DJLS Discourse journal on Law and Society

E-ISSN: 3089-6797
P-ISSN: 3089-6789

Application of Legal Sanctions Against Perpetrators of Social Media Account Theft Based on the Law on Information and Electronic Transactions

Marsa Zahirah Badzlin[1]*, Kayla Putri Adnin[2], Jose Mikha Sembiring[3], Jessica Cristiana Siahaan[4], Suci Ramadani[5]

[1] Law Study Program, Universitasi Pembangunani Pancai Budi, Indonesia; e-mai: marsazahirah@gmail.com
[2] Law Study Program, Universitasi Pembangunani Pancai Budi, Indonesia; e-mai: kaylaputriadnin21@gmail.com
[3] Law Study Program, Universitasi Pembangunani Pancai Budi, Indonesia; e-mai: sembiringjose70@gmail.com
[4] Law Study Program, Universitasi Pembangunani Pancai Budi, Indonesia; e-mai: jessikaasihaan06@gmail.com
[5] Law Study Program, Universitasi Pembangunani Pancai Budi, Indonesia; e-mai: suciramadani@dosen.pancabudi.ac.id
* Corresponding Author: Marsa Zahirah Badzlin

Abstract. The swift advancement of information technology has greatly influenced society, while also raising the threat of cybercrime. These offenses encompass the theft of social media accounts, unauthorized access to online information, and breaches of personal data security. This research intends to explore various types of cybercrime in Indonesia, the legal measures in place, and the obstacles law enforcement encounters when proving cybercrime incidents. The study adopts a qualitative method by reviewing literature, which includes laws, court rulings, academic articles, and reports from pertinent organizations. The findings reveal that even though laws like the Electronic Information and Transactions Law and the Personal Data Protection Law establish a legal framework, there are still issues related to digital evidence, coordination between agencies, and the public's understanding of data security. Consequently, there is a need for a more thorough law enforcement approach, enhanced digital education, and collaborative efforts among the government, law enforcement agencies, and the community to effectively combat and manage cybercrime.

Keywords: Cybercrime; Data Protection; Digital Evidence; Electronic Information; Transactions Law.

Received: August 11, 2025
Revised: October 29, 2025
Accepted: December 13, 2025
Published: February 28, 2026
Curr. Ver.: February 28, 2026

1. Introduction

Rapid changes in information and communication technology and globalization have led to significant transformations in various aspects of human life. Technological advancement improves the standard of human life (Muhammad Arif Sahlefi, 2023). The development of digital technology today not only affects the economic sector, education, and government, but also transforms the way people interact and communicate. Activities that used to be carried out physically are now conducted through various digital platforms, one of which is social media. Social media provides convenience for the community to establish relationships, share information, and express themselves without the constraints of space and time (Nasrullah, 2015). However, although it offers convenience, social media also presents new challenges, increasing the likelihood of misuse of technology that leads to crime (Rahmayanti, 2020). Cybercrime becomes a complex legal issue because it involves elements of technology and information that are difficult to track (Chairun Nasution:158). One type of cybercrime that often occurs and disturbs society is social media account theft. These actions are carried out by accessing other people's accounts without permission, abusing passwords, and taking control of systems (Arief, 2010).

Social media account theft can cause various social and legal consequences. For victims, this action not only results in financial losses due to the possibility of online fraud, but also intangible losses such as defamation, privacy violations, and mental harassment due

to misuse of identity in cyberspace (Simanjuntak, 2019). In many cases, stolen accounts are used to spread fake news (hoaxes), commit fraud, or carry out other criminal acts such as phishing and scamming (Setiadi, 2020). As a legal system, Indonesia has regulations to deal with cybercrimes, including social media account theft, through Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE), which has been updated by Law No. 19 of 2016 (Ramadani, 2023). Article 30 of the UU ITE affirms that individuals are prohibited from accessing other people's electronic systems without permission. Violators of this provision are subject to criminal sanctions in accordance with Article 46, which stipulates imprisonment and/or fines (UU ITE, 2016).

However, the application of these legal regulations still faces various challenges in practice. One of the main challenges is the difficulty of proving digital crimes, because perpetrators often use technologies to hide their identities, such as virtual private networks (VPNs), proxy servers, or fake IP addresses, which make it difficult for law enforcement to track them. In addition, there are limitations in technical capabilities in digital forensics and cybersecurity, so the process of evidence and law enforcement is not yet optimal.

