Jurnal Ilmu Hukum Tambun Bungai
Vol. 8, No. 2, December 2023, 344-355
P-ISSN: 2502-9541 E-ISSN: 2685-9386
Published by Sekolah Tinggi Ilmu Hukum Tambun Bungai Palangka Raya

# HACKING AS A CHALLENGE FOR CHANGE AND THE DEVELOPMENT OF CYBER LAW IN INDONESIA

**Jay Sadikin Abdul Azis Mandala Putra**

*Muhammadiyyah University of Palangka Raya*
*Palangka Raya, Central Kalimantan, Indonesia*
jaysadikin49@gmail.com



| | | | |
|---|---|---|---|
| Submitted | : 2023-10-05 | Accepted | : 2023-10-13 |
| Revision | : 2023-10-13 | Publish | : 2023-12-15 |

***Abstract***: *This research explores the legal provisions for hacking as a cyber crime in Indonesia with a focus on the legal framework for hacking, criminal acts of hacking, and the challenges faced in dealing with changes and developments in cyber law. Indonesia's hacking legal framework, which primarily consists of the Information and Electronic Transactions Law (UU ITE), creates an important legal foundation for dealing with hacking. However, there are shortcomings in legal provisions that must be updated regularly to keep up with technological developments and increasingly sophisticated hacking tactics. This research aims to analyze the legal provisions that regulate hacking as a cyber crime in Indonesia. This includes an understanding of relevant legislation, the implementation of the law, as well as the obstacles faced in law enforcement related to hacking. This research uses normative legal research methods. By understanding the legal framework for hacking, criminal acts of hacking, and the challenges of changing cyber law in Indonesia, this research aims to provide deeper insight into how this country faces the threat of hacking in an increasingly complex digital era. With ongoing improvements in the legal framework, increased law enforcement capacity, and better public awareness, Indonesia can be more effective in protecting its society and digital infrastructure from the threat of cybercrime.*

***Keywords*** *: legal provisions, hacking, cyber crime.*

## Introduction

Hacking is a serious problem that requires careful attention and handling from law enforcement officials and related institutions in Indonesia. If there are significant cases of hacking that have not yet been uncovered, it is important for authorities to conduct a thorough investigation to identify the perpetrators and prosecute them to the

fullest extent of the law.[1] In addition, awareness about cyber security and best practices in protecting personal data and computer systems are also very important in efforts to prevent future hacking cases.[2] Hacking as a challenge in the change and development of cyber law in Indonesia is very relevant in the context of an increasingly advanced digital era. Indonesia, like many other countries, has experienced a significant surge in the use of information and communication technology in various aspects of life. While this technological advancement brings great benefits, it also brings serious risks in the form of cybercrime, including hacking.[3]

The main challenge is that hacking is becoming more complex as technology develops. Hackers continue to innovate in their tactics and methods, and often evade detection by using sophisticated techniques. Indonesia, with its large and increasingly internet-connected population, is an attractive potential target for hackers.[4] The existing legal framework in Indonesia, such as the Information and Electronic Transactions Law (UU ITE), creates an important legal basis for dealing with hacking. However, the rapid advance of cybercrime raises questions about whether these legal provisions are responsive enough to evolving threats. A lack of understanding of cyber law and a lack of resources in cyber law enforcement are also challenges that need to be addressed.

The importance of this research lies in the need to understand and evaluate the effectiveness of existing legal provisions in dealing with hacking in the digital environment.[5] With the rapid development of technology, the law must be able to adapt and provide adequate protection against the threat of cyber crime. Therefore, this research will dig deeper into the legal framework that regulates hacking in Indonesia, as well as identify obstacles that may hinder law enforcement in the context of cyber

---

[1] Yogi Oktafian Arisandy, "Penegakan Hukum Terhadap Cyber Crime Hacker," *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 1, no. 3 (2021): 168, https://doi.org/10.18196/ijclc.v1i3.11264.

[2] Dwi Ayu Astrini, "Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman Cybercrime," *Lex Privatum* 3, no. 1 (2015).

[3] Aditama Candra Kusuma and Ayu Diah Rahmani, "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)," *SUPREMASI : Jurnal Hukum* 5, no. 1 (2022): 56, https://doi.org/10.36441/supremasi.v5i1.721.

