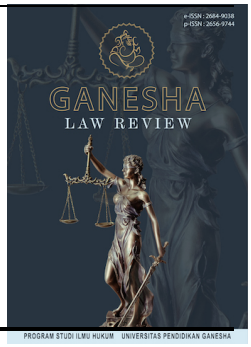
GANESHA LAW REVIEW

Volume 3 Issue 1, May 2021
P-ISSN: 2656 – 9744 , E-ISSN: 2684 – 9038
Open Access at : https://ejournal2.undiksha.ac.id/index.php/GLR
Program Studi Ilmu Hukum
Fakultas Hukum dan Ilmu Sosial
Universitas Pendidikan Ganesha Singaraja



FACEBOOK LEAKS: HOW DOES INDONESIAN LAW REGULATE IT?

Ridwan Arifin[1], Taza Ratna Atika[2]

[1]Faculty of Law, Universitas Negeri Semarang, Indonesia
Department of Criminal Law,
[2]Faculty of Law, Universitas Negeri Semarang, Indonesia
Researcher at Security and Privacy Data Protection

Info Artikel

Masuk: 3 Januari 2021
Diterima: 21 February 2021
Terbit: 2 May 2021

Keywords:
Personal data, Cyber crime, Facebook, Leaks.

Abstract

Along with the development in the world of technology, especially in the internet sector, which has provided so many benefits and advantages and conveniences for many people, in addition to these advantages there are also developments in negative aspects, the existence of risks, and the negative impact of its misuse by parties who not responsible. Some time ago the Indonesian people were quite troubled by the emergence of cases of leakage of personal data of Facebook users. The personal data leakage scandal of Facebook users that has been broken into by the analytical research firm Cambridge Analytica is targeting the entire world population, one of which is Indonesia. Many people are wondering who is to blame and responsible for this case. What is the cause of this case and can it be prevented.

Kata kunci:
Data pribadi, Kejahatan dunia maya, Facebook, Kebocoran.

Abstrak

Seiring dengan perkembangan dunia teknologi khususnya di bidang internet yang telah memberikan banyak sekali manfaat dan keuntungan serta kemudahan bagi banyak orang, selain kelebihan tersebut juga terdapat perkembangan aspek negatif, adanya resiko, dan dampak negatif penyalahgunaannya oleh pihak-pihak yang tidak bertanggung jawab. Beberapa waktu lalu masyarakat Indonesia cukup direpotkan

Corresponding Author:
Ridwan Arifin, E-mail : ridwan.arifin@mail.unnes.ac.id

DOI:
xxxxxxx

dengan munculnya kasus kebocoran data pribadi pengguna Facebook. Skandal kebocoran data pribadi pengguna Facebook yang dibobol oleh firma riset analitik Cambridge Analytica menyasar seluruh penduduk dunia, salah satunya Indonesia. Banyak orang yang bertanya-tanya siapa yang harus disalahkan dan bertanggung jawab atas kasus ini. Apa penyebab kasus ini dan apakah bisa dicegah.

I. INTRODUCTION

Facebook or what is commonly known as FB is a social network website (website) that can connect people globally around the world, where users can connect and interact with each other, join communities like friends. , school, work, city and region, as well as getting to know new people by adding their friends. In addition, Facebook users can also send messages, post photos, and update their personal profiles so that other people can see and find out about themselves.

Facebook was founded by Mark Zuckerberg, a Harvard University graduate, Facebook was launched for the first time on February 4, 2004. Initially, Facebook was only used for Harvard College students, then Facebook was developed and expanded its membership to other schools in the Boston area such as Boston University, Stanford university, and all schools included in the Ivy League.

In its current development, Facebook can be used by global communities around the world from all walks of life, including Indonesians. Among the Indonesian people the use of Facebook is very familiar. With Facebook, it is very helpful and profitable in the field of communication, especially for those who have distant family, relatives, friends and colleagues. However, besides the positive impact it has, Facebook also has a negative impact when it is misused, one example of the recent misuse of advances in technology and the internet is a cyber crime related to the scandal of leaking personal data of users. Facebook. Not less than 87,000.

