



INNOVATIVE: Journal Of Social Science Research

Volume 3 Nomor 6 Tahun 2023 Page 7768-7777

E-ISSN 2807-4238 and P-ISSN 2807-4246

Website: <https://j-innovative.org/index.php/Innovative>

Data Breach In Indonesia: A Contemporary View

Jauhar Rizqullah Sumirat

University of York

Email: jauharsumirat@gmail.com

Abstrak

Perlindungan data kemudian diperlukan untuk menjamin keamanan data dari hal tersebut, salah satunya adalah pelanggaran data. Pelanggaran data terkait internet pertama terjadi pada tahun 2005 ketika lebih dari 1 juta catatan dari 1,4 juta rekening kartu kredit yang terdaftar di Gudang Sepatu DSW bocor. Kasus pelanggaran data di Indonesia tidak sedikit. Selama dua tahun terakhir, data pribadi masyarakat banyak yang bocor, mulai dari data milik perusahaan e-commerce seperti Lazada dan Tokopedia hingga data milik organisasi pemerintah seperti Badan Kesehatan dan Jaminan Sosial serta Komisi Pemilihan Umum. Pelanggaran Data merupakan kejahatan yang kompleks dan baru terjadi di Indonesia akhir-akhir ini sehingga memprihatinkan. Pemerintah Indonesia pun bersikap reaktif terhadap hal tersebut dan segera mengesahkan Undang-Undang Perlindungan Data Pribadi sebagai landasan hukum perlindungan data di Indonesia. Hal ini merupakan langkah nyata pemerintah dalam menangani kasus pembobolan data di Indonesia. Bersamaan dengan kasus Bjorka yang melakukan pembobolan data di beberapa instansi pemerintah, pemerintah juga membentuk satuan tugas untuk menangani kasus tersebut.

Kata Kunci: *Data, Indonesia, Kontemporer*

Abstract

Data protection is then needed to ensure data security from this, one of which is data breach. The first ever internet-related data breach occurred in 2005 when more than 1 million records of 1.4 million credit card accounts registered with the DSW Shoe Warehouse were leaked. Data breach cases in Indonesia are not small. Over the past two years, people's personal data has been leaked, ranging from data belonging to e-commerce companies such as Lazada and Tokopedia to data belonging to government organizations such as the Healthcare and Social Security Agency and the General Elections Commission. Data Breach is a complex crime, and it only happened in Indonesia recently, which has made it a concern. The Indonesian government also became reactive to this and immediately passed the Personal Data Protection Law as the legal basis for data protection in Indonesia. This is a concrete step by the government to handle data breach cases in Indonesia. Simultaneously with the case of Bjorka who had committed a data breach on several government bodies, the government also formed a task force to handle the case.

Keywords: *Data, Indonesia, Contemporary*

INTRODUCTION

In today's internet era, data security is an important part of ensuring human interests. This is because someone's personal data can be used for malicious purposes by irresponsible parties. Data protection is then needed to ensure data security from this, one of which is data breach. The first ever internet related data breach occurred in 2005 when more than 1 million records of 1.4 million credit card accounts registered with the DSW Shoe Warehouse were leaked. But this problem only received major attention when data owned by Facebook users has been utilized by Cambridge Analytica to analyze the profile of the American population in the 2015 general election. Cambridge Analytica, a company that works for Donald Trump's election team, has used Facebook user data without permission and was used to build predictors for the general election at that time. Not only that, they also use the data obtained to provide personalized political advertisements. This is of course a personal data breach.

Data breach cases in Indonesia are not small. Over the past two years, people's personal data has been leaked, ranging from data belonging to e-commerce companies such as Lazada and Tokopedia to data belonging to government organizations such as the Healthcare and Social Security Agency and the General Elections Commission. The data breach that occurred at the General Elections Commission has especially been in the spotlight and involved a hacker with the alias Bjorka who has leaked 2.3 million population data and threatened to leak 200 million more. Another hacker via his Twitter account

@son1x777 also stated that he had entered the system of the Indonesian National Police to obtain personal data of 28,000 officers. This then shows that not only the general public is vulnerable to data breaches and trade in personal data, but also to law enforcement officials.

RESEARCH METHOD

..

