



ISSN 2809-672X (Online)
IUS POSITUM: Journal of Law Theory and Law Enforcement

<https://journal.ifpublisher.com/index.php/jlte>

Vol. 4 Issue 1, January 2025

doi.org/10.56943/jlte.v4i1.754

Penalty Against Phone Credit Hacking through the 'Isi Pulsa Massal.exe' Application

Poppi Rahmawati^{1*}, Sri Priyati²

¹poppirahmawati27@gmail.com, ²priyati@ubhara.ac.id

Faculty of Law, Universitas Bhayangkara Surabaya

*Corresponding Author: Poppi Rahmawati

Email: poppirahmawati27@gmail.com

ABSTRACT

Cyber crime is defined as a type of crime related to the misuse of information technology. The causes include unrestricted internet access, as well as negligence from users. In Indonesia, the increase in cyber attacks and data hacking cases in the past year according to the National Cyber Security Index report and Reboot Digital PR Service is the worst cybersecurity country in Asia with a cyber danger score of 82.5 out of 100. Using normative legal research using secondary data including laws, judicial decisions, legal theories. As well as with the Legislative Approach which is carried out by examining all relevant laws and regulations and the Case Approach which is carried out by examining cases related to the issues at hand and court decisions. Law Number 11 of 2008 concerning Electronic Information and Transactions or commonly called the ITE Law has special rules regarding the use of information technology, in the discussion of cybercrime. In hacking through artificial applications, especially hacking the credit balance of an individual can be subject to criminal sanctions, such as the case, two people from Wonosobo, Central Java named Abdul Aziz and Tahyan, have been caught by the Special Investigation Directorate team or Ditreskrimsus at the South Kalimantan Police (KalSel). Criminalization of credit balance hacking through artificial applications can be applied by. ionally, challenges such as a shortage of police personnel and insufficient public outreach on traffic law compliance contribute to the system's inefficiency.

Keyword: Cyber, Electronic, Hacking

INTRODUCTION

In the development of human life, many changes have occurred in the era of globalization, particularly during the industrial revolution 5.0. This globalization era represents a social process that removes geographic boundaries in the economy, politics, society, and cultural norms.¹ As the use of internet technology continues to grow, new challenges arise in the protection of personal data, especially regarding the collection, utilization, and distribution of individual personal data.² Alongside technological advancements, cyber threats have evolved and will continue to be an ongoing issue.

Cybercrime can be defined as a type of crime related to the misuse of information technology without boundaries, and it is closely tied to technological advancements, relying on high-security measures and the assessment of information accessed by internet users. In general, cybercrime refers to criminal activities that utilize computers, based on advancements in digital technology. Factors contributing to the occurrence of cybercrime include, among others, unlimited internet access, negligence by computer users, ease of execution with low security risks, and inadequate network security systems.³

Recently, the state of cyber data in Indonesia has attracted attention due to the increase in cyberattacks and data hacking cases over the past year. According to reports from the National Cyber Security Index and Reboot Digital PR Service, Indonesia is one of the countries with the worst cyber security in Asia, receiving a cyber danger score of 82.5 out of 100. During the third quarter of 2022, 12.74 million accounts in Indonesia were hacked, making Indonesia the third country with the most data breaches in the world. From 2021 to 2022, cybercrime increased by 14 times. Data from e-MP Robinopsal Bareskrim Polri shows that the police handled 8,831 cybercrime cases from January 1 to December 22, 2022. The Metro Jaya Regional Police handled the most cases, with 3,709 cases, while in 2021, the total number of cases handled across Indonesia was 612.⁴

Various types of criminal hacking offenses that have occurred in Indonesia share a common goal, which is to benefit the perpetrators by obtaining personal data, credit balances, and even draining the bank accounts of the victims. Hacking

¹ Wisnu Prabowo, Satriya Wibawa, and Fuad Azmi, "Perlindungan Data Personal Siber di Indonesia," *Padjadjaran Journal of International Relations* 1, no. 3 (January 31, 2020): 218–39, <https://doi.org/10.24198/padjir.v1i3.26194>.