*Cambridge Analityca*This is a political consulting firm used by Donald Trump in his campaign in the US presidential election in 2016 (US Presidential Election 2016). Although Cambridge Analityca actually targeted American Facebook users for Donald Trump's victory, in fact Facebook users from Indonesia were also victims of the leakage of personal data on their Facebook accounts that had been hacked and stolen by the analytical research firm. According to data shared by the Facebook Newsroom, Indonesia has recorded 1,096,666 (one million ninety-six thousand six hundred and sixty-six) or about 1.26% (one point twenty six percent) of the total amount of personal data from Facebook users from around the world that was leaked and stolen from their Facebook accounts by the Cambridge Analytica firm (Hasan, 2018; Nugroho, 2018).

The personal data of the leaked Facebook account users can be used for various purposes. Starting from political interests to business interests. This is because the Facebook personal data contains various kinds of important personal information such as place and date of birth, place of residence, gender, location, friendship,

habits, photos of account owners, conversation history, places commonly visited, psychological profiles, styles life, work, up to the current political views of the Facebook account owner which can be seen from the status of the upload and the conversation. The personal data of the users of the leaked Facebook account also has the potential to be misused to commit an extortion crime (blackmail).

The impact of the leakage and theft of personal data from Facebook users is very large and dangerous. Then how do the Indonesian government and law enforcers solve this problem? In writing this paper, we will discuss the handling and law enforcement related to leakage and theft of Facebook personal data.

II. METHOD

The method in this case is defined as a method and effort that must be made to achieve a goal by using certain tools. The writing method used in writing this paper is a descriptive qualitative method because this writing aims to determine the causes, impacts, handling, and law enforcement of cases of personal data leakage scandal of Facebook users based on existing empirical facts. Data sources: in writing this paper, two data sources were used, namely primary data sources obtained from direct observation on the internet and social networks Facebook, as well as secondary data sources obtained from literature studies and from news in print and electronic media. Data collection and analysis methods:

1. *Library* Research
   Library Research is a type of data collection technique sourced from literature studies of books, articles, journals and other scientific works related to cyber crime, law and technology, as well as developments in technology and the internet.
2. *Field* Research
   Field Research is a data collection technique that is done directly by observing developments in the world of Facebook and the internet.

III. RESULTS AND DISCUSSION

A. The Cause of Cyber Crime Leaking Personal Data of Facebook Users.

Global threats, as a result of the development and advancement of technology and information are not only aimed at attacking government and military agencies, but also threatening all aspects of human life, such as the economy, politics, culture and security of a country (Rahmawati, 2017; Aswandi, Muchin, & Sultan, 2020). Data leakage cases that have occurred can be triggered by a number of things. If we observe carefully and carefully data leaks and thefts are caused by things that are non-technical in nature. Limited knowledge and education of the public as users of information and communication technology, ignorance of technology users, carelessness and negligence of data owners and users of information and communication technology or in this case Facebook and internet users. Apart from these things,

Crimes that are closely related to the use of computer-based technology and telecommunication networks are classified into several forms according to the modus operandi used (Panjaitan, Pranoto, Siregar, & Fahmi, 2005). The intrusion and theft of personal data from Facebook users is a cyber crime in the form of infringements of privacy, crimes aimed at personal and confidential information,

such as computerized personal data forms, credit card numbers, ATM PINs, disabilities or illnesses. hidden away and so on (Maskun, 2013).