[4] Bambang Hartono, "Hacker Dalam Perspektif Hukum Indonesia," *Masalah-Masalah Hukum* 43, no. 1 (2014): 23.

[5] Jefry Tarantang, Rahmad Kurniawan, and Gusti Muhammad Ferry Firdaus, "Electronic Money Sebagai Alat Transaksi Dalam Perspektif Islam," *An-Nisbah: Jurnal Ekonomi Syariah* 07, no. April (2020): 12, https://doi.org/https://doi.org/10.21274/an.2020.7.1.1%20-%2021.

crime.[6] With a better understanding of this, we can build a stronger foundation to protect the data, privacy and information security of Indonesian people in this increasingly complex digital era.[7]

Hackers are increasingly sophisticated in their actions, using advanced techniques to evade detection and capture. This phenomenon poses challenges for law enforcement officials and requires constant review and improvement in existing legal provisions.

People are increasingly aware of the importance of protecting their data and privacy in the digital world.[8] Hacking incidents involving theft of personal data have given rise to greater demand for strong legal provisions to protect individual rights.[9] Cybercrime often involves perpetrators from various countries. This phenomenon emphasizes the importance of international cooperation in cyber law enforcement and requires coordination in dealing with cross-border hacking.

The research method used in the study of hacking as a challenge in the change and development of cyber law in Indonesia will include a normative legal research approach and comprehensive qualitative analysis. This research method will provide a comprehensive understanding of hacking as a challenge in the change and development of cyber law in Indonesia, as well as challenges in law enforcement that need to be overcome. It is hoped that the data obtained can be used as a basis for improvements in the existing legal system to protect society from the growing threat of cyber crime. Through this research, it is hoped that better solutions can be found to protect Indonesia from the threat of cyber crime, strengthen existing legal provisions, and ensure effective law enforcement in dealing with hacking in this digital era.

**Legal Framework for Hacking in Indonesia**

Indonesia's hacking legal framework is critical to understanding how the country faces cybercrime challenges. This legal framework is based on various laws and

---

[6] Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *SASI* 27, no. 1 (2021): 51, https://doi.org/10.47268/sasi.v27i1.394.

[7] Jefry Tarantang et al., "Perkembangan Sistem Pembayaran Digital Pada Era Revolusi Industri 4.0 Di Indonesia," *Jurnal Al-Qardh* 4, no. 1 (2019): 71, https://doi.org/10.23971/jaq.v4i1.1442.

[8] Jefry Tarantang et al., "PERLINDUNGAN HUKUM TERHADAP NASABAH BANK DALAM TRANSAKSI DIGITAL," *Morality: Jurnal Ilmu Hukum* 9, no. 10 (2023): 23, https://doi.org/http://dx.doi.org/10.52947/morality.v9i1.321.

[9] Vincent Pane, Grace Tampongangoy, and Renny Nansy Koloay, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik," *Lex Privatum* XI, no. 2 (2023).

regulations that cover different aspects related to hacking. One of the key laws that plays a role in law enforcement related to hacking is Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE). The ITE Law is the main basis for regulating hacking in the digital sphere and contains articles that regulate legal sanctions against hacking perpetrators. Apart from the ITE Law, the Criminal Code (KUHP) also has relevant provisions related to hacking, especially in the context of data theft and illegal access to computer systems.[10] Criminal law also provides a legal basis for the prosecution of hacking perpetrators.

Furthermore, there are other regulations and policies issued by the government and related institutions, such as the Ministry of Communication and Information, which regulate certain aspects of cyber security and law enforcement related to hacking. This legal framework creates an important legal basis for dealing with hacking as a cyber crime in Indonesia. However, the challenge faced is the ability to keep up with technological developments and the legal adaptations needed to address increasingly sophisticated cybercrime threats. Therefore, evaluation and updating of this legal framework needs to be carried out continuously in order to be able to respond to rapidly developing cyber security challenges.[11]

Indonesia has developed an important legal basis for dealing with cybercrime. Law Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE) is the main pillar in regulating hacking and cyber security. The ITE Law provides a legal basis for law enforcement against hacking perpetrators, by regulating various illegal acts in the digital realm. Even though this legal framework already exists, the challenge faced is the ability to keep up with rapid technological developments. Cybercrime continues to develop and become more sophisticated, so legal provisions must always be updated and adapted. In addition, cyber law enforcement requires cooperation between various agencies and related parties, including the private sector, to overcome the threat of hacking.

