IP-TECH

BUSINESS LAW SOCIETY
FACULTY OF LAW
UNIVERSITAS INDONESIA

BLS LEGAL NEWS ON COVID-19

Intellectual Property and Technology Division

Legal Protection for Technological Utilization Due To Large-Scale Social Restrictions as an Impact of COVID-19

Allesia Bayu Eureka
(FH UI 2018)

Herdyanto Kenya Putera
(FH UI 2019)

1. Overview

The name COVID-19 has been mentioned frequently ever since December 2019, when the World Health Organization ("WHO")'s office in China first heard the reports of an unknown pneumonia-like virus in Wuhan, a city in Eastern China. The virus is infectious and spreads quickly, that it's spread to many other countries as well now, including Indonesia. To deal with the condition, Indonesia's government decided to implement Large Scale Social Restrictions ("PSBB") as regulated in the Minister of Health Regulation Number 9/2020 on Guidelines to Large-scale Social Restrictions in Accelerating COVID-19 Mitigation. The implementation of PSBB brought many changes to society since people need to stay connected with each other to do their daily activities. In order to keep in touch with others, people became reliant on technology. Meetings now turn into online meetings, learnings are done through Skype, Zoom or similar applications, and buying groceries are even done through online services. Technology has become human's main need in this pandemic Covid-19 and unexpectedly, problems started to show up in cyberspace, such as the increase of data breaches and malicious code threats.

One of the most-heard cases was a data breach that happened in Tokopedia, where allegedly 91 million accounts had their data breached illegally.[1] The massive data leak reportedly consisted of email addresses, password hashes, names of the account users, which are put up for sale on dark webs.[2] This issue can show the vulnerability of data protection in Indonesia and this issue also leads to the loss of reputation which the company has beforehand.[3] Other than that, Zoom is also infamous for having data breaches that happen a lot in their application. Zoom's popularity exploded when the quarantine started and people began using it as a platform for communicating. Companies, schools, universities, and many more use Zoom to do meetings, teachings, and other daily activities. However, security researchers call Zoom a 'privacy disaster' as it's notorious for selling users' data.[4] Other than that, it was found out that over 500.000 Zoom accounts were sold on hacker forums or even given for free.[5] Besides the data breach, Zoom also causes security concerns as it has no end-to-end encryption, which is a method of secure communication that prevents third-parties from accessing data while it's transferred from one end system or device to another.[6] Without this system that protects data, illegal and irresponsible parties may be able to have access to personal information and cause damage.

---

[1] The Jakarta Post News Team, "Stop Data Breaches", https://www.thejakartapost.com/academia/ 2020/05/06/stop-data-breaches.html, accessed on June 22nd, 2020.

[2] Rizki Fachriansyah, "Data Breach Jeopardizes More Than 15 Million Tokopedia Users, Report Finds", https://www.thejakartapost.com/news/2020/05/03/data-breach-jeopardizes-more-than-15-million-to kopedia-users-report-finds.html, accessed on June 22nd, 2020.

[3] Iskandar, "Attacked by the Hackers, Here Are The Effects of Data Breach to Tokopedia's Workers and Customers", https://www.liputan6.com/tekno/read/4244527/tokopedia-diserang-hacker-ini-da mpak-bagi-karyawan-dan-pelanggan, accessed on June 17th, 2020.

[4] Kari Paul, "'Zoom is Malware': Why Experts Worry About The Video Conferencing Platform", https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing, accessed on June 17th, 2020.

[5] Lawrence Abrams, "Over 500,000 Zoom accounts sold on hacker forums, the dark web", https:// www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/, accessed on June 17th, 2020.

[6] Nadeem Unuth, "What is End-to-End Encryption?", https://www.lifewire.com/what-is-end-to-end- encryption-4028873, accessed on June 22nd, 2020.

