SOCIAL SCIENCES INSIGHTS JOURNAL
https://journal.midpublisher.com/index.php/ssij

The Urgency of Increasing National Cyber Security as an Effort to Protect Personal Data

Febriansyah
Fakultas Hukum Universitas Pancasila
5222220026@univpancasila.ac.id

ARTICLE INFO

Received: December 2023
Accepted: December 2023
Published: December 2023

Keywords:
Cybercrime, Cyber Security, Data Protection, Law

ABSTRACT

One form of Cybercrime is social media hacking and piracy which leads to personal data breaches. One of the cases that went viral in 2022 was that carried out by Bjorka. Bjorka once claimed to have 26 million browsing histories of Indihome customers, even confidential state documents. This can happen of course because of weak cyber security in Indonesia. This research aims to determine the legal construction of resolving hacking cases against personal data according to Indonesian laws and regulations, and how the government should make efforts to improve national cyber security. The research method used is normative juridical. The research results show that the ITE Law provides regulations that are still too general regarding the criminal act of hacking personal data. After the Personal Data Protection Law was introduced, Indonesia now has special regulations for this. However, to improve national cyber security, Indonesia must be more involved in international conventions regarding cybercrime.

INTRODUCTION

The rapid development of technology has had a significant positive impact, especially in thecurrent era of globalization. One of the positive impacts is that it makes it easier and faster for the wider community to obtain and provide information. In fact, at the same time, people can find out what events are happening elsewhere. Not only that, with just a smartphone in hand, we can bring pizza, masseurs, taxis or goods from online stores in just a few minutes.

According to the results of a survey conducted by the Alvara Research Center, in 2022, 20.4% of the millennial generation will become addicted internet users. Of that number, 13.7% use the internet for 7-10 hours a day, 3% for 11-13 hours a day, and 3.7% for more than 13 hours a day (Dataindonesia.id, 2022). Digital actions determine its existence, such as: uploading, chatting, posting, and so on.

Apart from the positive impacts as mentioned above, this rapid technological development also has negative impacts. One of them is that new crimes arise along with improvements in information technology, namely Cyber2crime. Cyber3crime can be translated as illegal activities carried out using computers via the internet network (Lilik Muladi, 2009).

Cybercrime is closely related to cyber space. Cyberspace, also called cyberspace, is a communication medium on a computer that is carried out using the internet. Cyberspace is a social space that is not limited by distance and time. Abuse

that occurs in cyberspace is then referred to as cybercrime (Maskun, 2013). One form of Cybercrime is social media hacking and piracy which leads to breaches of personal data. In fact, this personal data is then bought and sold via the dark web for up to US$ 1,500 (Albert Lodewyk Sentosa Siahaan, 2022). One case of personal data leakage that went viral was that carried out by Bjorka.

The case of black hat hacker (Qorry Aina Fitroh, Bambang Sugiantoro, 2023) Bjorka shocked the public in 2022. How could it not be, Bjorka once claimed to have 26 million browsing histories of Indihome customers, 1.3 billion SIM card registration data, and 105 million KPU data. Through his Telegram group, Bjorka distributed the personal data of a number of public officials such as the Minister of Communications and Information, Johnny Plate. This information contains NIK, Family Card number, address, telephone number, names of family members, and Vaccine ID. Bjorka also opened a number of letters addressed to President Joko Widodo. One of them is a letter from the State Intelligence Agency (CNBN Indonesia, 2022). This can happen of course because of weak cyber security in Indonesia.

Based on the description above, this article will examine further the 2 (two) main issues, namely: *First*, what is the legal construction for resolving hacking cases of personal data according to laws and regulations in Indonesia? *Second*, what should the government's efforts be to improve national cyber security?

METHOD

Legal science has a unique character, namely in terms of its normative, practical and prescriptive nature. Departing from this, in this article, in order to answer the problem formulation above, the author uses a type of normative legal research (normative juridical), namely legal research that places law as a system of norms. The norm system in question is about principles, norms, rules, laws and regulations, and court decisions (Mukti Fajar & Yulianto Achmad, 2010). The focus of this research will be on matters related to legal systematics, namely identifying the main meanings in law, including legal subjects, legal acts, legal events in relation to the application of legal theory, legal doctrine and statutory regulations. One of the uses is a statutory approach. The data collection method used by the author uses the library research (Kornelius Benuf and Muhamad Azhar, 2020).