² 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 (July 15, 2020), <https://jca.esaunggul.ac.id/index.php/law/article/view/6>.

³ Issha Harruma, "Kejahatan Siber: Pengertian, Karakteristik Dan Faktor Penyebabnya," *Kompas.com*, 2022, <https://nasional.kompas.com/read/2022/09/16/02400071/kejahatan-siber--pengertian-karakteristik-dan-faktor-penyebabnya>.

⁴ Rumi Aulia Rahmanisa, Joyo Nur Suryanto Gono, and Tandiyu Pradekso, "Hubungan Terpaan Berita Peretasan Data dan Persepsi tentang Perlindungan Data dengan Citra Kementerian Komunikasi dan Informatika," *Interaksi Online* 11, no. 3 (June 15, 2023): 71–79.

comes in many forms and methods to access the victim's personal data. For instance, some perpetrators create a wedding invitation link, which is randomly sent to victims with a wedding invitation title. When the victim clicks the link, the hacker can easily access the victim's personal data, and the victim's bank account balance will be completely drained. Another method involves SMS/text messages offering a prize, which informs the victim that they have won a prize, along with a link and instructions to access the link to register as a winner. However, when the victim accesses the link, it is no different from the wedding invitation link method, as the victim is also hacked, and their bank account balance is drained. Additionally, one of the methods involves a QR code circulating in the market, purportedly for donations to orphans. Victims are prompted to scan the code, but in most hacking cases, this QR code can only hack the victim's bank account balance, resulting in the hacker draining the victim's entire bank account.

Hacking itself is an act of infiltrating digital systems and networks through illegal access to accounts or computer devices. Not all hacking activities are malicious and harmful, but many individuals misuse it for illegal activities and data breaches in cyberspace. Hacking involves the misuse of systems such as smartphones, computers, and network systems, leading to damage, the acquisition of personal data, the collection of victim information, and disruption of the victim's data activities.⁵

In 2021, there were approximately 193 hacking incidents, a 38% increase from the previous year, which had 147 hacking incidents. In 2023, hacking continued to evolve, with one of the methods involving hacking through a custom-made application designed to steal mobile credit balances, which trapped and harmed many victims. This hacking crime is part of cybercrime enabled by technological advances, as regulated in Article 28, Paragraph (1) of Law No. 19 of 2016 concerning Information and Electronic Transactions, which states that anyone who deliberately and unlawfully spreads false and misleading information that causes harm to consumers in electronic transactions is guilty.⁶

The process of determining punishment and the imposition of criminal sanctions is known as criminal sentencing. Typically, sentencing is a characteristic of punishment, which itself is a crime.⁷ Criminal sentencing can be defined as the process by which a judge imposes a criminal sentence on an individual proven

⁵ Fadhi Khoiru Nasrudin and Rosalinda Elsina Latumahina, "PERLINDUNGAN HUKUM TERHADAP KONSUMEN KARTU SIM YANG MENGALAMI KEBOCORAN DATA AKIBAT PERETASAN," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 2, no. 1 (April 30, 2022): 331–43, <https://doi.org/10.53363/bureau.v2i1.137>.

⁶ Vika Azkiya Dihni, "Peretasan, Bentuk Serangan Digital Paling Banyak Terjadi di Indonesia pada 2021 | Databoks," databoks, 2022, <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/f062c5cb0a427ac/peretasan-bentuk-serangan-digital-paling-banyak-terjadi-di-indonesia-pada-2021>.

⁷ Failin Alin, "SISTEM PIDANA DAN PEMIDANAAN DI DALAM PEMBAHARUAN HUKUM PIDANA INDONESIA," *JCH (Jurnal Cendekia Hukum)* 3, no. 1 (September 28, 2017): 14–31, <https://doi.org/10.33760/jch.v3i1.6>.

guilty of committing a criminal offense.⁸ Criminal law is one aspect of the legal system of a country. According to Van Kan Hamel, a criminal (or straf) is a punishment imposed with the appropriate authority as a factor of the general legal rules of the state for the offender, in the event that the offender disregards the legal order that must be enforced by the state.⁹

Based on the principles outlined above, the author finds it necessary to analyze the legal aspects of this case and to address it in a thesis entitled 'Criminal Sentencing Against Mobile Credit Balance Hacking Through the Custom-Made Application "ISI PULSA MASAL.exe".'