As an example, in Riau, specifically in the city of Pekanbaru, there was a young man with the initials R who was involved in a cybercrime case and detained at Lapas Kelas IIA Pekanbaru. He indicated that his modus operandi was individual but highly structured. R admitted that his actions were based on psychological manipulation techniques without direct threats and used methods to hide his identity. He believed that the success of the crime was due to the victim's negligence in protecting personal information. R also used other methods, such as creating fake websites that closely resemble original sites, exploiting victims through email, and utilizing software such as scripts and Trojan backdoors.

Based on this case, methods of social media account theft, especially phishing, show that perpetrators use structured strategies and take advantage of the lack of public understanding or digital literacy. This is in line with the statement of Iptu Arwan and Panit 3 Unit 1 Subdit V, Hendri Jony, a member of the Riau Regional Police, who served as a resource person in this case. He stated that phishing methods are not limited to one form, but are dynamic and continue to evolve along with the development of information technology. Therefore, this crime not only causes financial losses but also damages the reputation of victims and their families. One effective prevention effort is a multidimensional approach, including strengthening legal aspects, improving technological security, and most importantly, increasing public education and digital literacy regarding information technology and social media.

In addition to institutional factors, the level of digital literacy in Indonesian society is still relatively low, particularly in aspects of personal data protection and social media account security. Many users rely on easily guessed security features, do not activate two-factor authentication, and share personal information on digital platforms without considering the risks (Ministry of Communication and Informatics, 2021). This situation contributes to the increasing number of account theft cases on various social media platforms such as Facebook, Instagram, and WhatsApp. Therefore, a more comprehensive analysis is needed regarding the application of legal sanctions against perpetrators of social media account theft in accordance with the UU ITE, both from a normative perspective and its implementation in practice. This research is important to evaluate the extent to which the UU ITE can provide legal protection for victims and uphold justice in cyberspace. On the other hand, this study is also expected to provide input for criminal law reform in information technology and increase public awareness about the importance of digital security (Rahardjo, 2006).

2. Research Methods

This research applies metode yuridis normatif yang melibatkan pendekatan legislasi dan pendekatan kasus. Normative juridical methods are used to analyze the legal norms found in the ITE Law as well as other rules related to cybercrime, while the case approach is focused on assessing the application of legal norms in the courts.

The source of research data is obtained through a literature review and is supported by legal materials consisting of primary, secondary, and tertiary categories:

a. The primary legal materials include UU Nomor 11 Tahun 2008, UU Nomor 19 Tahun 2016, and the Criminal Code.
b. Secondary legal materials consist of legal literature, journal articles, and previous research related to cybercrime.
c. Tertiary legal materials include legal dictionaries and reliable online information sources.

Data analysis is carried out using a descriptive-qualitative approach by describing and interpreting the application of provisions in the ITE Law in relation to cases of social media account theft.

3. Research Results

Application of the ITE Law to Social Media Account Theft Cases

The results of the study indicate that account theft on social media platforms can be classified as a criminal act of unauthorized access, in accordance with the provisions of Article 30 paragraph (1) of Law No. 11 of 2008 which regulates Information and Electronic Transactions. Pasal said that "Setiap orang yang secara intentional dan tanpa hak or secara illegitimate access to computer and/or system electronic have other people with cara apa even." Unsur-unsur in this article, that covers "intentionally," "without rights," dan "illegal," is considered fulfilled if the perpetrator knowingly does access media social orang other people without permission, with intention to take over, taking advantage of the akun or the akun aquini.

In this case, the element of "intentionally" refers to the perpetrator's understanding of his actions which is found to have resulted in certain consequences, that is mastery of overcoming akun possess other people. Unsur "without rights" indicates that the perpetrator does not have permission or authority from the owner of the company to access the electronic system. While the unsur "illegal" indicates that there is a violation of the rules laws that apply, correct it as a clarification through the law or as a direct action through the principle of protection of privacy.