RESULTS AND DISCUSSION

1. Legal Construction in Resolving Hacking Cases of Personal Data According to the ITE Law and PDP Law

Talking about legal construction related to case resolution means it concerns a set of rules that can be used in law enforcement efforts. Law enforcement is a process of realizing legal desires into reality. The legal desires here are nothing other than the thoughts of the law-making body which are formulated in legal regulations (Satjipto Raharjo, 2009). I can describe the relevant legal regulations related to the case being discussed as follows:

In Chapter VII of the ITE Law, starting from Article 27 to Article 37, it regulates prohibited acts. However, if you look at all the prohibited rules in that chapter, there

is not a single word or phrase that explicitly regulates Personal Data. In the ITE Law, provisions that specifically use the phrase 'Personal Data' are only found in the provisions of Article 26 paragraph (1). However, if you look at the subsequent regulations in the ITE Law, there is not a single article or paragraph that contains criminal threats for actions as intended in Article 26 paragraph (1). On the other hand, the provisions of Article 26 paragraph (2) of the ITE Law give every person who is disadvantaged by the use of personal data without permission the right to file a lawsuit. In other words, the use of other people's personal data without permission, according to Article 26 paragraph (1) of the ITE Law, is included in the civil domain (Febriansyah, 2023). Next we will discuss hacking.

Hacker is a popular term in the world of data hacking, but there is another term that is quite popular in the world of hacking, namely Cracker. Even though they seem the same, they both have differences in terms of how they work and their goals. The way hackers work is to look for company security gaps and fix them to make them tighter or safer. Meanwhile, the way crackers work is by looking for security gaps in a network, then destroying and stealing the data (Kementerian Keuangan, 2021). Apart from that, both of them are carrying out legal actions using computers, computer networks and/or electronic media. Therefore, these actions are included in the scope of Electronic Transactions as regulated in the ITE Law. In relation to the regulations in the ITE Law, what differentiates the two is that a cracker carries out the legal action in question in a way that is 'without rights or against the law'

In the ITE Law there are several relevant legal rules to be applied for law enforcement against Cracker actions, including:

Article 30

(1) *Every person intentionally and without right or against the law accesses another person's computer and/or electronic system in any way.*

(2) *Any Person intentionally and without right or against the law accesses a computer and/or Electronic System in any way with the aim of obtaining Electronic Information and/or Electronic Documents.*

(3) *Every person intentionally and without authority or unlawfully accesses a computer and/or electronic system in any way by violating, breaching, surpassing or breaching the security system.*

Article 32

(1) *Every person intentionally and without right or against the law in any way changes, adds, reduces, transmits, damages, deletes, moves, hides electronic information and/or electronic documents belonging to other people or public property.*

(2) *Every person intentionally and without right or against the law in any way transfers or transmits electronic information and/or electronic documents to another person's electronic system without the right.*

(3) Against actions as intended in paragraph (1) which result in the disclosure of confidential Electronic Information and/or Electronic Documents being accessible to the public with data integrity that is not as it should be

Sanctions for violating the provisions above are regulated in Articles 46 and 48 of the ITE Law.

Furthermore, in relation to Personal Data, the ITE Law only mentions objects in the form of Electronic Information (EI) and/or Electronic Documents (ED). If you look at the broad meaning of EI and ED as specified in Article 1 number 1 and number 4 of the ITE Law, it is known that EI and ED are objects that can be displayed via a computer or electronic system, including but not limited to writing, drawings, maps, plans, photos, letters, signs, numbers, Access Codes and so on. Based on this, in an electronic system, a person's personal data will appear in the form of EI and/or ED.

In line with what I explained above, on September 29 2021, the Constitutional Court (MK) decided regarding the constitutionality of Article 32 of the ITE Law, in one part of its considerations, the MK stated (Mahkamah Konstitusi, 2021) :

> *"...according to the Court, the existence of Article 32 and Article 48 of the ITE Law is very important to guarantee the security of personal data, as well as ensuring that transactions or exchange of electronic information run smoothly without harming any user. Guarantees of the security of personal data as well as guarantees of valid and honest exchange of information are preconditions for the fulfillment of the constitutional rights of the Petitioners and all citizens;"*

Finally, Article 32 in conjunction with Article 51 paragraph (2) of the ITE Law provides for the threat of heavier sanctions for the above actions if they are proven to be detrimental to other parties, namely with a maximum imprisonment of 12 (twelve) years and/or a maximum fine of IDR 12,000,000,000. 00 (twelve billion rupiah).

After the enactment of the PDP Law, the government also provides protection for IE and/or DE which concerns a person's personal data contained in an electronic system and/or electronic media where the acquisition, collection, disclosure, and/or use must be carried out legally and not causing harm to other people as personal data subjects.

The PDP Law is currently the basis for legal certainty for Personal Data Owners. In this regard, the PDP Law provides regulations regarding the management of prohibited personal data, which include (Rahmadi Indra Tektona & Fendi Setyawan, 2023):

a) Article 65 paragraph (1) contains the prohibition on obtaining or collecting personal data that does not belong to you with the intention of benefiting yourself or another person which could result in loss to the personal data subject.

b) Article 65 paragraph (2) contains a prohibition on disclosing personal data that does not belong to you with the intention of benefiting yourself or another person which could result in harm to the personal data subject.