LITERATURE REVIEW

Criminal Sentence

According to Barda Nawawi Arief, if the definition of criminal sentencing is broadly seen as the process of granting or imposing a criminal penalty by a judge, it can be said that the criminal sentencing system encompasses all legislative provisions that regulate how criminal law is established or enforced clearly, so that an individual can be subjected to criminal sanctions. This means that all legislative norms concerning substantive criminal law, procedural criminal law, and the execution of criminal penalties can be regarded as a unified form of criminal sentencing.¹⁰ Unlike the previous definition, Barda Nawawi Arief argues that statutory rules or *the statutory rules* are limited to substantive criminal law as outlined in the Indonesian Criminal Code (KUHP), including both general and specific provisions concerning the formulation of criminal acts, which fundamentally constitute a unified form of criminal sentencing.¹¹

Hacking

Hacking refers to the activity of breaking into computers and systems, either with or without permission, and is done illegally. An individual who engages in this activity is called a hacker. Hacking itself is an act of infiltrating digital systems and networks through illegal access to accounts or computer devices. Not all hacking activities are malicious and harmful, but many individuals misuse it for illegal activities and data breaches by cybercriminals. Hacking involves the misuse of systems such as smartphones, computers, and network systems, causing damage,

⁸ Tomi Wicaksono Putra, HAMidah Abdurrahman, and Achmad Irwan Hamzani, *Pertanggungjawaban Pidana Terhadap Kejahatan Hacking* (Pekalongan: Penerbit NEM, 2023).

⁹ Feibi Kamu, Herlyanty Bawole, and Marcel Maramis, "Pemberlakuan Ketentuan Pidana Apabila Melakukan Tindak Pidana Di Bidang Industri Pertahanan," *LEX CRIMEN* 12, no. 3 (June 5, 2023), <https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/48533>.

¹⁰ Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana* (Prenada Media, 2016).

¹¹ Arief.

taking personal data, collecting victim information, and disrupting the victim's data activities.¹²

Phone Credit

Phone credit refers to the content and electronic payment tool in the modern globalization era, which can be easily found today. Even in payment methods, phone credit is very advantageous, as users can make payments for electricity tokens, internet access, and other payments using phone credit as one of the alternatives in contemporary payment methods. In this era, mobile phones are the main communication tools used by everyone and are most commonly found across all segments of society. This device is used to pay for phone or credit charges. Credit charges can be paid in advance (prepaid) or after use (postpaid). Postpaid credit can be purchased in the form of physical and non-physical vouchers. Physical vouchers involve the process of recharging credit by using a card containing a code, while non-physical vouchers involve the process of recharging credit directly through payment via transfer with electronic signals.¹³

Custom-Made Mobile Application

Custom-made applications, or commonly referred to as mobile applications, are software applications designed to run on mobile phones. Custom-made applications are useful to provide users with the same services available on a PC. An application, in general, is a small unit of software with a very limited load. Custom-made applications are far different from general software programs typically found on PCs. Unlike earlier versions, each application offers limited functionalities such as games, calculators, and mobile web browsing. Although early mobile applications were largely limited by hardware resources and therefore avoided multitasking, their main advantage today is their ability to provide users with the freedom to choose what they want to do next on their devices.¹⁴

According to Pressman and Bruce, mobile applications are applications specifically created for mobile platforms (e.g., iOS, Android, or Windows Mobile). Mobile applications often have their own user interface (UI) mechanisms, provided by the mobile media, interoperability with web-based resources offering access to various information related to the application, and local processing capabilities for data collection, analysis, and formatting, making them suitable for mobile platforms.¹⁵

¹² Nasrudin and Latumahina, "PERLINDUNGAN HUKUM TERHADAP KONSUMEN KARTU SIM YANG MENGALAMI KEBOCORAN DATA AKIBAT PERETASAN."