In law enforcement, authorities have taken advantage of this article to arrest the perpetrators of social media account theft. One of the cases that became an example was the hacking of WhatsApp in Jakarta in 2021, where the perpetrator used the SIM swap method to control the victim's account. After getting access to the account, the perpetrator sends a message to the victim and the victim commits fraud to get money. Based on the decision of the Supreme Court Nomor 178/Pid. Sus/2021/PN. Jkt. Sel, the perpetrator was declared guilty of violating Pasal 30 ayat (1) jo. Pasal 46 ayat (1) UU ITE, dan sentenced to imprisonment for ten months. This case is an illustration of the fact that the application of the UU ITE in the case of digital crime involves access without permission. Through the decision, the Court affirmed that although the social media is not a "physical thing," namun but receives legal protection because it is included in the category of system electronic personal that stores data and digital identity of individuals. Oleh because of that, theft of social media is not only a violation of privacy, but it also reflects the acquisition of digital identity which is recognized in cyber law.

In addition to that case, this study also found several similar incidents handled by the Directorate of Criminal Investigation of Siber Bareskrim Polri. For example, in 2022 there were reports related to the theft of an Instagram account by a celebrity, di mana the perpetrator hasil controlled the akun through the phishing method and then sold it di online forum international. In the procession of its handling, the perpetrator is also charged with Pasal 30 ayat (1) dan Pasal 46 ayat (1) UU ITE, and Pasal 362 of the Criminal Code because it is proven that he took advantage of his actions (Bareskrim Polri, 2022). Although the law has been passed, the application of UU ITE in the case of theft has been met with several challenges. First, proves that unsur "without rights" often sulit is carried out because the perpetrator uses technology to disguise his identity, such as Virtual Private Network (VPN) or fake IP address. Second, there are shortcomings in the ability of digital forensicists to use law enforcement apparatus, which results in the procession of investigations to be more than delayed (Widyarto, 2021). Third, there are regulations in particular, which provide for the protection of social media as part of personal data, so that the victims do not get adequate recovery (Ministry of Communication and Informatics, 2022).

In addition to repressive methods in the form of law enforcement, some recent literature also highlights the importance of preventive approaches to prevent theft from social media. Actions such as education on digital security, implementation of two-factor authentication, and improvement of understanding of cyber crime in Indonesia (Saputra dan Wibowo, 2022). Thus, the application of UU ITE is not only functional in the aspect of law enforcement, but also becomes a dasar for to build a culture law digital yang more secure and protective of privacy in the virtual world. Overall, the analysis shows that the application of the ITE Law in the case of theft in social media is carried out in accordance with the principles of special criminal law, although in practice it is needed to strengthen regulations and the

technical capacity of law enforcement. Future, collaboration between UU ITE, Criminal Code, and UU Protection of Personal Data is expected to provide more effective legal protection for social media users in Indonesia.

Obstacles to Law Enforcement Against Perpetrators of Social Media Account Theft

Although the legal basis for the crime of theft of social media accounts has been described in detail in Law No. 11 Tahun 2008 concerning Information and Electronic Transactions (UU ITE) and its amendments, the application and enforcement of it in the field of Mathematics and Electronic Transactions (UU ITE) and its amendments, the application and enforcement of it in the field of mathematics face various challenges. Hambatan ini covers technical problems, structural, cultural problems. First, the main challenge is located on digital proof. Proof of electronics is very variable and easy to manipulate, so that it requires special expertise in handling. Criminals use technology to hide their identities, such as Virtual Private Network (VPN), proxy servers, or anonymous browser (Tor network) to obscure their digital tracks. This situation makes the investigation of the identity of the perpetrator very complicated and slows down the investigation procession.

Second, the lack of technical capabilities of law enforcement officials in the field of digital forensics is also a big obstacle. Although the training has improved in several institutions, the number of investigators who have expertise in technology information is very little, especial di di remote areas. As a result, process investigation dan analysis of evidence digital sering kali time lama dan dan depend on various institutions such as Directorate Criminal Action Siber Bareskrim Polri. Third, low, level literacy digital di kalangan society worse this situation. Many victims of theft are social media who do not know the procedures of security such as the use of double authentication, or do not understand how to report crimes in the same way as they are true. This condition results in many cases not being handled because the victim is late or does not report to the authorities.

In addition to internal factors, external challenges in the form of limited international cooperation in the enforcement of the law are also major problems. Some perpetrators of cybercrime operate from the jurisdiction of Indonesia, so that law enforcement is necessary to involve interstate cooperation through mechanisms such as the Mutual Legal Assistance (MLA) and the division of the Interpol cybercrime. However, coordination of the country's infrastructure sering memakan time yang sufficient lama because there are systemic differences hukum dan administrative procedures between countries.