Article 65 paragraph (3) contains a prohibition on using personal data that does not belong to you with the intention of benefiting yourself or another person which could result in loss to the personal data subject.

2. Hacker Threats and the Urgency of Improving National Cyber Security

Based on the latest E-Governance Academy (EGA) report in April 2023, Indonesia has a national cyber security index value of 63.64 which is ranked 49th. This is far below the national cyber security index value of neighboring country, Malaysia which is in 22nd position with index values 79.22 and 71.43 (E-Governance Academy, 2023). This index value shows that Indonesia's cyber security is still relatively weak, therefore its security can be penetrated by hackers quite easily. This is proven by the many cyber attacks that occurred in Indonesia, one of which was carried out by Bjorka.

One important indicator that influences the value of the cyber security index is how the country protects the personal data of its people. In 2020, before Indonesia had the Personal Data Protection Law, Indonesia was ranked 84th with a Personal data protection authority score of 0/3 (zero out of three). Currently it has increased to 3/3 (three out of three). This is because through the PDP Law the government intends to establish an independent institution which has the function of protecting personal data (Article 58 of the PDP Law).

However, in order to improve cyber security, it is necessary to study in Belgium, which is a country with cyber security ranking 1 (one) in the world. Based on data obtained from NSCI, I will try to compare the achievements between Indonesia and Belgium regarding cyber security efforts based on several indicators used, including the following:

Table 1. Comparison of cyber security between Indonesia and Belgium, 2023.

Cyber Security Indicators	**Indonesia (Rank 59th)**	**Belgium (Rank 1st)**
	Score	**Score**
Cyber security policy development	3/7	6/7
Cyber threat analysis and information	2/5	5/5
Education and professional development	6/9	9/9
Contribution to global cyber security	1/6	6/6
Protection of digital services	1/5	5/5

Source: E-Governance Academy, 2023 (edited)

The table above shows that there are quite significant differences in the 'contribution to global cyber security' indicator. One of the sub-indicators at this point is the Convention on Cybercrime. Based on this, Indonesia must begin to be actively involved in various international conventions regarding cybercrime. Cyberspace is a space that has no national borders, so the perpetrators of the crime

are certainly not only from Indonesia. Therefore, in facing the threat of cyber attacks which can result in the leakage of personal data, even in a more "sophisticated" way than Bjorka, Indonesia really needs actualization regarding cyber developments in the global arena, which in the end is "too late" in dealing with various cases. what happened in the realm of telematics law, does not happen anymore.

Apart from that, the gap between Indonesia and Belgium is also found in the Protection of digital services indicator. In the first paragraph, it was stated that Bjorka had "mastered" 26 million Indihome customers' browsing history and 1.3 billion SIM card registration data. This shows the weakness of the data protection system for digital services. Information security is something that is very important and needs to be maintained, especially for companies that provide or use IT services to their consumers. Therefore, it is very necessary to have information security standards for all digital service providers, which can protect their consumers from black hat hacker attacks. Finally, public understanding regarding the importance of protecting personal data also needs to be increased and they need to be more alert to activities on the internet. According to the United States Department of Justice, one of the causes that often occurs in cases of personal data theft is precisely the negligence of the victims who easily believe e-mail spam that offers various benefits by asking for the personal data of potential victims (The United States Department of Justice, 2023).

As stated in the Case Position Analysis section, Cyberspace is a space that has no national borders, so the perpetrators of the crime are certainly not only from Indonesia. This is certainly a serious problem in law enforcement.

In relation to Jurisdiction, basically according to Article 2 of the ITE Law, the expansion of jurisdiction has been determined, namely wherever the act is carried out, as long as... it has legal consequences in the Indonesian jurisdiction. In full, Article 2 of the ITE Law reads as follows:

> *"This Law applies to every person who commits legal acts as regulated in this Law, whether within the jurisdiction of Indonesia or outside the jurisdiction of Indonesia, which have legal consequences in the jurisdiction of Indonesia and/or outside the jurisdiction of Indonesia. Indonesia and is detrimental to Indonesia's interests"*

Even though the jurisdiction has been expanded, if the law enforcement process regarding this matter goes beyond national borders, it will certainly be very difficult. Therefore, in my opinion, national legal regulations alone will not be enough to overcome this crime phenomenon. As a suggestion, Indonesia must actively encourage the creation of an International Agreement regarding the handling and enforcement of Cybercrime law, especially regarding the protection of personal data of the Indonesian people. This is also to improve Indonesia's cyber security, one of the indicators of which is Contribution to global cyber security, especially in the sub-Convention on Cybercrime.