¹³ Ika Inayati, "Pulsa Elektronik atau Pulsa Elektrik?," March 27, 2025, <https://kantorbahasababel.kemdikbud.go.id/info/info-bahasa/pulsa-elektronik-atau-pulsa-elektrik/>.

¹⁴ Yusuf Wahyu Setiya Putra et al., *PENGANTAR APLIKASI MOBILE* (Penerbit Widina, 2023).

¹⁵ Jainuri, Nurasih, and Yulita Hermilasari, "PERANCANGAN DAN PEMBUATAN APLIKASI MOBILE POINT OF SALE PADA OUTLET MAKARONI JUDES BERBASIS ANDROID," *Insan Pembangunan Sistem Informasi Dan Komputer* 9, no. 2 (December 2021): 44–52, <https://doi.org/10.58217/ipsikom.v9i2.201>.

RESEARCH METHODOLOGY

This research uses a normative legal research approach, prioritizing the use of secondary data such as laws, court decisions, and legal theories. Normative legal research aims to examine the legal norms contained in legislation and legal decisions, as well as to study relevant legal concepts within the context of the issues being investigated.¹⁶

In this study, two main approaches are used: the Legislative Approach and the Case Approach. The Legislative Approach is carried out by reviewing and analyzing all relevant regulations related to the research topic. This approach aims to understand the legal norms found in the applicable laws and regulations, as well as their legal implications.¹⁷ Additionally, this approach also includes an examination of the legal policies contained in laws or other regulations that may influence the issue being studied.

Furthermore, the Case Approach is applied by conducting an in-depth review of legal cases relevant to the issue being discussed. This approach involves analyzing court decisions related to the legal problem being studied. By examining court rulings, the researcher can gain insights into how the law is applied in practice and the interpretation provided by judges regarding the regulations in the context of the case.

This research method allows for a deeper understanding of the prevailing legal norms, as well as how the law is applied in real-life cases, which ultimately can contribute to the development of legal theory and practice in Indonesia.

RESULT AND DISCUSSION

Regulation of Hacking Offenses Using Custom-Made Applications: Indonesia's Hacking Regulations

In Law No. 27 of 2022 concerning Personal Data Protection (UU PDP), Personal Data is defined as data concerning an individual who is identified or can be identified manually or by combining it with other information, either directly or indirectly through electronic and non-electronic processes.¹⁸ Additionally, Minister of Communication and Information Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems states that Personal Data refers to certain

¹⁶ Muhammad Ishar Helmi, "Pengaruh Teori Hukum Dan Implementasinya Dalam Sistem Hukum Di Indonesia," *SALAM: Jurnal Sosial Dan Budaya Syar-i* 9, no. 6 (October 24, 2022): 1859–70, <https://doi.org/10.15408/sjsbs.v9i6.28735>.

¹⁷ Dr Jonaedi Efendi M.H S. H. I. and Prof Dr Johnny Ibrahim M.Hum S. H. , S. E. , M. M., *Metode Penelitian Hukum: Normatif dan Empiris* (Prenada Media, 2018).

¹⁸ Republik Indonesia, "Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," Pub. L. No. 27, 1 1 (2022).

individual data that is maintained, stored, and protected for its accuracy and confidentiality.¹⁹

Cybercrime Offenses Using Custom-Made Applications

Indonesia has legal provisions regulating law enforcement efforts through preventive measures for all forms of crimes related to computers, particularly in the cyber domain. It is essential to review the existing laws, such as the Criminal Code (KUHP) and other regulations outside of the KUHP. Incorporating these provisions into the existing legal framework can help prevent and mitigate excessive or far-reaching crimes.²⁰

Before the enactment of Law No. 11 of 2008 concerning Information and Electronic Transactions, commonly referred to as the ITE Law, there were specific regulations regarding the use of information technology. In discussing cybercrimes, there was no legal gap, as Indonesian criminal law applies an interpretive approach known in legal science, which forms the basis for law enforcement against actions with new aspects that are not specifically regulated by law. In such cases, the Criminal Code (KUHP) is applied to crimes in cyberspace, commonly referred to as internet crimes.

Criminal Sentencing Provisions According to the Indonesian Criminal Code

The Indonesian Criminal Code does not provide specific explanations regarding intent and guidelines for criminal sentencing. Therefore, criminal penalties are defined based on the perspectives of law enforcement officers and the judiciary, who may hold individual opinions. In the Criminal Code, penalties are also characterized as rigid, which means that it is unlikely that the penalty will transform in response to changes or developments in the offender's stance. The sentencing process outlined in the Criminal Code clearly shows that it does not grant judges the authority to select appropriate penalties for a criminal offender. When deciding or applying the basis for penalizing an act, the Criminal Code has a positivist characteristic, meaning that it must be accompanied by a law or the principle of formal legality. As such, the Criminal Code is reluctant to provide a platform for evolving laws within society, as implicitly stated in the law itself. Therefore, in the context of societal knowledge, the Criminal Code is considered

¹⁹ Menteri Komunikasi, "Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik," Pub. L. No. 20 (2016).

²⁰ Febbi Citra Halifah, Panji Kusuma Prasetyanto, and Jalu Aji Prakoso, "ANALISIS KONSEKUENSI PEMBANGUNAN EKONOMI AKIBAT KEJAHATAN DI INDONESIA," *DINAMIC : Directory Journal of Economic* 3, no. 2 (2021): 492–506, <https://doi.org/10.31002/dinamic.v3i2.2669>.

outdated and does not align with the evolving quality of law within the community.²¹

Criminal Sentencing for Hacking through Custom-Made Application

In cases of hacking through custom-made applications, particularly when hacking an individual's phone credit, the offender may face criminal penalties. An example of this is the case of two individuals from Wonosobo, Central Java, named Abdul Aziz and Tahyan, who were apprehended by the Special Criminal Investigation Directorate (Ditreskrimsus) of the South Kalimantan Police (Polda KalSel). They were arrested after executing their scheme by hacking the server or network of a credit agent in Pelaihari, South Kalimantan. By hacking the network of a credit agent in Pelaihari, Tanah Laut, the perpetrators successfully gained a profit of IDR 50,000,000.00 (fifty million rupiahs).

At the time of their arrest, the perpetrators were actively hacking the network of a credit agent named Duta Pulsa Pelaihari. The perpetrators breached the Android application system called DigiPos using the victim's personal account, Imanudin. This operation began after a report was made by the credit agent, the victim of the hacking, and following the report, the Ditreskrimsus team of Polda KalSel immediately conducted an investigation leading to the arrest of the two perpetrators.

After successfully breaching the network, the perpetrators freely transferred the phone credit to SIM cards via transfer to a designated handler. As a result, the perpetrators earned IDR 205,000,000.00 (two hundred five million rupiahs). It is suspected that the perpetrators had been carrying out their criminal activities for months, which was only realized by the victim after reviewing the transaction history on their personal credit application. Upon review, the victim realized that their phone credit balance had decreased by IDR 57,000,000.00 (fifty-seven million rupiahs).

Interestingly, the perpetrators did not reside in Banjarmasin but in Wonosobo, Central Java, at the time of committing the crime. The perpetrators deceived the victim by creating a custom-made application that allowed them to transfer the victim's phone credit balance to themselves. The results from hacking the victim's phone credit were then sold to potential buyers online and through vouchers.

As a result of their actions, law enforcement seized evidence, including ATM cards, the perpetrators' personal bank books, 60 SIM cards, 1 computer, 1 modem, and cash amounting to IDR 74,000,000.00 (seventy-four million rupiahs), 1 mobile phone, and a transaction book for credit sales.²²

²¹ Badan Pembinaan Hukum Nasional, *Perencanaan Pembangunan Hukum Nasional Bidang Hukum Pidana Dan Sistem Pemidanaan (Politik Hukum Dan Pemidanaan)* (Jakarta: Kementerian Hukum dan HAM Republik Indonesia, 2010).

²² Muhammad Risanta, "Bobol Server Distributor Pulsa, 2 Hacker Asal Jateng Diciduk Polda Kalsel," *detiknews*, 2020, <https://news.detik.com/berita/d-5252310/bobol-server-distributor-pulsa-2-hacker-asal-jateng-diciduk-polda-kalsel>.

For their actions, the perpetrators were charged under Article 30, Paragraph (1) of Law No. 11 of 2008, amended by Law No. 19 of 2016, which states that anyone who intentionally and unlawfully accesses another person's computer or electronic system in any manner shall be sentenced to a maximum of 6 years in prison and a fine of up to IDR 600,000,000.00 (six hundred million rupiahs).²³

They were also charged under Article 46, Paragraph (1) of Law No. 11 of 2008, amended by Law No. 19 of 2016, which stipulates that anyone who meets the criteria outlined in Article 30, Paragraph (1) shall be sentenced to a maximum of 6 years in prison and a fine of up to IDR 600,000,000.00 (six hundred million rupiahs).²⁴

CONCLUSION

Based on the discussion outlined in this thesis, the author can draw several conclusions, which also address the problem formulation presented. First, the modus operandi of criminal acts aimed at gaining personal profit can violate regulations concerning the leakage of personal data, as stipulated in Law No. 27 of 2022 on Personal Data Protection (UU PDP) and Law No. 19 of 2016 on Electronic Information and Transactions, as amended by Law No. 11 of 2008. These regulations mandate criminal penalties for cybercrimes and emphasize the importance of understanding the various types of hacking that are increasingly prevalent, fostering public awareness as detailed in Articles 28 (1), 46 in conjunction with Article 30, Article 48 in conjunction with Article 32, Article 34 (1), and Article 26 in conjunction with Article 30. Second, the Indonesian Penal Code (KUHP) provides guidelines for penalizing hackers, ensuring that penalties are imposed based on the rigid and fixed nature of the code. Additionally, criminal penalties for hacking prepaid balances through modified applications can be applied under Article 362 of the KUHP, which addresses theft. The implementation of sanctions for hacking offenses, as demonstrated through case studies and the application of relevant articles, serves to provide public security and a deterrent effect on offenders. In these instances, the offenders are subject to sanctions based on principles of responsibility, justice, discretion, and professionalism.

REFERENCES

Alin, Failin. "SISTEM PIDANA DAN PEMIDANAAN DI DALAM PEMBAHARUAN HUKUM PIDANA INDONESIA." *JCH (Jurnal Cendekia Hukum)* 3, no. 1 (September 28, 2017): 14–31. <https://doi.org/10.33760/jch.v3i1.6>.

²³ H. Adami Chazawi and Ardi Ferdian, *Tindak Pidana Informasi Dan Transaksi Elektronik Ed. Revisi*, Revisi (Malang: Media Nusa Creative (MNC Publishing), 2022).

²⁴ Ahmad M. Ramli, "Aturan Akses Ilegal dan Penyadapan dalam KUHP Baru," *KOMPAS.com*, March 5, 2023, <https://nasional.kompas.com/read/2023/03/05/10105771/aturan-akses-ilegal-dan-penyadapan-dalam-kuhp-baru>.