---

[10] I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiartha, "Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)," *Jurnal Konstruksi Hukum* 1, no. 2 (2020): 34, https://doi.org/10.22225/jkh.2.1.2553.334-339.

[11] Amelia Widya Octa Kuncoro Putri et al., "Serangan Hacking Tools Sebagai Ancaman Siber Dalam Sistem Pertahanan Negara (Studi Kasus: Predator)," *Global Political Studies Journal* 6, no. 1 (2022): 36–37, https://doi.org/10.34010/gpsjournal.v6i1.6698.

Indonesia's hacking legal framework is an important first step in protecting society and digital infrastructure from the threat of cybercrime. However, continuous evaluation and updates in cyber laws and law enforcement are key in maintaining the country's cyber security.[12] Public awareness about the importance of cyber security is also very necessary to protect personal data and national interests from increasingly complex hacking attacks.

The legal framework for hacking in Indonesia has a number of shortcomings that need to be taken into account. One of the main shortcomings is the lack of provisions that are sufficiently detailed and responsive to technological developments. Cybercrime continues to evolve rapidly, and current laws may not always be able to address new and more sophisticated hacking tactics. Therefore, there needs to be ongoing efforts to update and improve existing legal provisions to make them more relevant to today's cybercrime challenges. Apart from that, the implementation of law in cyber law enforcement can also face obstacles. One of them is the lack of human resources who have special expertise in handling hacking cases. Training and capacity building in the field of cyber security is essential to ensure law enforcement officials have the necessary capabilities to handle complex hacking cases.[13]

Another shortcoming is the lack of optimal coordination between agencies involved in cyber law enforcement. Cybercrime often crosses borders, and cooperation between various law enforcement agencies and related parties, such as the private sector, can be more effective in addressing hacking threats. Public awareness about cyber security also needs to be increased. A lack of understanding of cybersecurity risks and practices can make individuals and companies more vulnerable to hacking. Therefore, education and public awareness campaigns about cybercrime need to be strengthened. By fixing these shortcomings, Indonesia's hacking legal framework can become more effective in protecting society and digital infrastructure from increasingly complex cybercrime threats.

---

[12] Irzak Yuliardy Nugroho, "Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia," *Al-Daulah: Jurnal Hukum Dan Perundangan Islam* 5, no. 1 (2015): 174, https://doi.org/10.15642/ad.2015.5.1.171-203.

[13] Asfarina Oktaviani and Emmilia Rusdiana, "Alternatif Pidana Bagi Pelaku Tindak Pidana Peretasan Di Indonesia Dalam Undang-Undang Informasi Dan Transaksi Elektronik," *Novum: Jurnal Hukum*, no. 11 (2023): 253.

**Hacking Crime in Indonesia**

The crime of hacking in Indonesia is a serious threat in the world of cyber crime. Hacking cases involve illegal access to a computer system or network, with the aim of stealing data, destroying information, or disrupting system operations. This criminal act of hacking includes various forms, such as hacking against companies, government institutions, individuals, and even large-scale cyber attacks on crucial infrastructure.[14]

The legal provisions governing criminal acts of hacking in Indonesia are mainly regulated in Law Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE). Articles in the ITE Law categorize various hacking acts as criminal acts, such as illegal access to computer systems, data theft, distribution of malware and other cyber attacks. Perpetrators who are found guilty may be subject to legal sanctions, including fines and prison sentences.[15] However, hacking can also involve cross-border cyber attacks, which require international cooperation in law enforcement. Indonesia has also participated in international efforts to tackle cybercrime, including cooperation with law enforcement agencies from other countries in the investigation and prosecution of hacking perpetrators.

Hacking crimes have serious impacts, including financial losses, theft of personal data, and threats to national security. Therefore, law enforcement and protection of computer systems and data are important priorities within the scope of cyber security in Indonesia.[16] Continuous evaluation of existing legal provisions and increased cyber law enforcement efforts are key to protecting the nation's society and digital infrastructure from increasingly sophisticated hacking threats.[17]

One example of a criminal hacking case that emerged in Indonesia is a hacking incident that occurred in 2021 which targeted the communications and information systems of the National Cyber and Crypto Agency (BSSN). In this case, a group of

---

[14] Ridwan Ridwan, Muhammad Nur, and Sulaiman S, "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan (Hacker) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik," *Jurnal Ilmiah Mahasiswa Fakultas Hukum Universitas Malikussaleh* 6, no. 1 (2023): 114, https://doi.org/10.29103/jimfh.v6i1.7007.