Efforts to Increase the Effectiveness of Law Enforcement Against Perpetrators of Social Media Account Theft

To increase the success of the implementation of the law in the face of theft in social media, strategic steps that cover the rules, institutions, and community awareness are needed (Ramadani, 2023).

First, the improvement of the ability of law enforcement apparatus in the field of forensics and digital technology must be the main focus. This can be achieved through continuous training programs, certification for cyber investigators, collaboration with international institutions such as Interpol Digital Crime Centre and Cyber Capacity Development Project ASEAN (Putra, 2023). Second, it is necessary to have further regulations from the UU ITE which are specifically to discuss criminal acts of theft in the social media to avoid ambiguity of norms. Rules in are expected to provide an explanation of the "illegal access to digital information" dan and reinforce the punishment for perpetrators who use akun for fraud, the dissemination of false information, or defamation of the name of the person (Rahmawati dan Prakoso, 2022). Third, digital literacy, society, must be improved, as a whole, through government initiatives, education, and social media. Education about cyber security, protection of personal data, use of authentication ganda must be part of the national movement of literasi digital (Kominfo, 2023). Fourth, need to strengthen the cooperation of various institutions between the Ministry of Communication and Informatics, the Police, the Authority of the Financial Service (OJK), and the provision of internet services and banking. Collaboration in is very important in overcoming crimes that use social media for financial fraud or illegal transactions (Bareskrim Polri, 2022).

These steps are expected to increase the effectiveness of law enforcement and strengthen the national digital security ecosystem which is more responsive to the threat of cybercrime.

4. Conclusions

Based on the findings of the research, it was concluded that the act of stealing social media access including in the category of access without permission was entered in Article 30 of Law No. 11 of 2008 concerning Information and Electronic Transactions. Although it has a clear legal foundation, its application is in the field of law and it faces a number of challenges, especially with the evidence of digital technology and the limitations of the technical capabilities of law enforcement.

To increase the effectiveness of law enforcement related to cybercrime, it is necessary to take strategic steps such as increasing capacity in the field of digital forensics, strengthening regulations and regulations in accordance with technological developments, and improving understanding of digital technology in the community. Work together between the government, law enforcement apparatus, community and society is very important to build a digital security ecosystem that is kokoh dan fair.

Thus, the implementation of legal sanctions against the perpetrators of theft in social media is expected not only to create a deterrent effect, but also to strengthen the protection of the law for users of technology di digital era.

Refferences

Arief, B. N. (2010). *Crime and law enforcement in Indonesia*. Jakarta: Kencana Prenada Media.

Arief, B. N. (2010). *Cybercrime action (cybercrime)*. Jakarta: RajaGrafindo Persada.

Bareskrim Polri. (2022). *Report on the handling of social media account theft cases in Indonesia in 2022*. Jakarta: Directorate of Cyber Crime.

Faculty of Social and Political Sciences, University of Indonesia. (2023). *Cybercrime: Types of crimes that are increasing significantly in Indonesia*. Retrieved from https://fisip.ui.ac.id

Institut Pemerintahan Dalam Negeri. (2023). *Cybercrime and legal enforcement challenges in the digital era*. Retrieved from https://ejournal.ipdn.ac.id/konstituen/article/view/3208

Kompas Nasional. (2022). *Cybercrime: Definition, characteristics, and causal factors*. Retrieved from https://nasional.kompas.com/read/2022/09/16/02400071/kejahatan-siber-pengertian-karakteristik-dan-faktor-penyebabnya

Ministry of Communication and Information Technology of the Republic of Indonesia. (2021). *Digital literacy report Indonesia 2021*. Jakarta: Kominfo.

Ministry of Communication and Information Technology of the Republic of Indonesia. (2021). *Annual report on digital literacy and cybercrime in Indonesia*. Jakarta: Kominfo.

Ministry of Communication and Information Technology of the Republic of Indonesia. (2022). *Law on personal data protection and its implementation in digital infrastructure*. Jakarta: Kominfo.

Ministry of Communication and Information Technology of the Republic of Indonesia. (2023). *Annual report on handling cybercrime cases and digital literacy in Indonesia*. Jakarta: Kominfo.

Nasrullah, R. (2015). *Social media: Communication, cultural, and sociotechnological perspectives*. Bandung: Simbiosa Rekatama Media.