RESULT AND DISCUSSION

Cyber Fraud in Indonesia Nowadays

Legal Frameworks

The legal framework for personal data protection in Indonesia is based on Law Number 27 of 2022 concerning Personal Data Protection and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law). The Personal Data Protection Law is a law recently issued by the government to regulate the definition of personal data, types, ownership rights, processing, exceptions, controllers and processors, transmission, authorized institutions that regulate personal data, and dispute resolution. The parties who are responsible as controllers of personal data are individuals including business people. Issuance of this rule is expected to be able to reduce disclosure of personal data without control which has the potential to cause risks of various criminal acts. Besides that there is Information and Electronic Transactions Law, the first law which became a pioneer that lays the basis for regulation in the field of Information Technology utilization in Indonesia. Therefore, before the publication of the Personal Data Protection Law, this law was used as the legal framework of reference in handling personal data violations such as data breaches.

Institutional Frameworks

Several agencies are involved in handling data breaches in Indonesia, mainly the agencies under the Criminal Justice System. Among them, the Indonesian National Police (INP) has an important role in investigating cases of personal data breaches in this country. Based on the Criminal Procedure Code in force in this country, the investigator's task is to find and collect evidence with this evidence to shed light on the crime that occurred and find the suspect. More than that, INP investigators are guided by the Circular of the Chief of Police Number SE/2/11/2021 which is a derivative rule from the Information and Electronic Transactions Law in conducting investigations into cybercrimes.

Analysis

Best Practices in Indonesian Countermeasures to Data Breach Issues

Legal Approach

Indonesia has just issued a new law in dealing with data breach issues, namely the Personal Data Protection Law. This law comes into effect on 20 September 2022 with the aim of protecting public personal data managed by electronic system operators and preventing misuse of this data by irresponsible parties. This law is seen as a sign of a new era of governance of people's personal data, especially in digital matters. The existence of this law has become the legal basis for the protection of the personal data of the Indonesian people with the prohibition to disseminate specific data and general data and if this is distributed without permission there will be legal consequences.

In addition, there is also the ITE Law which is the legal basis for carrying out investigations into cybercrimes including data breaches. Article 43 paragraph 1 of the ITE Law states that Investigating Police have the duty and responsibility to carry out cybercrime investigations, which are carried out with due regard to protection of privacy, confidentiality, smooth running of public services, and data integrity or integrity in accordance with statutory provisions. Based on these provisions, Police Investigators can make efforts related to the investigation of data breach criminal acts including searches, examinations, confiscations, and so on. Therefore the existence of the ITE Law has become the legal basis for carrying out data breach investigations.

Institutional Approach

Based on statutory provisions, the Criminal Justice System is responsible for resolving legal issues, including handling personal data breaches. The police as part of CJS have the same responsibility in law enforcement, especially in carrying out investigations. The Indonesian police themselves already have a special unit to handle cybercrimes, namely through the Directorate of Cyber Crime. This unit works under INP's criminal investigation to handle computer crime and computer-related crime, including data breach and data theft. The Directorate of Cyber Crime is equipped with a digital forensic laboratory that has assisted in examining digital evidence at various levels and police work units throughout Indonesia. This unit has also collaborated with various agencies, both domestic and foreign, to facilitate coordination in disclosing transnational and organized cybercrimes. This then shows that the INP has sufficient capability in handling personal data breach.

Case Studies

The data breach case that was committed by a hacker who calls himself Bjorka has become a hot topic of conversation in Indonesian society. It boasts that it has successfully made access to several government accounts and data. This then received the attention of the people of Indonesia which then gave rise to the notion of the government's inability to provide robust data protection policies even in the government sector. Following the law violations committed, the Indonesian government then formed a data protection task force consisting of several agencies including the INP, National Cyber and Encryption Agency and several ministries to handle cases. The task force then attempted to carry out an investigation and try to identify Bjorka and his actual location. As a result, the Police have conducted interrogation of a man who resides in Madiun regency, East Java, who is suspected of having assisted Bjorka in creating a Telegram channel. They use these leads to carry out further investigations in this case. But then Bjorka, who claims to be from Poland, will introduce new complications to the INP investigation. At one point when it is proven that Bjorka is not an Indonesian citizen, a jurisdictional problem will arise. This case will be a transnational case whose resolution will depend on cooperation between countries.