[15] Indah Sari, "Mengenal Hacking Sebagai Salah Satu Kejahatan Di Dunia Maya," *Jurnal Sistem Informasi Universitas Suryadarma* 10, no. 2 (2014): 172–73, https://doi.org/10.35968/jsi.v10i2.1086.

[16] Michael Leunard, Sari Mandiana, and Jusup Jacobus Setyabudhi, "Analisis Yuridis Tentang Peretasan Data Pribadi Penumpang Lion Air," *YUSTISIA MERDEKA : Jurnal Ilmiah Hukum* 6, no. 2 (2020): 55, https://doi.org/10.33319/yume.v6i2.51.

[17] Abd. Rahman Saleh, "Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana," *HUKMY : Jurnal Hukum* 1, no. 1 (2021): 107, https://doi.org/10.35316/hukmy.2021.v1i1.91-108.

hackers accessed BSSN's internal system and stole various confidential documents, including cybersecurity policy and strategy documents. This hacking action became a national concern because it exposed potential vulnerabilities in the Indonesian government's cybersecurity infrastructure. An investigation by law enforcement officials led to the arrest of several suspects involved in this hack. They were identified as part of an international hacker network that used various advanced techniques to access BSSN systems. This case is proof that hacking in Indonesia is not only carried out by individual perpetrators, but also by groups of hackers who have significant resources and technical capabilities.

The impact of this incident includes significant data loss, potential threats to national security, and cybersecurity system vulnerabilities that require remediation. This case also highlights the importance of cooperation between government and private institutions in mitigating the threat of hacking and the need for in-depth evaluation of existing legal provisions in cyber law enforcement in Indonesia.

Hacking crime in Indonesia is a serious problem and continues to grow for several main reasons. First, the rapid growth of information and communications technology has opened the door wide for hacking. The increasing number of devices connected to the internet and the use of digital technology in everyday life has provided greater opportunities for hacks to access sensitive data and systems.[18]

Second, financial gain is the main motivation behind many hacking cases. Hackers often seek material gain from their activities, such as theft of personal or company data that can be sold or financially exploited. This potential large reward encourages perpetrators to continue looking for loopholes in the security system.[19]

Third, challenges in cyber law enforcement are also a factor that influences the prevalence of hacking crimes. Cybercrime often crosses geographic boundaries and involves international networks, which makes it difficult to catch and prosecute. Additionally, a lack of specialized expertise in cyber law enforcement can be a barrier to investigating and pursuing hacking perpetrators.

---

[18] Ardiansyah, "ANALISIS YURIDIS TERHADAP SISTEM PEMBUKTIAN PADA KEJAHATAN PERETASAN SITUS WEBSITE," *JOM Fakultas Hukum Universitas Riau Volume* 6, no. 2 (2019): 3.

[19] Indriana Firdaus, "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan," *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (2022): 30, https://doi.org/10.52005/rechten.v4i2.98.

Fourth, some hackers are motivated by ideological or political motives, such as hacktivism or cyber attacks aimed at influencing policy or public opinion. This results in cyber attacks that can have a significant impact on the social and political order.[20]

Fifth, lack of awareness about cyber security and unsafe practices in using technology are also factors that cause hacking crimes. Many individuals and organizations do not sufficiently understand the risks and do not implement adequate security measures.

By understanding these reasons, further efforts can be developed to increase protection against cyber crime in Indonesia, including improvements in the legal framework, increasing public awareness, and developing cyber law enforcement capabilities. The development of cyber law in Indonesia must always be responsive to increasingly sophisticated hacking threats.[21] Hacking also often involves crossing borders, so international cooperation and close coordination between government and private institutions is essential. In addition, increasing public awareness about cyber security is also needed so that individuals and organizations can protect themselves from the threat of hacking.

**Hacking as a Challenge for Change and Development of cyber law in Indonesia**

New ideas in research regarding the legal provisions of hacking as a cyber crime in Indonesia can include several important aspects that enrich the understanding and relevance of this research. One of these ideas is an examination of changes and developments in cyber law in Indonesia in recent years. With the rapid rate of technological development, there is a need to evaluate the extent to which Indonesian law has adapted to new challenges in cybercrime.

Also worth considering in this case are the social, economic and political impacts of a successful hack.[22] This study can reveal the significant economic impact

---

[20] Tobing Musa Sahat et al., "Tinjauan Terhadap Modus-Modus Kejahatan Dalam Hukum Cyber Crime," *Jurnal Hukum Dan Sosial Politik* 1, no. 2 (2023): 60, https://doi.org/10.59581/jhsp-widyakarya.v1i2.239.

[21] 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 (2022): 332–33, https://doi.org/10.53363/bureau.v2i1.137.

[22] Nurul Khasanah and Tata Sutabri, "Analisis Kejahatan Cybercrime Pada Peretasan Dan Penyadapan Aplikasi Whatsapp," *Blantika : Multidisciplinary Journal* 2, no. 1 (2023): 46, https://doi.org/10.57096/blantika.v2i1.13.

that a cyberattack may have on a company, as well as the political and national security impacts that could occur if crucial systems are hit by a hack.[23] Through this approach, research will provide broader insight into the importance of cyber law enforcement for stability and economic growth in Indonesia. Furthermore, new ideas could also involve a review of the private sector's role in protecting themselves and their customers from hacking. This study can explain the responsibilities of companies related to cybersecurity, the best practices adopted by the private sector, and the obstacles they face in trying to protect their data and systems.

New ideas could detail possible solutions and recommendations that can be implemented to strengthen cyber law enforcement in Indonesia. This could include increasing cooperation between the public and private sectors, developing new policies that are more responsive to technological change, as well as efforts to increase public awareness about the threat of cybercrime.[24] By incorporating these new ideas into research, we can expand the scope of knowledge about hacking as a cyber crime in Indonesia, provide more concrete recommendations for improvements in the legal system and cyber law enforcement, and face increasingly complex cyber security challenges in the future.

Hacking is a challenge that continues to grow as cyber law changes and develops in Indonesia. Cyber law in Indonesia, such as the Information and Electronic Transactions Law (UU ITE), has undergone several changes over time to accommodate the increasingly sophisticated dynamics of cyber crime.[25] However, hackers also continue to adapt and create new methods to evade law enforcement. These changes create a paradox in which the law must constantly be updated to meet new threats, while the process of lawmaking tends to move more slowly than technological developments. In addition, the new legal framework must also consider

---

[23] Nyoman Amie Sandrawati, "Antisipasi Cybercrime Dan Kesenjangan Digital Dalam Penerapan TIK Di KPU," *Electoral Governance* 3, no. 2 (2022): 235.

[24] Jefry Tarantang et al., "PERLINDUNGAN HUKUM NASABAH DALAM PENYELENGGARAAN LAYANAN PERBANKAN DIGITAL," *BelomBahadat : Jurnal Hukum Agama Hindu* 13, no. 1 (2023): 23.

[25] Tri Andika Hidayatullah and Nani Mulyati, "Perlindungan Hukum Terhadap Korban Tindak Pidana Peretasan (Hacking) Berkaitan Dengan Pencurian Data," *Unes Law Review* 6, no. 1 (2023): 1365.

the balance between protecting privacy and security, so as not to sacrifice individual rights in the fight against cybercrime.[26]

Furthermore, hacking also involves cross-border aspects which are becoming more frequent. Hackers often operate abroad, so cyber law enforcement in Indonesia also requires close international cooperation. This cooperation includes information exchange, extradition and effective handling of cross-border hacking cases. In facing the challenges of changes and developments in cyber law in Indonesia, it is important to have a holistic and sustainable approach. This involves continuous improvements in the legal framework, increasing the capacity of law enforcement officials, increasing public awareness of cyber security, and strong cooperation with international institutions. Only with a comprehensive approach like this, Indonesia can more effectively overcome the threat of hacking and maintain the country's cyber security amidst ongoing changes in the digital world.

