but must still be considered in order to reduce the risk of data theft happening to you. You never know when and where your data will be at risk of being stolen by others. Therefore, prevent it before it's too late by using the methods above.

4. CONCLUSIONS

After researching the "Analysis of E-commerce data breaches and theft", it can be concluded that the vulnerability of public (Consumer) data being stolen by irresponsible parties is due to the lack of increased security by the E-commerce service provider quite a lot occurs in Indonesia at this time. this. The existence of laws governing data theft in Indonesia is still very minimal. Examples of laws concerning ITE include: Article 26 paragraph (1) of Law 19/2016, Article 84 paragraph (1) of Law 24/2013, Article 30 paragraph (3) of the ITE Law, etc. Despite the existence of these articles, of course the data security system in Indonesia is still not safe. In fact, the ways/modes of data theft are also developing along with technological developments as a result, it is very difficult for the government to catch up with the system which is very, very far away if it is not immediately reviewed and eradicated as soon as possible. This data theft varies from theft through planting viruses on consumer devices to wiretapping that is completely unknown to this community. And also many people who often underestimate or do not know the risk of data being stolen from them so that people pay less attention to the level of security in E-commerce services and the devices they use. Thus, the public only realized the great risk of this after becoming a victim of the data theft.

REFERENCES

Books

Barkatullah, A.H. (2017). Hukum Transaksi Elektronik. Nusa Media Ujung berung. Bandung. h. 11.

Magdalena, M. (2013). UU ITE : Don’t be the next victim. Gramedia Pustaka Utama. h. 57.

Diantha, I.M.P. (2016). Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum, Prenada Media. h.145.

Rukin. Metodologi Penelitian Kualitatif Edisi Revisi. Jakad Media Publishing. h. 10.

Yudhanto, Y. (2018). Panduan Pintar Virus dan Trojan. Khazanah Intelektual. h. 52.

Sari, I.Y. (2020). Keamanan Data dan Informasi. Yayasan Kita Menulis. h. 117-118.

Sinaga, A.S.R. (2020). Keamanan Komputer. CV Insan Cendekia Mandiri. h. 48.

Journals

Situmeang, S.M.T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. Jurnal Sarjana Hukum Pattimura (Pattimura Bachelor Law Journal), 27(1). doi:10.47268/sasi.v27i1.394.

Online / World Wide Web

Legal Smart Channel (2022). Konsultasi Hukum. Retrieved From https://lsc.bphn.go.id/konsultasiView?id=3329, diakses 25 Juli 2022.

Hukum Online (2019). Langkah hukum terhadap pencurian data pribadi (Identity Theft). Retrieved From https://www.hukumonline.com/klinik/a/langkah-hukum -terhadap- pencurian-data- pribadi- iidentity- theft -i-lt5d904597bfa6e, diakses 27 Juli 2022

Law

- Kitab Undang-Undang Hukum Perdata.
- Undang-Undang Nomor 19 Tahun 2016 tentang ITE.
- Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan.
- Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi.