TATOHI: Jurnal Ilmu Hukum
Volume 5 Issue 6 August, 2025: p. 271 - 279
E-ISSN: 2775-619X
https://fhukum.unpatti.ac.id/jurnal/tatohi/index
TATOHI: Jurnal Ilmu Hukum
doi : 10.47268/tatohi.v5i6.2994

Cyber Crime Social Media Account Data Hacking in Indonesia

Ari Sapta Pribowo[1*], Muhammad Nurcholis Alhadi[2]

[1,2] Faculty of Law, Universitas Muhammadiyah Kalimantan Timur, Samarinda, Indonesia.
: 2011102432056@umkt.ac.id
Corresponding Author*

Abstract

Introduction: *Legal regulations and sanctions against perpetrators of social media account data hacking. Data hacking is one of the criminal acts of cybercrime (cyber crime).*
Purposes of the Research: *To find out and analyze the legal arrangements regarding hacking and criminal acts against social media account data hacking in Indonesia and the liability for criminal sanctions against perpetrators of social media account data hacking.*
Methods of the Research: *Normative legal research, researchers use a statutory approach, and a case approach.*
Findings of the Research: *The results of this study show that, what are the legal arrangements that discuss the formulation of the problem and what are the criminal sanctions against the perpetrators of hacking. The results of this study show that Article 30 of the Electronic Information and Transaction Law regulates the criminal acts of hacking and criminal sanctions received by the defendant from the results of the discussed decision, namely Article 30 Paragraph 2 Jo. Article 46 Paragraph 2 of Law Number 19 of 2016 concerning Information and Electronic Transactions.*

Keywords: Cybercrime; Hacking; Criminal Liability.

Submitted: 2025-04-10 *Revised: 2025-08-23* *Accepted: 2025-08-25* *Published: 2025-08-31*

How To Cite: Ari Sapta Pribowo, Muhammad Nurcholis Alhadi. "Cyber Crime Social Media Account Data Hacking in Indonesia." *TATOHI: Jurnal Ilmu Hukum* 5 no. 6 (2025): 271-279. https://doi.org/10.47268/tatohi.v5i6.2994

INTRODUCTION

In Indonesia, the use of social media platforms is becoming more widespread. In this digital era, many criminal activities exploit personal data both as a tool and as a target, so the protection of this information is more important than ever. Unfortunately, a large number of individuals are unaware that their personal data is very vulnerable to misuse by irresponsible parties.

Personal data refers to any information about an individual that is considered highly sensitive and private. Therefore, individuals should take precautions to safeguard their data and prevent unauthorized access or exploitation for personal gain. More specifically, personal information includes details that are closely related to individuals and can be used to determine their unique attributes or behavior patterns. According to the UK Data Protection Act of 1998, which replaced the previous version of 1984, "personal data is defined as information relating to a living person that can be identified through specific details held by a data controller". Personal data also includes details regarding individual characteristics, such as full name, age, gender, education level, and other relevant personal attributes.[1] In Indonesia, the absence of robust data security measures has resulted in many cases of information leaks and widespread unauthorized disclosures. The incidents are

[1] Hadi Prasetyo, "Penegakan Hukum Terhadap Debt collector yang Melakukan Penyebaran Data Pribadi Pengguna Fintech Ditinjau dari Pasal 26 UU No 19 Tahun 2016 tentang Informasi Teknologi Elektronik", *Jurnal Bandung Conference Series: Law Studies* 2, no. 1 (2022): p. 616.

categorized as cybercrimes, including social media account hacking and identity theft, which can lead to data breaches, extortion, and deceptive online activity. The Indonesian government's initiative to draft and enact Law Number 27 of 2022 concerning Personal Data Protection, highlights the growing awareness of the need for comprehensive regulations on the protection of personal information.[2]