**Conclusion**

Indonesia's hacking legal framework is an important first step in protecting society and digital infrastructure from the threat of hacking. The Information and Electronic Transactions Law (UU ITE) and related legal provisions provide a strong legal basis for law enforcement against hacking perpetrators. However, cyber law enforcement in Indonesia still faces several challenges that need to be overcome. Shortages in resources and expertise within law enforcement agencies, rapid technological change, and increasingly complex hacking threats are some of the major obstacles. Apart from that, cyber law enforcement also requires close cooperation between various government and private institutions as well as strong international cooperation to overcome cross-border hacking. Hacking is also a challenge which shows that cyber law must always adapt to technological developments. Effective cyber law enforcement requires continuous changes and updates in the legal framework and increased public awareness of cyber security. Thus, Indonesia needs to continue to be committed to improving its legal provisions, increasing the capacity of law enforcement officials, and increasing public awareness about the risks of

---

[26] Ririn Aswandi, Putri Rofifah Nabilah Muchsin, and Muhammad Sultan, "PERLINDUNGAN DATA DAN INFORMASI PRIBADI MELALUI INDONESIAN DATA PROTECTION SYSTEM (IDPS)," *Legislatif*, no. 14 (2018): 170, https://doi.org/10.15900/j.cnki.zylf1995.2018.02.001.

hacking. Only with a comprehensive and sustainable approach can Indonesia be more effective in dealing with the threat of hacking in an ever-changing digital world.

**Bibliography**

Ardiansyah. "ANALISIS YURIDIS TERHADAP SISTEM PEMBUKTIAN PADA KEJAHATAN PERETASAN SITUS WEBSITE." *JOM Fakultas Hukum Universitas Riau Volume* 6, no. 2 (2019): 1–15.

Arisandy, Yogi Oktafian. "Penegakan Hukum Terhadap Cyber Crime Hacker." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 1, no. 3 (2021): 162–69. https://doi.org/10.18196/ijclc.v1i3.11264.

Astrini, Dwi Ayu. "Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman Cybercrime." *Lex Privatum* 3, no. 1 (2015).

Aswandi, Ririn, Putri Rofifah Nabilah Muchsin, and Muhammad Sultan. "PERLINDUNGAN DATA DAN INFORMASI PRIBADI MELALUI INDONESIAN DATA PROTECTION SYSTEM (IDPS)." *Legislatif*, no. 14 (2018): 63–65. https://doi.org/10.15900/j.cnki.zylf1995.2018.02.001.

Firdaus, Indriana. "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan." *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (2022): 23–31. https://doi.org/10.52005/rechten.v4i2.98.

Hartono, Bambang. "Hacker Dalam Perspektif Hukum Indonesia." *Masalah-Masalah Hukum* 43, no. 1 (2014): 23–30.

Hidayatullah, Tri Andika, and Nani Mulyati. "Perlindungan Hukum Terhadap Korban Tindak Pidana Peretasan (Hacking) Berkaitan Dengan Pencurian Data." *Unes Law Review* 6, no. 1 (2023): 1356–66.

Khasanah, Nurul, and Tata Sutabri. "Analisis Kejahatan Cybercrime Pada Peretasan Dan Penyadapan Aplikasi Whatsapp." *Blantika : Multidisciplinary Journal* 2, no. 1 (2023): 44–55. https://doi.org/10.57096/blantika.v2i1.13.

Kusuma, Aditama Candra, and Ayu Diah Rahmani. "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)." *SUPREMASI : Jurnal Hukum* 5, no. 1 (2022): 46–63. https://doi.org/10.36441/supremasi.v5i1.721.

Leunard, Michael, Sari Mandiana, and Jusup Jacobus Setyabudhi. "Analisis Yuridis Tentang Peretasan Data Pribadi Penumpang Lion Air." *YUSTISIA MERDEKA : Jurnal Ilmiah Hukum* 6, no. 2 (2020): 55–58. https://doi.org/10.33319/yume.v6i2.51.

Musa Sahat, Tobing, Utari Wulandari, Sihotang Marito Sari, and Raihana Raihana. "Tinjauan Terhadap Modus-Modus Kejahatan Dalam Hukum Cyber Crime." *Jurnal Hukum Dan Sosial Politik* 1, no. 2 (2023): 60–67. https://doi.org/10.59581/jhsp-widyakarya.v1i2.239.