2. Legal Issues and Responsibilities in Cyberspace

Technology could bring many benefits to the user, but if a user isn't careful enough, they may encounter certain issues instead. Some of the most common issues a person can face when using technology is a data breach or malicious code threats that are often mentioned as "bugs". Malicious codes are harmful because they are designed to create system vulnerabilities that may lead to security breaches, data theft, and other kinds of damages.[7] Regulations about electronic information and transactions became important in order to deal with these problems. In Indonesia, the electronic information and transactions regulations are legislated under the Law No.11/2008 on Electronic Information and Transactions that have been amended with Law No.19/2016 on the Amendment of Law No.11/2008 on Electronic Information and Transactions ("**EIT Law**"). Regulations regarding electronic systems are also regulated in the Government Regulation of the Republic of Indonesia No.71/2019 on Operation of Electronic Systems and Transactions ("**PP PSTE**"). The EIT Law of Indonesia protects rights in technology utilization, such as the protection of personal data when using an electronic system, as provided in Article 26 paragraph (1) of the EIT Law. First, this article obligates electronic system providers to ask their users' permission before using or processing customer's data. This is also regulated in Article 14 of PP PSTE.

Secondly, the EIT Law grants the user the right to use an electronic system safely, reliably, and functioning as it should in accordance with Article 15 paragraph (1) of the EIT Law. It means that the electronic system must function according to the specifications of the electronic system and must ensure no presence of malicious codes in their electronic system that could harm users, and electronic system providers must explain the purpose of every action they do towards the users' data.[8] Electronic system providers are also obligated to keep their electronic system safe and working well, so it may avoid troubles or losses, as regulated in Article 24 of PP PSTE. Another right of a user is also mentioned in Article 29 of PP PSTE, which states that an electronic system provider must provide every important information to its users. The protection of a user's data is also mentioned in Article 59 of Government Regulation of the Republic of Indonesia No. 80/2019 on Tradings using Electronic System ("**PP PMSE**"), which regulates that every business person must protect their user's personal data which is obtained through legal ways and must keep a system to avoid any data breach.

However, the EIT Law regulates several forms of accountability if there are violations of the provisions of the EIT Law. If an electronic system user has suffered damages due to the presence of malicious codes or "bugs" that are present due to the negligence of the provider towards Article 15 paragraph (1) EIT Law, the electronic system provider can be asked for their responsibility for damages that is experienced by the user.[9] In the case of a data breach that leads to the violation of private data, two parties could be held responsible, that is the electronic system provider and the party that caused the data breach. A person who caused the data breach is threatened with imprisonment up to 7 (seven) years and/or must pay a compensation up to Rp 700.000.000,00.[10] Also, the electronic system provider must

---

[7] Kaspersky Team, "What is Malicious Code?", https://www.kaspersky.com/resource-center/definiti ons/malicious-code, accessed on June 23rd, 2020.

[8] Widyawan & Partners, "Data Protected - Indonesia", https://www.linklaters.com/en/insights/data- protected/data-protected---indonesia#rights, accessed on June 22nd, 2020.

[9] Indonesia, Electronic Information and Transaction Law, Law No. 11/2008, LN. No. 58 Tahun 2008, TLN No.4843, Article 46 paragraph (2).

[10] *Ibid*, Article 15 paragraph (2).

issue a written statement to the users that their data has been breached, according to Article 14 paragraph (5) PP PSTE.

Experiencing damages while using an electronic system is not a pleasant event, hence the EIT Law especially in Article 21 paragraph (3) EIT Law, the electronic system provider could be sued in a civil lawsuit by the victims of a data breach. It means, the EIT Law provides mechanisms of damage mitigation by granting a user the ability to ask for damages to an electronic system provider by a civil lawsuit or alternative dispute resolutions like arbitration and mediation.[11] The ability to litigate this issue is further regulated in Article 1365 of the Indonesian Civil Code ("ICC"), which regulates all unlawful actions that cause damages may be requested for compensation. Besides that, if a user no longer uses a certain electronic system or a user wants to remove their data on a certain electronic system as a result of data breach or malicious codes, it is best to request for the termination or removal of their data, which is allowed by Article 59 paragraph (3) PP PSME.