Future Challenges

Legal Challenges

The Personal Data Protection Bill, which had been submitted since 2016, was soon formalized as an aftermath of the Bjorka case. After the enactment of this law, if someone is proven to have malicious intent in mishandling data, they can be jailed for up to six years. The preparation of the PDP Law is based on the reason to provide protection to personal data holders in managing personal data. This places individuals, legal and non-legal entities, public bodies, and/or organizations/institutions as the parties responsible for managing personal data, including when a breach occurs. Processing of personal data according to the PDP Law must be carried out based on the consent of the data owner. Data owners are granted certain rights, but this does not apply to aggregate data that is processed for specific purposes such as statistics and scientific research within the context of state administration.

The Indonesian PDP Law adopts the General Data Protection Regulation (EU GDPR) as a standard in regulating personal data protection. Similarities can be seen in the definition of personal data, the rights of data subjects, as well as the responsibilities of data controllers and processors. However, these laws are not identical and there are several differences between the PDP Law and the EU GDPR which then presents weaknesses in the PDP Law as

the legal basis for data protection in Indonesia. Some GDPR concepts and instruments are not included in the PDP Law, such as the authority responsible for data protection and data portability. The PDP Law also points out several shortcomings with its non-detailed and unclear rules regarding the rights of data subjects and the responsibilities that must be met by data controllers and processors. This then allows for reduced effectiveness of the legislation in providing oversight, law enforcement and data protection policies in Indonesia as a whole.

In addition, in the event that there is a leak of personal data, there is an obligation for the victim to immediately report the chronology of events to the authorities. This is done in writing with a minimum reporting time of 3x24 hours after the incident. This is the only way for victims to get help from the police. But then what if the person fails to report data theft or doesn't realize that someone else's personal data has been used? Is it not possible for him to get the same protection? This then shows another weakness of the recently passed PDP Law, which places victims in the position of having to report with a certain time limit.

Based on this, it appears that although the government has enacted several laws as the basis for dealing with personal data breaches and cybercrimes in general, existing laws are still seen as ineffective. Legal and cybercrime experts in Indonesia also view that the PDP Law still fails to properly define the classification of personal data. Without a precise definition, efforts to determine punitive sanctions in cases of data security violations will also be inappropriate. It also prevents proper countermeasures from being designed.

Institutional Challenges

In addition to the legal issues as explained above, there are quite complex institutional problems in Indonesia. This is because there are various institutions that are responsible for handling cyber cases. As happened in the case study in the previous section, to deal with a single hacker, the government must employ several institutions and form a new task force to be able to investigate cases and perpetrators. This is due to Indonesia's cyber infrastructure arrangements delegating responsibility and coordinating cyber security capacities to multiple agencies, instead of creating a centralized organization that handles the country's overall cyber issues.

The state has a National Cyber and Encryption Agency (BSSN) which is authorized to formulate an Indonesian Cyber Security Strategy as a common reference for all national cyber security stakeholders in formulating and developing cyber security policies in their respective agencies. Meanwhile, regulation of financial data such as banking data, protection of consumer financial data, and supervision of consumer data is carried out by

the Financial Services Authority (OJK). INP in this case serves as an investigator in cyber cases including the occurrence of data breaches. The existence of these various institutions will enable each institution to build its internal capabilities based on the needs and availability of resources of each institution. However, this has the potential to undermine the central government's ability to efficiently coordinate a rapid response to cyber threats.

Other weaknesses can also arise from within each institution itself. The INP, which serves as an investigator in tackling data theft, still has its drawbacks. The INP has not been able to carry out its duties optimally as a result of limited personnel capabilities. Research shows that INP investigators still have difficulties in investigating cybercrime cases due to a lack of computer knowledge; limited knowledge and technical experience in investigating cyber cases; and the difficulty of finding evidence. Particularly with regard to the search for evidence, evidence of cyber-crimes committed on the internet can easily be changed, deleted or hidden by perpetrators. Perpetrators can also carry out their actions anonymously which further complicates the investigation conducted by the police. In addition to difficulties based on such technical factors, there has been significant delay in disseminating the recently passed law. Inadequate socialization of the law causes the police to be ignorant of the laws that are currently in force.

