IJLRSA
The International Journal of Law Review and State Administration
E-ISSN : 3025-843x
Vol 1, No 3, (November - Desember 2023) Pages: 120–128

Law Enforcement in Efforts to Combat Cyber Crime in Indonesia: Building Future Digital Security

Sri Jaya Lesmana
Syekh-Yusuf Islamic University, Tangerang, Indonesia
sjlesmana@unis.ac.id

Inas Sofia Latif
Syekh-Yusuf Islamic University, Tangerang, Indonesia
inaslatif@gmail.com

Felina
Women University, *Philippines*
felina@gmail.com

Abstract
The development of information technology can change social order and behavior. The wrong use of advances in information technology refers to crime. The level of cybercrime in Indonesia has reached an alarming stage, therefore the existence of a security system and regulations related to this matter is an urgent need. The purpose of this study is to examine and analyze law enforcement efforts in combating cybercrime in order to build future digital security in Indonesia. Normative legal research is used by researchers to answer related problems through a legal approach with a literature study method. The results showed that although cybercrime has been regulated in positive law in force in Indonesia, the regulation and implementation of security can be said to be still not optimal. Researchers suggest that cybersecurity-related regulations should be specific. Furthermore, harmonization and synchronization of related rules must be carried out so that the handling of cybercrime becomes integrated. Finally, the establishment of a special institution for handling cyber problems is important so that Indonesia has a strong cyber defense.

Keywords: law enforcement; cybercrime; digital security.

A. Introduction

The significant development of information technology has changed the understanding and view of the world. In the era of globalization, cyber space has become a basic need for humans that can connect people across borders. Although intangible, the existence of cyber space is real. The presence of cyber space is brought through the internet (Mahzar, 1999; Sari, 2022). The world formed is a virtual world without borders that does not recognize the dimensions of place, time, and space (Prabowo, 2020). This ease in a borderless relationship certainly has logical consequences for it.

In this regard, cyber security is a real and urgent need because it has an impact that has the potential to damage or destabilize conditions both individually and in a wider scope, namely the state. The urgency of cybersecurity is becoming increasingly urgent because the internet has a

certain dark side. Concerns over security and crimes that occur in cyberspace have been in the spotlight of the world. As evidenced by the discussion related to this at the 10th UN Congress on Crime Prevention and Treatment of Offenders in Vienna, Austria, 2000 is Computer Network-Related Crimes (Rizal & Yani, 2016).

So far, not all countries have cybercrime laws, and not all countries pay attention to this problem (only developed countries and some developing countries have such laws). As a developing country, Indonesia is slightly behind in following the development of information technology (Yulianto, 2021). This lagging lag results in the transfer of technology from developed countries is not accompanied by mastery of the technology itself. So that the use of existing information technology cannot be done optimally, including in terms of security of its use.

From data compiled by the National Criminal Information Center (Pusiknas), it is known that the number of cybercrime crimes increased significantly in 2022 compared to the same period in 2021. Even in numbers, the number of cybercrimes has increased up to 14 times. When seen, the e-MP Robinopsnal Bareskrim Polri shows that the police have cracked down on 8,831 cybercrime cases from January 1 to December 22, 2022 (Tim Penulis Pusiknas, 2023). Some examples of cybercrime cases that occur include data theft (phishing) (CNN Indonesia, 2023), unauthorized access, illegal contents (Yakhamid, 2023), malware, to ransomware (Ibrahim, 2023).

The severity of some of these cybercrimes befalls websites owned by institutions or institutions that have an important and strategic role in the state administration order (Lintasarta Cloudeka, 2023). Some of the institutions in question include the General Elections Commission (KPU), the House of Representatives of the Republic of Indonesia (DPR RI), the Health Social Security Organizing Agency (BPJS Kesehatan), the Police, and the Attorney General's Office (Farid, 2022). Looking at some examples of cybercrime cases that occur, it is worth saying that Indonesia is experiencing a cyber emergency.

This of course must be the government's attention to be able to immediately overcome and take steps so that this cybercrime does not increase in the number of cases (Anam & Syahputra, 2023). Based on this background description, the researcher views to review and conduct analysis related to law enforcement efforts in combating cybercrime in order to build future digital security in Indonesia. Therefore, researchers intend to express the results of researchers' thoughts in a study entitled "**Law Enforcement in Efforts to Combat Cyber Crime in Indonesia: Building Future Digital Security**".

B. Research Method

This research is a prescriptive research that is included in normative legal research. The statutory approach was used in this study to help researchers answer existing problems. Researchers use secondary data obtained through literature studies. Laws and other related regulations are used as references or what we call primary legal material.

The legislation in question is Law Number 11 of 2008 concerning Electronic Information and Transactions jo. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). While secondary legal materials are obtained from journal articles, books, or scientific publications relevant to the regulation of cybercrime in force in Indonesia. Analysis of legal materials is carried out using descriptive methods in order to produce conclusions that can be accounted for (Marzuki, 2017).