Nasution, C. (2020). Jurisprudence model of media literacy in analyzing hoax information on social media. *Journal of Responsive Jurisprudence, 7*(2), 157–170.

Nurhalimah, D. (2021). Kajian hukum terhadap pencurian akun media sosial dalam perspektif UU ITE. *Jurnal Hukum Siber Indonesia, 5*(2), 65–80.

Polda Kepulauan Riau. (2023). *Definisi dan motif cybercrime*. Retrieved from https://pid.kepri.polri.go.id/definisi-dan-motif-cybercrime-2

Putra, R. A. (2023). Analysis of the effectiveness of criminal sanctions against cybercrime in Indonesia. *Journal of Applied Journalism and Digital Technology, 4*(2), 77–90.

Rahardjo, S. (2006). *Hukum dan masyarakat*. Bandung: Sinar Baru.

Rahmawati, L., & Prakoso, B. (2022). UU ITE sebagai alat hukum dalam penanggulangan cybercrime di Indonesia. *Journal of National Law and Cybersecurity, 3*(1), 55–68.

Rahmayanti, Y. A., & Rahtan, A. (2020). Judicial review terkait manipulasi data elektronik oleh pengemudi GrabCar (Putusan No. 853/Pid.Sus/2018/PN MKS). *Jurnal Mercatoria, 13*(2), 118–130.

Ramadani, S. (2023). Kajian hukum tindak pidana penipuan online ditinjau dari UU No. 19 Tahun 2016 tentang ITE. *International Journal of Society and Law, 1*(1).

Ramdani, M., & Kurniawan, A. (2023). Cybercrime dan perlindungan data pribadi di Indonesia. *Journal of Criminology and Information Technology, 9*(1), 21–34.

Sahlepi, M. A. (2023). Tinjauan yuridis terhadap tindak pidana penipuan online berdasarkan UU No. 19 Tahun 2016 tentang ITE. *INNOVATIVE: Journal of Social Science Research, 3*(6), 1402–1412.

Sakina, P. Y., Fikri, R. A., & Sahlepi, M. A. (2025). Perlindungan hukum terhadap korban ancaman dalam pinjaman online (Analisis Putusan No. 438/Pid.Sus/2020/PN Jkt.Utr). *INNOVATIVE: Journal of Social Science Research, 5*(3), 6905–6918.

Saputra, R., & Wibowo, H. (2022). Analysis of social media account security based on user behavior in Indonesia. *Journal of Technology and Cyber Security, 4*(3), 55–68.

Setiadi, A. (2020). Analisis kriminologis terhadap kejahatan di dunia maya. *Jurnal Ilmiah Hukum, 7*(2), 115–128.

Simanjuntak, F. (2019). Dampak pencurian akun media sosial terhadap perlindungan data pribadi. *Jurnal Hukum Siber Indonesia, 3*(1), 45–58.

Siregar, F., & Ardiansyah, M. (2023). Analysis of lex specialis principles in cybercrime law enforcement. *Jurnal Ilmiah Hukum dan Teknologi Informasi, 5*(2), 40–53.

Supreme Court of the Republic of Indonesia. (2021). *Decision No. 178/Pid.Sus/2021/PN Jkt.Sel regarding illegal access in social media accounts*. Jakarta: Directorate of Supreme Court Decisions.

Sutanto, Y. (2021). Keterkaitan Pasal 362 KUHP dengan pencurian data dan akun digital di era siber. *Jurnal Kriminologi Indonesia, 8*(1), 101–115.

Sutarman. (2012). *Cybercrime: Cara kerja dan cara mengatasinya*. Jakarta: Pustaka Reka Cipta.

Tuju, M. C., Ramadani, S., & Nasution, C. (2025). Law enforcement against cybercrime related to online marketplace fraud from a criminological perspective. *INNOVATIVE: Journal of Social Science Research, 5*(2), 1763–1776.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Widyarto, T. (2018). Forensik digital dan tantangan dalam penegakan hukum di Indonesia. *Jurnal Keamanan Siber dan Hukum, 5*(1), 33–47.

Widyarto, T. (2021). Forensik digital dan kendala pembuktian dalam kasus kejahatan siber di Indonesia. *Jurnal Keamanan Siber dan Hukum, 6*(1), 22–39.