- Arief, Barda Nawawi. *Bunga Rampai Kebijakan Hukum Pidana*. Prenada Media, 2016.
- Badan Pembinaan Hukum Nasional. *Perencanaan Pembangunan Hukum Nasional Bidang Hukum Pidana Dan Sistem Pemidanaan (Politik Hukum Dan Pemidanaan)*. Jakarta: Kementrian Hukum dan HAM Republik Indonesia, 2010.
- Chazawi, H. Adami, and Ardi Ferdian. *Tindak Pidana Informasi Dan Transaksi Elektronik Ed. Revisi*. Revisi. Malang: Media Nusa Creative (MNC Publishing), 2022.
- Dihni, Vika Azkiya. "Peretasan, Bentuk Serangan Digital Paling Banyak Terjadi di Indonesia pada 2021 | Databoks." databoks, 2022. <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/f062c5cb0a427ac/peretasan-bentuk-serangan-digital-paling-banyak-terjadi-di-indonesia-pada-2021>.
- Halifah, Febbi Citra, Panji Kusuma Prasetyanto, and Jalu Aji Prakoso. "ANALISIS KONSEKUENSI PEMBANGUNAN EKONOMI AKIBAT KEJAHATAN DI INDONESIA." *DINAMIC: Directory Journal of Economic* 3, no. 2 (2021): 492–506. <https://doi.org/10.31002/dinamic.v3i2.2669>.
- Harruma, Issha. "Kejahatan Siber: Pengertian, Karakteristik Dan Faktor Penyebabnya." Kompas.com, 2022. <https://nasional.kompas.com/read/2022/09/16/02400071/kejahatan-siber--pengertian-karakteristik-dan-faktor-penyebabnya>.
- Inayati, Ika. "Pulsa Elektronik atau Pulsa Elektrik?," March 27, 2025. <https://kantorbahasababel.kemdikbud.go.id/info/info-bahasa/pulsa-elektronik-atau-pulsa-elektrik/>.
- Jainuri, Nurashia, and Yulita Hermilasari. "PERANCANGAN DAN PEMBUATAN APLIKASI MOBILE POINT OF SALE PADA OUTLET MAKARONI JUDES BERBASIS ANDROID." *Insan Pembangunan Sistem Informasi Dan Komputer* 9, no. 2 (December 2021): 44–52. <https://doi.org/10.58217/ipsikom.v9i2.201>.
- Kamu, Feibi, Herlyanty Bawole, and Marcel Maramis. "Pemberlakuan Ketentuan Pidana Apabila Melakukan Tindak Pidana Di Bidang Industri Pertahanan." *LEX CRIMEN* 12, no. 3 (June 5, 2023). <https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/48533>.
- Menteri Komunikasi. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, Pub. L. No. 20 (2016).
- Nasrudin, Fadhi Khoiru, and Rosalinda Elsinia Latumahina. "PERLINDUNGAN HUKUM TERHADAP KONSUMEN KARTU SIM YANG MENGALAMI KEBOCORAN DATA AKIBAT PERETASAN." *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 2, no. 1 (April 30, 2022): 331–43. <https://doi.org/10.53363/bureau.v2i1.137>.
- Prabowo, Wisnu, Satriya Wibawa, and Fuad Azmi. "Perlindungan Data Personal Siber di Indonesia." *Padjadjaran Journal of International Relations* 1, no. 3 (January 31, 2020): 218–39. <https://doi.org/10.24198/padjir.v1i3.26194>.
- Putra, Tomi Wicaksono, HAmidah Abdurrachman, and Achmad Irwan Hamzani. *Pertanggungjawaban Pidana Terhadap Kejahatan Hacking*. Pekalongan: Penerbit NEM, 2023.

- Putra, Yusuf Wahyu Setiya, Aisyah Mutia Dawis, Novi Novi, Fauzan Natsir, Fitria Fitria, Anak Agung Sandatya Widhiyanti, Firman Noor Hasan, Somantri Somantri, and Maniah Maniah. *PENGANTAR APLIKASI MOBILE*. Penerbit Widina, 2023.
- Rahmanisa, Rumi Aulia, Joyo Nur Suryanto Gono, and Tandiyo Pradekso. "Hubungan Terpaan Berita Peretasan Data dan Persepsi tentang Perlindungan Data dengan Citra Kementerian Komunikasi dan Informatika." *Interaksi Online* 11, no. 3 (June 15, 2023): 71–79.
- Ramli, Ahmad M. "Aturan Akses Ilegal dan Penyadapan dalam KUHP Baru." *KOMPAS.com*, March 5, 2023. <https://nasional.kompas.com/read/2023/03/05/10105771/aturan-akses-ilegal-dan-penyadapan-dalam-kuhp-baru>.
- Republik Indonesia. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pub. L. No. 27, 1 1 (2022).
- Risanta, Muhammad. "Bobol Server Distributor Pulsa, 2 Hacker Asal Jateng Diciduk Polda Kalsel." *detiknews*, 2020. <https://news.detik.com/berita/d-5252310/bobol-server-distributor-pulsa-2-hacker-asal-jateng-diciduk-polda-kalsel>.
- Satrio, Muhamad Bayu, 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 (July 15, 2020). <https://jca.esaunggul.ac.id/index.php/law/article/view/6>.