Based on cases of data leakage scandals that have occurred and tracing of these cases, there are several main causes of leakage and theft of Facebook's personal data that need to be paid close attention to by the public as the subject of users or users of Facebook and the internet and similar social networks. other. The main causes are as follows:

1. **The behavior, habits, and culture of the Indonesian people who like or like to share and disseminate information and data relating to their associations, close people around them, their groups, their families, and their close relatives.**

Indonesian people are known to be very friendly and very happy to socialize. The friendliness and reluctance of the Indonesian people makes it no wonder that Indonesians have many friends. The habit of exchanging data and personal information has become a common thing for Indonesians because it is based on mutual trust. The habit of exchanging personal data is often carried out by Indonesians such as exchanging telephone numbers or Whatsapp numbers as well as their social media accounts (social media) such as Facebook, Instagram, Twitter, notifying their e-mail address and even other similar social networking accounts. This is also often done by the Indonesian people towards people they have just met on various occasions. In addition, it is also the custom of Indonesians to include their personal data on their social network accounts (such as Facebook, Instagram, Twitter, and others). These data and information tend to be listed relatively completely and honestly in their social network profiles. In connection with this, the characteristics of the internet and cyberspace are very free and open, the data and information listed are easily accessible by other people around the world, and of course flow and move from one place to another without being controlled.

2. **Carelessness or negligence of data owners in managing their confidential data due to negligence or ignorance.**

The habit and / or behavior of providing confidential information and data such as passwords and usernames to trusted people is often used by some Indonesians. The real goal is good, namely to help manage and carry out the various tasks concerned. However, if the person who is trusted is not a good person and has evil intentions behind it, then giving confidential information and data such as passwords and usernames to other people will be very fatal. Other people will be able to access your account freely, and can do piracy, or act maliciously on behalf of your name, for example spam, blackmail (extortion).

3. **Characteristics of a free and open internet.**

The internet was originally known as the ARPANet, which is a network system through connections between computers in vital areas in order to overcome the problem of nuclear attacks (Kamarga, 2002). The presence of the internet in all corners of the world is a sign that globalization is something that cannot be avoided by the world community (Ismail, 2009). The Internet is a global network that people around the world can connect to and access. The internet has the characteristics of

being free and open. We can find any information and data from the internet using search engines such as Google, Yahoo, Bing, MSN Search, Ask, Yandex, AOL, and so on. By using the internet we can improve the flow of information, accelerate the flow of information, provide opportunities for everyone, especially internet users, to gain broader horizons (Pratama, 2013). We can easily find personal information and data about a person, such as biography, curriculum vitae, address / place of residence and others. Leading applications on the internet such as Facebook, Twitter, Gmail, Yahoo, Blogspot, Instagram, Youtube, and various game applications that must be connected to the internet (online games) often require users to register their identity correctly in order to be able to. use features in applications on the internet. This makes internet users register their personal data and location correctly and relatively completely because in addition to obeying internet ethics.

4. The deliberation of certain parties to commit cyber crimes to achieve certain specific goals.

One of the main causes of leakage of personal data on the internet is because there is a deliberate intention by certain parties to find and break into the data they need to achieve a certain goal. Crimes that are usually deliberately committed in the internet world are data theft, account number breach, account hijacking, alteration of information, blackmail (extortion) on behalf of other innocent people, usually the name of the account owner being compromised, use of fake data, public deception, customer fraud. , and many more crimes that are deliberately committed by certain parties in the internet world. An individual or a group armed with hacking techniques and knowledge in the field of technology and the internet can hack the accounts and privacy of others and steal the data they need to commit a crime. The characteristics of Cyber Crime are more universal, even though they have special characteristics, namely that crimes are committed by people who are experts and master the use of the internet and its applications (Sumarwani, 2014). Some people can abuse their abilities in the world of technology, especially the internet, to commit crimes for personal or group gain. Hackers can carry out their actions via Internet Relay Chat (IRC), Voice Over IP (VoIP), ICQ, Online Forums, and encryption (Arifah, 2011).

Therefore, it is important that every individual must have concern and awareness of the ethics of using the internet so that there is no misuse of their knowledge, skills and abilities in the world of technology and the internet. This needs to be implemented for the security of all parties' data and for the convenience of all internet usage. There are three approaches to maintaining security in cyberspace / internet, namely the technological approach, the socio-cultural approach, and the legal approach (Mansur & Gultom, 2011).