Several previous studies have explored related themes and challenges similar to this study. To confirm the uniqueness of this study, the authors conducted a review of previous research on comparable issues and identified key differences in their core perspectives. During the literature review, the author found various academic publications, one of which was a research conducted by Muhamad Bayu Satrio and Gan Wih Widiatno, entitled "Legal Protection of Personal Data in Electronic Media (Analysis of Facebook User Data Leakage Cases in Indonesia)".[3] Second, research by Muhammad Fathur entitled "Tokopedia's Responsibility for Consumer Personal Data Leakage".[4] Third, research by Deanne Destriani Firmansyah Putri and Muhammad Helmi Fahrozi entitled "Efforts to Prevent Consumer Data Leakage Through the Ratification of the Personal Data Protection Bill".[5]

Various data leak incidents that have occurred in Indonesia show that the current security system is still very limited in overcoming cyber threats. Some of the major social media platforms used by millions of Indonesian users, such as Facebook, Instagram, and Twitter, are often the target of hacks that can lead to large amounts of personal data leaks. Although the service provider has made efforts to tighten up its security systems, there are still many users who have not taken advantage of the security features provided, such as two-factor authentication or stricter privacy settings. This worsens the security condition of personal data in Indonesia, which opens up space for criminals to more easily hack.

One of the most common cyber-related threats involves digital attacks that impact online users. In November 2016, Norton Cyber Security published the Insight Report, which was based on an online survey involving 20,907 participants from 21 different countries around the world. The study specifically examined cybersecurity issues in three Southeast Asian countries: Malaysia, Singapore, and Indonesia. The study was conducted between September 14 and October 6, 2016, with an Indonesian sample of more than 1,000 randomly selected individuals aged 18 years and older. "Millennials have shown a decline in their online security practices," said Chee Choon Hong, director of Asian Consumer Business for Norton by Symantec.

Statistical findings show that around 20% of millennials consciously share their passwords, putting their digital security at risk. In addition, nearly 90% of Indonesian internet users regularly connect to public Wi-Fi networks, but only a small percentage of them have the necessary knowledge to secure their connections. Only 36% of individuals surveyed reported using Virtual Private Networks (VPNs) to access public networks securely through their mobile devices. In addition, 28% of consumers admit that they cannot recognize emails that contain malware infections. Choon Hong explained that "this study

[2] Albert Lodewyk Sentosa Siahaan, "Urgensi Perlindungan Data Pribadi Di Platform Marketplace Terhadap Kemajuan Teknologi," *Majalah Hukum Nasional* 52, no. 2 (2022): 210–22, https://Doi.Org/10.33331

[3] Muhamad Bayu Satrio and Men Wih Widiatno, "Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia)," *Jca of Law* 1, no. 1 (2020).

[4] Muhammad Fathur, "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen," *National Conference On Law Studies* (*Ncols*) 2, no. 1 (2020): 43–60

[5] Deanne Destriani Firmansyah Putri and Muhammad Helmi Fahrozi, "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)," *National Conference On Law Studies* (*Ncols*) 2, no. 1 (2020): 255–273

did not focus on a specific type of cyberattack, but rather on the behavior of millennials in securing their personal mobile devices". Although this research shows that users are increasingly aware of the importance of protecting their devices, especially to safeguard personal data, they are not motivated enough to take preventive measures. As many as 76 percent of mobile device owners are aware of the importance of protecting their personal data online, but only 22 percent protect their devices. As a result, as many as 39 percent of users faced password hacking, 28 percent experienced email account breaches, and 26 percent became victims of data hacking and social media accounts.

The impact caused by the existence of the cyber world, which has recently been known as cybercrime. Cybercriminals themselves have loosely translated to refer to cybercrime which can take the form of information theft, data destruction, theft of funds, pornography, jail-breaking, various actions that are not allowed by laws and regulations. Cyberspace not only has a positive impact, but also a negative impact that can harm the interests of individuals or society as a whole.

The Indonesian government needs to prepare itself carefully in dealing with cybercrime. One of the most important things is to have skilled and knowledgeable human resources in the field of cybersecurity. Qualified experts can support a positive mindset towards global change, increase awareness of technological and information advancements, and understand the impact of cyber threats on social life. In addition, Indonesia also needs an adequate state security system, which includes infrastructure and technology to detect, prevent, and handle cyberattacks. Investment in the development of state-of-the-art and effective security facilities is needed to deal with the increasingly complex threat of cybercrime, by strengthening human resources and security systems, Indonesia can improve its ability to overcome cyber threats. This includes adequate education and training for cybersecurity experts, as well as the development and improvement of technology infrastructure that can quickly and effectively identify, protect, and respond to cyberattacks.

Legal protection of personal data is of paramount importance to every individual, and the state as a policy-making institution has a responsibility to protect these fundamental rights. This has been regulated in Law Number 27 of 2022 concerning Personal Data Protection which is the basis for consideration: 1) That "personal data protection is one of the human rights related to personal personal protection, so there needs to be a legal basis that provides security for personal data, in accordance with the Constitution of the Republic of Indonesia of 1945"; 2) That "the protection of personal data aims to guarantee citizens' right to personal personal protection, increase public awareness, and ensure endorsement and attention to the significance of personal data protection". Regulations regarding personal data are currently covered by various laws and regulations. Therefore, to increase the effectiveness of personal data protection, more organized regulations are needed in the form of laws.

METHODS OF THE RESEARCH

In this type of research, the author will use a normative or normative juridical approach and solve a problem related to positive law against the perpetrators of hacking social media account data of the people who are hacked. This problem also focuses on investigating how legal rules or regulations are applied in legal practice, especially related to the case that is the subject of research, namely Decision Number: 515/Pid.Sus/2021/Pn Ckr.

RESULTS AND DISCUSSION

A. Legal Regulations Regarding Hacking and Criminal Acts Against Social Media Account Data Hacking in Indonesia

Cyber crime is a form of crime that uses the internet and computers as tools or ways to commit criminal acts.[6] Hacking is the act of illegally accessing a computer system or network without the owner's permission in the context of social media, this action includes stealing login data, changing data, or using an account without the owner's permission. This phenomenon is an important issue because its impact can harm account owners personally and professionally, such as the dissemination of personal data, defamation, or extortion. Indonesia already has a number of regulations governing hacking acts, although some still need to be strengthened in their implementation. These legal arrangements aim to protect individuals' rights to privacy and personal data and to sanction offenders who violate the law.

One of the most common forms of hacking is identity theft, which aims to steal personal information for the purpose of identity fraud involving the capture of sensitive data such as usernames, passwords, emails, phone numbers, and other information in various ways, including phishing, social engineering, password breaches, keyloggers, and malware. Social media account hacking falls into the category of identity theft, where personal information is used to commit identity fraud. This act is also a form of fraud crime.[7]

After the amendment of the 1945 Constitution, the right to privacy and protection of personal data was recognized as a constitutional right of citizens. This is reflected in Chapter XA Articles 28A to 28J, as well as in Article 28G paragraph (1) which guarantees such protection and reads "Everyone has the right to the protection of personal self, family, honor, dignity, and property under his or her control, as well as the right to a sense of security and protection from the threat of fear to do or not do something that is a human right."

The protection of personal data is crucial in online transactions because it relates to the security of users, who are vulnerable and require legal protection to maintain their privacy.[8] Personal data protection is the right of every individual to maintain the confidentiality of personal information. The state has a role as a protector through the provisions of Article 28G of the 1945 Constitution, which mandates the protection of personal data. This includes respect for human rights, equality, and respect for individual rights. Therefore, a strong legal foundation is needed to ensure the security of privacy and personal data, as well as create a conducive business climate.[9]

Website hacking has also been stipulated in "Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions." Law Number 19 of 2016, which is an amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, is the main regulation to overcome violations in the field of Information and Transactions. In addition to providing legal protection, this law also stipulates criminal sanctions for violators. The crime of website

---

[6] Widodo, *Hukum Pidana di Bidang Teknologi Informasi (Cyber crime Law); Telaah Teoritik dan Bedah Kasus*, (Yogyakarta: Aswaja Presindo, 2011) p. 12

[7] I Dewa Putu Gede Putra Sedana Jaya, I Nyoman Gede Sugiartha, I. B. Gede Agustya Mahaputra, "Analisis Yuridis Tindak Pidana Penipuan Melalui Peretasan Direct Message Akun Instagram", *Jurnal Analogi Hukum* 5, no. 3 (2023): 281-286

[8] Celina.Tri Siwi Kristiyanti, *Hukum.Perlindungan Konsumen*, (Jakarta: Sinar Grafika, 2011), p. 13.

[9] Sinta.Dewi Rosadi, 2018, *Perlindungan.Privasi dan Data Pribadi.dalam Era Ekonomi Digital.di Indonesia*, (Bandung: Fakultas.Hukum Universitas Padjadjaran, 2018): p. 96.

hacking is regulated in Article 30 of Law Number 19 of 2016, as an amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

Based on Article 30 of Law Number 19 of 2016, which is an amendment to "Law Number 11 of 2008" concerning Information and Electronic Transactions, it is explained that "Every individual who intentionally and without permission, or illegally, accesses the computer and/or electronic system belonging to another person in various ways, Every person who intentionally and without permission, or illegally, access computers and/or electronic systems to obtain electronic information and/or electronic documents, and Any person who intentionally and without permission, or illegally, accesses computers and/or electronic systems by means of damage, penetration, or breach the security of their systems".

Article 30 paragraph (1) of the Electronic Information and Transaction Law states that "any person who intentionally and without rights or illegally accesses the computer and/or electronic system belonging to another person in any way". It is seen that this article, there are clear elements such as: every person, intentionally and without rights, unlawfully accesses another person's computer or electronic system, as well as in any way. a) Element of each person: in this element each person referred to is a person as a subject of law who can be responsible and capable of law based on the Legislation; b) Elements deliberately and without the right to violate the law. This element refers to the intention or intentionality accompanied by the full awareness of the person in committing an act contrary to the law; c) Elements of accessing computers and/or electronic systems belonging to others. This element explains that the electronic system belonging to another person is something private and not in the public interest; d) Element in any way: in any way referred to herein is a hacker who accesses either through a device belonging to the victim that is hacked or using a device or internet network.

Criminal sanctions that can be imposed on the perpetrators of hacking are regulated in Article 46 paragraph 1 of Law Number 19 of 2016, which states that "every person who meets the elements in Article 30 paragraph (1) can be sentenced to a maximum of 6 (six) years in prison and/or a maximum fine of IDR.600,000,000.00 (six hundred million rupiah)". Based on "Article 30 paragraph (2) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions" Article 30 paragraph (2) has the same elements as paragraph (1), but this paragraph adds elements of obtaining electronic information and/or electronic documents. This means that the person trying to access the system has the intention to steal the data or electronic information that is in the victim's system. Article 30 paragraph (2) is directly related to other articles, namely Article 46 paragraph (2) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions regarding criminal threats if they violate the provisions of Article 30 paragraph (2), which reads: "Every person who meets the elements as referred to in Article 30 paragraph (2), sentenced to a maximum of 7 (seven) years in prison and/or a maximum fine of IDR.700,000,000.00 (seven hundred million rupiah)".

Elements in "Article 30 paragraph (3) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions" This element includes violations, penetrations, exceedances, or destruction of security systems. This indicates that "the perpetrator of the hack or destruction of the system performs an act by penetrating the computer's security". Criminal sanctions are regulated in Article 46

paragraph (3), which stipulates "a maximum prison sentence of 8 years and/or a maximum fine of IDR. 800,000,000.00 (eight hundred million rupiah)".

Article 32 paragraph 1 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, which reads: "(1) Every person deliberately and without rights or unlawfully in any way alters, adds, subtracts, transmits, damages, removes, hides an Electronic Information and/or Electronic Document belonging to another person or belonging to the public". Another rule, Article 22 letter B of Law Number 36 of 1999 concerning Telecommunications states that "everyone is prohibited from committing actions without rights, unauthorized or altering access to telecommunication networks, telecommunication services, or special telecommunication networks".

B. Criminal Accountability and Sanctions for Perpetrators of Social Media Account Data Hacking

Criminal liability, or criminal liability, refers to the ability to blame a person for an unlawful act he or she committed, resulting in him or her being held criminally liable for those acts.[10] Basically, criminal liability is imposed on the perpetrators of criminal acts, but must meet the following four main conditions:[11] 1) The existence of an action (either in the form of direct action or negligence) of the perpetrator; 2) The action meets the formulation of the delicacy regulated in the law; 3) The action is unlawful; 4) The perpetrator must be criminally accountable.

If the perpetrator cannot be held criminally accountable, then the sanctions imposed will be meaningless. Before a person can be held criminally responsible, it must first be proven that he meets all the elements contained in the criminal charge. Criminal liability means that individuals have the freedom to determine whether to commit an act or not, in one of the considerations and decisions of the Panel of Judges related to the hacking case, the Decision of the Cikarang District Court Number: 515/Pid.Sus/2021/PN Ckr which is as follows: Considerations and Decisions of the Panel of Judges: The Panel of Judges decided to immediately decide to immediately apply the indictment in the form of the first alternative as stipulated in "article 30 Paragraph (2) Jo. Article 46 Paragraph (2)" of Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions. The elements of the indictment are as follows: 1) Element of Everyone: The element of "everyone" refers to legal subjects for whom accountability can be demanded, including legal entities and individuals, which in this case applies to the Defendant Chandra Kirana Saputra; 2) Elements Intentionally: According to E. Y. Kanter, SH and S. R. Sianturi, SH in their book entitled "The Principles of Criminal Law in Indonesia and Its Application", Publisher Storia Grafika Jakarta 2002, what is meant is "deliberately means that a person wills and is aware of the actions and consequences arising from the act"; 3) Facts at the Trial: The defendant Chandra Kirana Saputra Bin Trisna Effendi Saputra used internet media to see news about the sale of Population Identification Number and Family Card data on RaidForums throughout Indonesia, then the defendant tried to do something similar to the news, Then the Defendant took data belonging to the Bekasi Regency Disdukcapil entered using the Bekasi Regency Disdukcapil Website with the http://sitepak.bekasikab.go.id

[10] Yunita Rahayu Kurniawati. "PertanggungJawaban Pidana Atas Penyebaran Berita Bohong (Hoax) di Media Sosial". *Dinamika*, *26*, no. 4 (2020): 422-437 2020.

[11] Romli Atmasasmita, *Perbandingan Hukum Pidana,* (Bandung: Penerbit Mandar Maju, 2000), p. 67

Website by registering as a new user using the Population Identification Number spread across google searches, then after the Defendant logged in using the Population Identification Number belonging to someone else on the http://sitepak.bekasikab.go.id website. Or websites related to the population of Bekasi; 4) Sociological Considerations: in the case of the Decision (Number 515/Pid.Sus/2021/PN Ckr), the aggravating and mitigating factors are: Incriminating circumstances: The Defendant's actions may damage the population data of Bekasi Regency; Mitigating circumstances: (1) The defendant has never been convicted; (2) The defendant behaved politely during the trial, admitted frankly his actions, expressed his remorse and promised not to repeat his actions. 5) Verdict: After considering all the elements of Article 30 Paragraph 2 Jo. Article 46 Paragraph 2 of Law of the Republic of Indonesia Number 19 of 2016 concerning Information and Electronic Transactions, the Panel of Judges decided that the Defendant was legally and convincingly proven to have committed a criminal act "deliberately and without rights or unlawfully accessing a computer in any way with the aim of obtaining electronic documents" as in the first alternative allegation. The defendant was sentenced "to imprisonment for 1 (one) year and a fine of Rp. 200,000,000 (two hundred million rupiah) with the provision that if the fine is not paid, it will be replaced with imprisonment for 3 (three) months. The evidence was in the form of 3 CPU units, 1 mobile phone, 1 Simcard to be destroyed, and 5 email accounts used to hack and the defendant was obliged to pay a case fee of IDR. 2000.

The hearing was held on October 28, 2021 by the Panel of Judges of the Cikarang District Court consisting of Ali Sobirin, S.H., M.H., as the Presiding Judge, Chandra Ramadhani, S.H., M.H., and Samsiati, S.H., M.H. each as Member Judges assisted by Evi Setia Permana, S.H., Substitute Registrar at the Cikarang District Court, and attended by Sudiarso, S.H., M.H. Public Prosecutor and in the presence of the Defendant.

Article 30 paragraph 2 of Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions "Any person who deliberately and without rights distributes and/or transmits or makes accessible Electronic Information and/or Electronic Documents that have content that violates morality as referred to in Article 27 paragraph 1 may be sentenced to imprisonment a maximum of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah)."

Article 46 paragraph 2 of Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions "Any person who deliberately and without the right disseminates or distributes electronic information or electronic documents containing content as referred to in Article 27 paragraph 1 may be subject to criminal penalties as intended in Article 30 paragraph 2." In this case, Chandra Kirana Saputra Bin Trisna Effendi Saputra was legally and convincingly proven to have committed a criminal act in the article because he had hacked social media account data. This is based on witness statements, evidence, confessions of the defendant, modus operandi supported by preliminary evidence, as stated in the indictment by the investigating prosecutor. Therefore, the defendant hacked account data for personal interests. Because of the principle *of lex specialis derogat legi generali* in criminal law. "If an act is included in the general criminal provisions but also included in the special criminal provisions, then only the special criminal provisions apply", which means that the criminal act (*lex specialis*) must include all the main elements of the criminal act (*lex generalis), including one or more special elements (lex specialis) that are not present in the element (lex generalis*). Article 30 paragraph 2 jo. Article 46 paragraph

2 of the Electronic Information and Transaction Law is an example of the same criminal law. In addition, the legal subjects of lex specialis and lex generalis must be the same. The defendant, Chandra Kirana Saputra Bin Trisna Effendi Saputra, is the subject of the law in one of the cases that the researcher analyzed. Based on the principle contained in Article 63 paragraph 2 of the Criminal Code, it states that: "If an act is included in the general criminal provisions but also included in the special criminal provisions, then only the special criminal provisions apply". Special criminal provisions apply if the offense goes against one or both of those criminal provisions. The condition is that the criminal act must include all the main elements of the criminal act (lex generalis), plus one or more special elements (lex specialis) that are not contained in the elements (lex generalis). Lex specialis and lex generalis must be balanced, not biased.

Based on the results of the above verdict, the judge should be able to increase the perpetrator's sentence because judging from sociological considerations, the perpetrator's criminal act can damage the population data system of the Bekasi community. The judge's decision does not reflect the principle of lex specialis derogat legi generali, which means that when law enforcement prosecutes and decides a case in court, the special rule of law overrides the rule of general law. Because hacking is carried out through online or internet, the law on information and electronic transactions regulates criminal acts related to the hacking of account data carried out by the defendant.