3. Conclusion

In conclusion, COVID-19 has caused a massive change as the enactment of PSBB has caused almost everyone to alter their usual lifestyle and begin using technology for their daily activities. However, when using a technology, a person may encounter losses as the result of data breach or malicious codes, that are usually caused by the negligence of the electronic system provider that failed to uphold the rules of safe, reliable, and functioning it should be in the electronic system. Therefore, to avoid or deal with problems like these, it's best to use applications of which the Electronic System Provider is trustworthy, also when encountering issues like these a user is allowed to sue the electronic system provider in accordance with applicable laws and regulations. Also it's advised to make sure that the site or software opened are the encrypted ones and if a user longer uses an electronic system they could request for the termination of their data. At the same time, the government also takes part in dealing with these issues by enacting regulations related to electronic information and transactions. With a regulation about electronic information and transactions, an individual's rights are hopefully able to be protected and could know the measures to take if they encounter damages when using technology.

[11] *Ibid.*, Article 38 paragraph (3).

REFERENCES AND BIBLIOGRAPHY

I. REGULATIONS

Indonesia. Electronic Information and Transaction Law, Law No. 11/2008, LN. No. 58 Tahun 2008, TLN No.4843.

Indonesia. Operation of Electronic Systems and Transactions. Government Regulation of the Republic of Indonesia No.71/2019.

Indonesia. Trade Through Electronic Systems. Government Regulation of the Republic of Indonesia No.80/2019.

II. INTERNET

Abrams, Lawrence. "Over 500.000 Zoom Accounts Sold on Hacker Forums, The Dark Web". https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-old-on-hacker-forums-the-dark-web/. Accessed on June 17th, 2020.

Bayern, Macy. "35% of Zoom Users Fear Data Leaks Amid The Platform's Security Issues". https://www.techrepublic.com/article/35-of-zoom-users-fear-data-leaks-a mid-theplatforms-security-issues/. Accessed on June 17th, 2020.

Eloksari, Eisya A. "Tokopedia Data Breach Exposes Vulnerability of Personal Data". https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html. Accessed on June 17th, 2020.

Fachriansyah, Rizki. "Data Breach Jeopardizes More Than 15 Million Tokopedia Users, Report Finds". https://www.thejakartapost.com/news/2020/05/03/data-breach-jeopardizes-more-than-15-million-tokopedia-users-report-finds.html. Accessed on June 22nd, 2020.

Iskandar. "Attacked by the Hackers, Here Are The Effects of Data Breach to Tokopedia's Workers and Customers". https://www.liputan6.com/tekno/read/4244527/tokopedia-diserang-hacker-ini-dampak-bagi-karyawan-dan-pelanggan. Accessed on June 17th, 2020.

Kaspersky Team. "What is Malicious Code?" https://www.kaspersky.com/resource-center/definitions/malicious-code. Accessed on June 23rd, 2020.

Krisetya, Beltsazar A. "COVID-19 Exposes Vulnerabilities in Our Cyberspace". https://www.thejakartapost.com/academia/2020/04/01/covid-19-exposes-vulnerabilities-in-our-cyberspace.html. Accessed on June 4th, 2020.

Paul, Kari. "Zoom is Malware': Why Experts Worry About The Video Conferencing Platform". https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing. Accessed on June 17th,2020.

The Jakarta Post News Team. "Stop Data Breaches". https://www.thejakartapost.com/academia/2020/05/06/stop-data-breaches.html. Accessed on June 22nd, 2020.

Unuth, Nadeem. "What is End-to-End Encryption?". https://www.lifewire.com/what-is-end-to-end-encryption-4028873. Accessed on June 22nd, 2020.

Widyawan & Partners. "Data Protected - Indonesia". https://www.linklaters.com/en/insights/data-protected/data-protected---indonesia#rights. Accessed on June 22nd, 2020.