B. The Negative Impact of the Facebook User's Personal Data Leakage Scandal.

The scandal of data leakage and personal information of facebok users resulted in the following things:

1) Moral loss for Facebook users whose personal data is leaked

As a result of data leakage, Facebook users become worried and feel insecure if one day such personal data and information is misused by malicious parties who have certain interests and purposes. Not only worried about the data that was stolen

yesterday but also worried that in the future there will also be a similar incident. So that the trust of Facebook users is reduced. Facebook account users feel that the personal data and information they have entered does not guarantee its security and confidentiality.

2) Decrease in shares owned by the company Facebook

Investors in the Facebook company are worried about the Facebook personal data leak scandal that befell Facebook users from all countries in the world. This resulted in shares owned by Facebook dropping to 6.77% (six point seventy-seven percent) (Pratomo, 2012). The valuation value of the Facebook company has decreased to USD 49.4 billion (forty-nine point four billion United States Dollars) or the equivalent of IDR 679.92 trillion (six hundred seventy nine point ninety two trillion rupiah).

3) Calls from around the world to remove Facebook

As a result of the leakage of personal data that occurred to Facebook users, it was not uncommon for them to choose to leave their Facebook account. Internet users are busy calling for deleting Facebook. Internet users, who are usually called netizens, are busy calling for opinions regarding the leakage of personal data from Facebook users using the hashtag #deletefacebook.

C. Handling and Law Enforcement of Cyber Crime Cases Leaking Personal Data of Facebook Users.

Law enforcement includes implementing institutions (courts, prosecutors, police), executing or law enforcement officials (judges, prosecutors, police), and administrative aspects (such as judicial processes, investigative processes, detention processes and so on) (Asshiddiqie, 2006). Based on data released by Facebook, Indonesia is the third country in the estimation of the misuse and breach of personal data by Cambridge Analytica after the United States and the Philippines (Yozami, 2018). Even though there has been no significant impact related to the leakage of personal data of Indonesian Facebook users, this incident still raises the feelings of concern for many parties. Because it does not rule out the possibility that one day the data will be misused to commit a crime. The government and law enforcement immediately take action and examine cybercrime leaks and theft of personal data of Facebook users. The Indonesian government through KOMINFO (Ministry of Communication and Information of the Republic of Indonesia) has provided a written warning to Facebook Indonesia regarding the leakage of the personal data of Indonesian Facebook users. The Facebook company as one of the Electronic System Providers (PSE) must fulfill its obligations in accordance with the standard obligations contained in the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems. The government has also summoned Facebook Indonesia for information regarding the leak of the personal data of Facebook users.

In addition, if Facebook does not provide further information regarding the Indonesian Facebook user's personal data leak scandal, KOMINFO (Ministry of Communication and Information of the Republic of Indonesia) will act decisively and may close Facebook access in Indonesia or block the Facebook application. It is not only administrative witnesses who can be dropped on Facebook. Based on

information from KOMINFO (Ministry of Communication and Information of the Republic of Indonesia), Facebook can also be subject to criminal sanctions with the threat of imprisonment of 12 (twelve years) and a fine of IDR 12,000,000,000 (twelve billion rupiah).

The Indonesian government through KOMINFO (Ministry of Communication and Information of the Republic of Indonesia), together with POLRI (National Police of the Republic of Indonesia) ensures that it has taken steps to handle the Facebook data leak scandal in accordance with the legal steps and procedures in force in Indonesia. Facebook Indonesia parties have been summoned to appear and asked for a number of information regarding the case. In addition, as a response to the occurrence of cases of leakage of personal data from Facebook users as well as efforts to deal with them, the Government of Indonesia together with the ASEAN (Association of South East Asian Nations) will design cooperation related to cyber crime security for the Southeast Asian region.

Facebook can also be criminalized by using the ITE Law or the so-called Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. Article 30 of the ITE Law states that every person who knowingly and without rights accesses another person's computer or electronic system in any way for the purpose of obtaining electronic information and / or electronic documents, and also any person who knowingly and against the law or without the right to access computer systems and / or electronic systems in any way by violating, bypassing, bypassing, or bypassing a security system.