CONCLUSION

Criminal liability in the context of hacking refers to the concept that a person can be held accountable for his unlawful actions if certain conditions are met, such as the existence of an unlawful act that can be proven and the perpetrator can be criminally accountable, in this case, the hacking of a social media account carried out by the Defendant Chandra Kirana Saputra is proven to meet the elements of a criminal act in accordance with Article 30 Paragraph 2 Article 46 Paragraph 2 of Law Number 19 of 2016 concerning Information and Electronic Transactions, which regulates "illegal access to electronic systems and theft of personal data". Indonesia already has regulations regulating hacking acts, especially through "Law Number 19 of 2016 which amends Law Number 11 of 2008 concerning Information and Electronic Transactions." Article 30 of the Electronic Information and Transactions Law regulates "the act of accessing computers and electronic systems belonging to another person without permission, either to obtain information or to damage such systems". This regulation provides criminal sanctions in the form of prison sentences and fines for hacking perpetrators. In addition, Indonesia also has legal protection for personal data as stated in the 1945 Constitution and Ministerial Regulation Number 20 of 2016 concerning Personal Data Protection, although its implementation still needs to be strengthened. The state, as a protector of human rights, has an obligation to protect the privacy and personal data of its citizens, as well as to impose strict sanctions on perpetrators of cybercrimes, including hacking. Overall, the existing legal arrangements in Indonesia already include the protection of personal data and regulations regarding hacking, but it needs to be strengthened in the implementation of these regulations to be more effective in dealing with the threat of hacking and maintaining the privacy and security of people's personal data. Criminal liability for hackers, based on the provisions of the Electronic Information and Transactions Law, shows "the importance of clear and firm legal protection in tackling cyber crimes, especially in the context of social media account hacking and identity theft".

REFERENCES

Albert Lodewyk Sentosa Siahaan, "Urgensi Perlindungan Data Pribadi Di Platform Marketplace Terhadap Kemajuan Teknologi," *Majalah Hukum Nasional* 52, no. 2 (2022): 210–22, https://Doi.Org/10.33331.

Celina.Tri Siwi Kristiyanti, *Hukum.Perlindungan Konsumen*, Jakarta: Sinar Grafika, 2011.

Deanne Destriani Firmansyah Putri and Muhammad Helmi Fahrozi, "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)," *National Conference On Law Studies* (*Ncols*) 2, no. 1 (2020): 255–273.

Hadi Prasetyo, "Penegakan Hukum Terhadap Debt collector yang Melakukan Penyebaran Data Pribadi Pengguna Fintech Ditinjau dari Pasal 26 UU No 19 Tahun 2016 tentang Informasi Teknologi Elektronik", *Jurnal Bandung Conference Series: Law Studies* 2, no. 1 (2022).

I Dewa Putu Gede Putra Sedana Jaya, I Nyoman Gede Sugiartha, I. B. Gede Agustya Mahaputra, "Analisis Yuridis Tindak Pidana Penipuan Melalui Peretasan Direct Message Akun Instagram", *Jurnal Analogi Hukum* 5, no. 3 (2023): 281-286.

Muhamad Bayu Satrio and Men Wih Widiatno, "Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia)," *Jca of Law* 1, no. 1 (2020).

Muhammad Fathur, "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen," *National Conference On Law Studies* (*Ncols*) 2, no. 1 (2020): 43–60.

Sinta.Dewi Rosadi, 2018, *Perlindungan.Privasi dan Data Pribadi.dalam Era Ekonomi Digital.di Indonesia*, Bandung: Fakultas.Hukum Universitas Padjadjaran, 2018.

Widodo, *Hukum Pidana di Bidang Teknologi Informasi (Cyber crime Law); Telaah Teoritik dan Bedah Kasus*, Yogyakarta: Aswaja Presindo, 2011.

Yunita Rahayu Kurniawati. "PertanggungJawaban Pidana Atas Penyebaran Berita Bohong (Hoax) di Media Sosial". *Dinamika*, *26*, no. 4 (2020): 422-437 2020.