CONCLUSION

Legal construction is closely related to law enforcement efforts. In Chapter VII of the ITE Law, prohibited acts are regulated, but there is not a single word or phrase that explicitly regulates Personal Data. In the ITE Law, provisions that specifically use the phrase 'Personal Data' are only found in the provisions of Article 26 paragraph (1). However, according to Article 26 paragraph (1) of the ITE Law, the Law is included in the civil domain. Based on the ITE Law, hackers who unlawfully 'steal' other people's Personal Data through electronic systems can be punished using the provisions of Article 30 and Article 32 of the ITE Law. After the enactment of the PDP Law, the government also provides protection for IE and/or DE which concerns a person's personal data. In the PDP Law, regulations related to the management of personal data that are prohibited include Article 65 paragraph (1), Article 65 paragraph (2), and Article 65 paragraph (3).

Based on the latest report by the E-Governance Academy (EGA) in April 2023, Indonesia's cyber security is ranked 49th. One important indicator that also influences the value of the cyber security index is how the country protects the personal data of its people. In order to improve cyber security, it is necessary to study in Belgium, which is a country with cyber security ranking 1 (one) in the world. The difference is quite significant in the 'contribution to global cyber security' indicator. One of the sub-indicators at this point is the Convention on Cybercrime. Based on this, Indonesia must begin to be actively involved in various international conventions regarding cybercrime. The gap between Indonesia and Belgium is also found in the Protection of digital services indicator. Bjorka has "mastered" 26 million Indihome customers' browsing history, and 1.3 billion SIM card registration data. This shows the weakness of the data protection system for digital services. Therefore, in my opinion, national legal regulations alone will not be enough to overcome this crime phenomenon. As a suggestion, Indonesia must actively encourage the creation of an international agreement regarding the handling and enforcement of cybercrime law, especially regarding the protection of personal data of the Indonesian people.

REFERENCES

Albert Lodewyk Sentosa Siahaan, Urgensi Perlindungan Data Pribadi Di Platform Marketplace Terhadap Kemajuan Teknologi, Jurnal Majalah Hukum Nasional, Vol. 52 No. 2, 2022, hlm 215-216

CNBN Indonesia, *Hacker Bjorka Tantang Pemerintah RI: Saya Menunggu Digerebek*!, https://www.cnbcindonesia.com/tech/20221226135118-37-400166/hacker-bjorka-tantang-pemerintah-ri-saya-menunggu-digerebek

Data Indonesia.ID, Survei: Generasi Z Indonesia Paling Gandrung Gunakan Internet, https://dataindonesia.id/internet/detail/survei-generasi-z-indonesia-paling-gandrung-gunakan-internet.

E-Governance Academy, *National Cyber Security Index (NCSI)*, https://ncsi.ega.ee/ncsi-index/, (diakses 28 Oktober 2023)

Febriansyah, *Financial Identity Theft* : Dari Tindak Pidana Informasi Elektronik Ke Kejahatan Data Pribadi, Jurnal Hukum Samudera Keadilan Volume 18 No 2 (2023), hlm 365

Kemenenterian Keuangan republic Indonesia, Perbedaan hacker dan Craker, https://www.djkn.kemenkeu.go.id/kanwil-rsk/baca-artikel/15422/Perbedaan-Hacker-dan Cracker.html#:~:text=Cara%20kerja%20hacker%20yakni%20mencari,bidang%20emrograman%20dan%20sistem%20operasi

Kornelius Benuf & Muhamad Azhar. (2020). Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Gema Keadilan,* 7(1), 20–33

Lilik Muladi, *Seraut Wajah Putusan Hakim: Studi Kasus Prita Mulyasari*, (Jakarta : Rineka Cipta, 2009), hlm. 40.

Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar*, (Jakarta: Kencana, 2013), hlm. 46.

Mukti Fajar ND dan Yulianto Achmad, *Dualisme Penelitian Hukum Normatif dan Penelitian Hukum Empiris*, (Yogyakarta: Pustaka Pelajar, 2010), 34

Putusan Nomor 17/PUU-XIX/2021, mengenai pengujian konstitusionalitas Pasal 32 UU ITE

Qorry Aina Fitroh, Bambang Sugiantoro, "Peran Ethical Hacking dalam Memerangi Cyberthreats", Jurnal Ilmiah Informatika vol 11, no 1 (2023), hlm 27. https://doi.org/10.33884/jif.v11i01.6593

Rahmadi Indra Tektona, Fendi Setyawan, dkk, *Kepastian Hukum Pemilik Data Pribadi Dalam Aplikasi Satu Sehat*, Jurnal Legislasi Indonesia, Vol. 20 No. 1, 2023, hlm 34-35

Satjipto Raharjo. *Penegakan Hukum Sebagai Tinjauan Sosiologis*. Genta Publishing. Yogyakarta. 2009. Hal 25

The United States Department of Justice, **What** *Are Identity Theft and Identity Fraud?*, https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud, (diakses 29 Oktober 2023)