The criminal threat for violating Article 30 of the Information and Electronic Transactions Law (ITE Law) is contained in Article 46, namely those who violate Article 30 paragraph (1) will be subject to imprisonment for a maximum of 6 (six) years and / or a maximum fine. IDR 600,000,000 (six hundred million rupiah). Anyone who violates Article 30 paragraph (2) will be subject to a maximum imprisonment of 7 (seven) years and / or a maximum fine of Rp. 700,000,000 (seven hundred million rupiah). Anyone who violates Article 30 paragraph (3) will be subject to a maximum imprisonment of 8 (eight) years and / or a maximum fine of Rp. 800,000,000 (eight hundred million rupiah). The threat to violation of each verse is different because of the difference in the severity of the offense committed as well. Article 30 of the Law on Information and Electronic Transactions (UU ITE) may be imposed on Facebook if it is proven that the leakage of the personal data of Facebook users is because the personal data was intentionally leaked or notified by Facebook to a third party for any purpose, be it business. , as well as up to politics. Cyber Crime, such as the case of Facebook data leakage, can be tackled globally by modernizing the material criminal law and its procedural laws in line with international conventions related to these crimes, increasing the quality standards of the national internet network according to international standards (Nasution, Hius, & Saputro, 2014).

D. Legal Constraints and Lack of Law in Indonesia in Handling Cyber Crime Cases Leaking Personal Data of Facebook Users.

Constraints and shortcomings of law in Indonesia that become obstacles in handling cases of cyber crime Facebook data leakage include the following:

a. Regulation of the Minister of Communication and Information Technology of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, only contains administrative witnesses and does not contain criminal sanctions.
b. Indonesia does not yet have a law regulating the protection of personal data in electronic systems.
c. The types of criminal sanctions that are regulated in the ITE Law are only imprisonment and fines as regulated in Article 10 of the Criminal Code, there is no type of development of special criminal sanctions for criminals in information and electronic transactions (Supanto, 2016; Handayani, 2016).
d. The examination of witnesses and victims encountered many obstacles, because at the time the crime took place not one witness saw him (testimonium de auditu) (Golose, 2006)
e. Currently, the crime reporting system related to cyber crime is still integrated with general criminal crimes and the method of reporting to the police is still conventional (Daryono & Sugiantoro, 2017).
f. In cyber crime cases, there are often obstacles, especially in terms of arresting suspects and confiscating evidence, the police have difficulty finding and determining who is the perpetrator because cybercrimes are often committed not using their own computers (Winarni, 2016).

IV. CONCLUSION

With the development of information and communication technology, it is accompanied by an increase in the risk of crime in cyberspace using computers and the internet or what is known as cyber crime. The leakage of Facebook users' personal data is one of the consequences of the increasingly sophisticated developments in technology and the internet. Unfortunately, Indonesia does not yet have adequate legal rules to regulate cyber crime.

V. REFERENCES

Arifah, D. A. (2011). Kasus cybercrime di indonesia. *Jurnal Bisnis dan Ekonomi*, *18*(2), 185-195.

Asshiddiqie, J. (2006). *Konstitusi dan Konstitusionalisme Indonesia*. Jakarta: Penerbit Sekretaris Jendral dan Kepaniteraan Mahkamah Konstitusi RI.

Aswandi, R., Muchin, P. R. N., & Sultan, M. (2020). Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS). *Jurnal Legislatif, 3*(2), 167-190.

Daryono, D., & Sugiantoro, B. (2017). Pengembangan Framework Pelaporan Cyber Crime. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *1*(3), 133-147.

Franedya, R. (2018). Data Facebook Juga Pernah Dibobol Cambridge Analytica. *CNBC Indonesia,* 01 October 2018, retrieved from https://www.cnbcindonesia.com/tech/20181001101309-37-35438/data-facebook-juga-pernah-dibobol-cambridge-analytica

Gollese, P. R. (2006). Perkembangan cybercrime dan upaya penanganannya di Indonesia oleh Polri. *Buletin Hukum Perbankan dan Kebanksentralan*, *4*(2), 29-42.