CONCLUSION

Data Breach is a complex crime, and it only happened in Indonesia recently, which has made it a concern. The Indonesian government also became reactive to this and immediately passed the Personal Data Protection Law as the legal basis for data protection in Indonesia. This is a concrete step by the government to handle data breach cases in Indonesia. Simultaneously with the case of Bjorka who had committed a data breach on several government bodies, the government also formed a task force to handle the case. The INP is a part of the task force whose job is to investigate cases. Despite facing some significant challenges, INP continues to develop capacity to tackle these crimes.

REFERENCES

- Aisyah Llewellyn. Bjorka, the Online Hacker Trying To Take Down the Indonesian Government. <https://thedi diplomat.com/2022/09/bjorka-the-online-hacker-trying-to-take-down-the-indonesian-government/> Accessed 17 March 2023
- Bawono, Bambang Tri. "Reformation of Law Enforcement of Cyber Crime in Indonesia."

- Jurnal Pembaharuan Hukum 6.3 (2019).
- Brilliannata, Jonathan, Rofikotul Jamiilah, and Haidar Talib. "Protection of Personal Data Information in Indonesia." *LEGAL BRIEF* 11.4 (2022): 2263-2267.
- Carole Cadwalladr and Emma Graham-Harrison. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. (2018). <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> Accessed 17 March 2023
- Cory Warren. A Brief History of Data Breaches. (2018) <https://lifelock.norton.com/learn/data-breaches/history-of-data-breaches#:~:text=What%20was%20the%20first%20data,and%20names%20on%20those%20accounts>). Accessed 17 March 2023
- Indonesia National Police. Direktorat Tindak Pidana Siber Bareskrim Polri. <https://patrolisiber.id/about> Accessed 17 March 2023
- Kate Lamb. Indonesia probe police hack in latest cyber breach. (2021). <https://www.reuters.com/world/asia-pacific/indonesia-probe-police-hack-latest-cyber-breach-2021-11-19/> Accessed 17 March 2023
- Laila Afifa. 6 Major Data Breach Cases in Indonesia in Past 1.5 Years. (2021). <https://en.tempo.co/read/1700688/tokopedia-helps-women-owned-msmes-to-obtain-nib> Accessed 17 March 2023
- Rosadi, Sinta Dewi, et al. "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?." *International Review of Law, Computers & Technology* (2022): 1-13.
- Sinulingga, D. A. (2022). Legal Certainty of Aggregate Data Utilization in The Design o Personal Data Protection Bill. *Jambura Law Review*, 4(1), 18-37.
- Cory Warren. A Brief History of Data Breaches. (2018) <https://lifelock.norton.com/learn/data-breaches/history-of-data-breaches#:~:text=What%20was%20the%20first%20data,and%20names%20on%20those%20accounts>). Accessed 17 March 2023
- Carole Cadwalladr and Emma Graham-Harrison. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. (2018). <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> Accessed 17 March 2023
- Laila Afifa. 6 Major Data Breach Cases in Indonesia in Past 1.5 Years. (2021). <https://en.tempo.co/read/1700688/tokopedia-helps-women-owned-msmes-to->

obtain-nib Accessed 17 March 2023

Kate Lamb. Indonesia probe police hack in latest cyber breach. (2021).

<https://www.reuters.com/world/asia-pacific/indonesia-probe-police-hack-latest-cyber-breach-2021-11-19/> Accessed 17 March 2023

Indonesia National Police. Direktorat Tindak Pidana Siber Bareskrim Polri.

<https://patrolisiber.id/about> Accessed 17 March 2023

Sinulingga, D. A. (2022). Legal Certainty of Aggregate Data Utilization in The Design of Personal Data Protection Bill. *Jambura Law Review*, 4(1), 18-37.

Rosadi, Sinta Dewi, et al. "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?." *International Review of Law, Computers & Technology* (2022): 1-13.

Brilliannata, Jonathan, Rofikotul Jamiilah, and Haidar Talib. "Protection of Personal Data Information in Indonesia." *LEGAL BRIEF* 11.4 (2022): 2263-2267.

Bawono, Bambang Tri. "Reformation of Law Enforcement of Cyber Crime in Indonesia." *Jurnal Pembaharuan Hukum* 6.3 (2019).