Nasrudin, Fadhi Khoiru, 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 (2022): 331–43. https://doi.org/10.53363/bureau.v2i1.137.

Nugroho, Irzak Yuliardy. "Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia." *Al-Daulah: Jurnal Hukum Dan Perundangan Islam* 5, no. 1 (2015): 171–203. https://doi.org/10.15642/ad.2015.5.1.171-203.

Oktaviani, Asfarina, and Emmilia Rusdiana. "Alternatif Pidana Bagi Pelaku Tindak Pidana Peretasan Di Indonesia Dalam Undang-Undang Informasi Dan Transaksi

Elektronik." *Novum: Jurnal Hukum*, no. 11 (2023): 249–64.
Pane, Vincent, Grace Tampongangoy, and Renny Nansy Koloay. "Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik." *Lex Privatum* XI, no. 2 (2023).
Putri, Amelia Widya Octa Kuncoro, Abdul Razzaq Matthew Aditya, Desta Lesmana Musthofa, and Pujo Widodo. "Serangan Hacking Tools Sebagai Ancaman Siber Dalam Sistem Pertahanan Negara (Studi Kasus: Predator)." *Global Political Studies Journal* 6, no. 1 (2022): 35–46. https://doi.org/10.34010/gpsjournal.v6i1.6698.
Ridwan, Ridwan, Muhammad Nur, and Sulaiman S. "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan (Hacker) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik." *Jurnal Ilmiah Mahasiswa Fakultas Hukum Universitas Malikussaleh* 6, no. 1 (2023): 113–23. https://doi.org/10.29103/jimfh.v6i1.7007.
Saleh, Abd. Rahman. "Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana." *HUKMY : Jurnal Hukum* 1, no. 1 (2021): 91–108. https://doi.org/10.35316/hukmy.2021.v1i1.91-108.
Sandrawati, Nyoman Amie. "Antisipasi Cybercrime Dan Kesenjangan Digital Dalam Penerapan TIK Di KPU." *Electoral Governance* 3, no. 2 (2022): 232–57.
Sari, Indah. "Mengenal Hacking Sebagai Salah Satu Kejahatan Di Dunia Maya." *Jurnal Sistem Informasi Universitas Suryadarma* 10, no. 2 (2014): 169–86. https://doi.org/10.35968/jsi.v10i2.1086.
Singgi, I Gusti Ayu Suanti Karnadi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiartha. "Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)." *Jurnal Konstruksi Hukum* 1, no. 2 (2020): 334–39. https://doi.org/10.22225/jkh.2.1.2553.334-339.
Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *SASI* 27, no. 1 (2021): 38. https://doi.org/10.47268/sasi.v27i1.394.
Tarantang, Jefry, Annisa Awwaliyah, Maulidia Astuti, and Meidinah Munawaroh. "Perkembangan Sistem Pembayaran Digital Pada Era Revolusi Industri 4.0 Di Indonesia." *Jurnal Al-Qardh* 4, no. 1 (2019): 60–75. https://doi.org/10.23971/jaq.v4i1.1442.
Tarantang, Jefry, Rahmad Kurniawan, and Gusti Muhammad Ferry Firdaus. "Electronic Money Sebagai Alat Transaksi Dalam Perspektif Islam." *An-Nisbah: Jurnal Ekonomi Syariah* 07, no. April (2020): 1–21. https://doi.org/https://doi.org/10.21274/an.2020.7.1.1%20-%2021.
Tarantang, Jefry, Ibnu Elmi A.S. Pelu, Wahyu Akbar, Rahmad Kurniawan, and Aldina Sri Wahyuni. "PERLINDUNGAN HUKUM TERHADAP NASABAH BANK DALAM TRANSAKSI DIGITAL." *Morality: Jurnal Ilmu Hukum* 9, no. 10 (2023): 15–25. https://doi.org/http://dx.doi.org/10.52947/morality.v9i1.321.
Tarantang, Jefry, Syawaliah, Ni Nyoman Adi Astiti, and Dekie G.G. Kasenda. "PERLINDUNGAN HUKUM NASABAH DALAM PENYELENGGARAAN LAYANAN PERBANKAN DIGITAL." *BelomBahadat : Jurnal Hukum Agama Hindu* 13, no. 1 (2023): 9–25.