Handayani, P. (2016). Penegakan Hukum Terhadap Kejahatan Teknologi Informasi (Cyber Crime). *Jurnal Dimensi*, *2*(2), 1-18.

Hanny Kamarga, *Belajar Sejarah Melalui E-Learing: Alternatif Mengakses Sumber Informasi Kesejarahan.* Jakarta: Intimedia, 2002.

Hasan, R. A. (2018). Cambridge Analytica Diduga Cemarkan Hillary Clinton dalam Pilpres AS 2016. *Liputan 6,* 21 March 2018, retrieved from https://www.liputan6.com/global/read/3393654/cambridge-analytica-diduga-cemarkan-hillary-clinton-dalam-pilpres-as-2016

Ismail, D. E. (2009). Cyber Crime di Indonesia. *Jurnal Inovasi*, *6*(3), 242-247.

Mansyur, D. M. A., & Gultom, E. (2005). *Cyber Law dan HAKI dalam Sistem Hukum Indonesia.* Jakarta: Refika Aditama.

Maskun, M. (2013). *Kejahatan Siber (Cyber Crime).* Jakarta: Kencana.

Nasution, A., Hius, J. J., & Saputra, J. (May, 2014). Mengenal dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari-Hari dalam Pendidikan, Pemerintahan dan Industri dan Aspek Hukum Yang Berlaku. *SNIKOM Banda Aceh*, No. ISBN, 978-602.

Nugroho, B. P. (2018). Cambridge Analytica, Konsultan Politik Super yang Gunakan Big Data. *Detik News,* 12 March 2018, retrieved from https://news.detik.com/berita/d-3912026/cambridge-analytica-konsultan-politik-super-yang-gunakan-big-data

Pandjaitan, H. I. P., Pranoto, H., Siregar, M. D. A., & Fahmi, I. (2005). *Membangun Cyber Law Indonesia yang Demokratis*. Jakarta: IMLPC.

Pratama, E. A. (2013). Optimalisasi Cyberlaw untuk Penanganan Cybercrime Pada E-Commerce. *Bianglala Informatika*, *1*(1), 1-10.

Pratomo, Y. (2018). Zuckerberg Akhirnya Angkat Bicara soal Kebocoran Data Facebook. *Kompas,* 22 March 2018, retrieved from https://tekno.kompas.com/read/2018/03/22/09070997/zuckerberg-akhirnya-angkat-bicara-soal-kebocoran-data-facebook

Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara, 7*(2), 35-50.

Republic of Indonesia. (2016). Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, (BN 2016, No. 1829).

Republic of Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, (LN 2016, No. 251, TLN No. 5952).

Rumlus, M. H., & Hartadi, H. (2020). Policy the Discontinuation of Personal Data Storage in Electronic Media). *Jurnal HAM, 11*(2), 285-299. DOI: http://dx.doi.org/10.30641/ham.2020.11.285-299

Sumarwani, S. (2014). Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif. *Jurnal Pembaharuan Hukum*, *1*(3), 287-296.

Supanto, S. (2016). Perkembangan Kejahatan Teknologi Informasi *(Cyber Crime) dan Antisipasinya dengan Penal* Policy. *Yustisia, 5*(1), 52, 70. https://doi.org/10.20961/yustisia.v5i1.8718

Winarni, R. R. (2016). Efektivitas Penerapan Undang–Undang ITE dalam Tindak Pidana Cyber Crime. *Jurnal Ilmiah Hukum dan Dinamika Masyarakat*, *14*(1), 16-27.

Yozami, M. A. (2018). Sanksi yang Bisa Dikenakan ke Facebook Terkait Bocornya Data Pengguna di Indonesia. *Hukum Online,* 10 April 2018, retrieved from https://www.hukumonline.com/berita/baca/lt5acc9325d6f81/sanksi-yang-bisa-dikenakan-ke-facebook-terkait-bocornya-data-pengguna-di-indonesia/