C. Result and Discussion

1. Criminal Law Policy Against Cyber Crime Based on Positive Law

Indonesia is a state of law, as stated in Article 1 paragraph (3) of the 1945 Constitution (UUD 1945) (Lesmana, 2020). The application of this statement is that everything related to governance in force in Indonesia must have a legal basis in the form of laws and regulations that have been passed by the government (Goce & Adhari, 2023). In line with national goals, governments are responsible for providing protection to all citizens. The role of the

government is a strategic role, especially as outlined through the making of laws and regulations (Sabardi, 2014; Supanto, 2016).

Legal needs in society must be considered and fulfilled as a guarantee of legal certainty and legal protection to every community, especially people in Indonesia (S, 2017). Human civilization in the modern era continues to develop into part of global society or what we refer to as globalization (Rais et al., 2018). The use of globalization according to Featherstone in the perspective of cyberspace globalists is that globalization is characterized by the latest developments in information technology and the growth of other discoveries that are able to make humans able to carry out their tasks more easily and quickly (Jati, 2013; Mewengkang et al., 2021).

Globalization, information technology, and law are three areas that are mutually sustainable. The advantages created by information technology promise a number of hopes. But behind it all, new concerns arise with the rise of cybercrime cases. The subject of cybercrime law itself can be human as individuals or corporations (Vitayanti & Santosa, 2015). The Criminal Code (KUHP) as the basis of criminal law in force in Indonesia (in addition to other laws and regulations) currently only recognizes humans who are subject to criminal law. Over time and seeing developments in Indonesian criminal law, by looking at the tendency of conditions that occur, in addition to humans as legal subjects, legal entities can also be used as legal subjects (Tomalili, 2015).

The legal system in Indonesia does not specifically regulate cyber law, but some laws have included provisions to prevent cybercrime. As "Law Number 36 of 1999 concerning Telecommunications, Law Number 19 of 2002 concerning Copyright, Law Number 15 of 2003 concerning Combating Terrorism, and Law Number 11 of 2008 concerning Electronic Information and Transactions jo. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law)", are some relevant laws (Ubaidillah et al., 2022).

Such laws and regulations have criminalized this type of cybercrime and established penalties for violators (Koto, 2021). In addition, aspects of criminalization related to cybercrime have also been regulated in the Criminal Code (KUHP) in the Second Book (Chapter VIII) with a focus on criminal acts that endanger public security, such as Articles 373-379 which regulate Crimes Against Informatics and Telematics. These articles cover acts such as illegal access, illegal interception, data interference, system interference, misuse of domain names, and child pornography (Situmeang, 2021).

In the context of future criminal law developments, the resolution and prevention of cybercrimes needs to be accompanied by the regulation and development of the entire criminal law system. This includes the construction of legal structures, cultural changes, and refinement of the substance of criminal law. Under these conditions, criminal law policy becomes very important in leading to the development of modern criminal law aimed at achieving peace and welfare for all parties.

The following are the forms of cybercrime regulated in the ITE Law, including: (Akub, 2018).

a. Acts that violate decency

   Article 27 paragraph (1) of the ITE Law states that "Everyone intentionally and without rights shares or disseminates or makes accessible Electronic Information or Electronic Documents that have contents that violate decency." However, the law does not specifically address the act of sharing, disseminating, or creating electronic information content or electronic documents that violate decency or decency. Violations of ethics or decency through internet media refer more to the Criminal Code.

   In the context of actions that violate decency through electronic media, Article 27 paragraph (1) of the ITE Law regulates electronic information and transactions, including issues such as online pornography and online prostitution. If these crimes are committed

against children, the severity will increase. One of the impacts of advances in information technology through the internet is the increasing number of sites that display pornographic content. It can be seen that nowadays, protecting the internet from interference by entertainment traders who sell pornographic material is a very difficult challenge (Idy, 2022; Wahid & Labib, 2005).

b. Gambling
Online gambling is regulated in Article 27 paragraph (2) ITE. In this regulation it is also stated that: "Everyone intentionally and without rights share/disseminate/make accessible electronic information/electronic documents that have gambling content."

c. Insult or contamination of a good name
Pollution of good name or contempt in the virtual world is a prohibition set out in Article 27 verse (3) of the ITE Act, which reads: "Every person willfully, and without the right to share/disseminate/make accessible electronic information/electronic documents that have a load of contempt or contamination of good name." Lawmakers are equating between insults and pollution. Self-deprecation is an act, whereas one of the forms of humiliation is pollution. The legislators themselves seem willing to direct the insults of the internet media as pollution. In Chapter XVI Book II regulates about acts of humiliation and pollution.
The crime of contempt consists of general insult and specific insult. General contempt refers to objects of self-respect and dignity of private persons, including pollution. While specific insults refer to insults that have objects of self-respect, honor and good name open (public) (Chazawi, 2020). Acts of insult or defamation can be found in various comment columns in cyberspace, especially when victims scan their personal identities, photos, or videos. The perpetrator may also write derogatory or defamatory text on the statement wall to make the statement or connect the statement to the victim.

d. Blackmail or threats
Article 27 paragraph (4) of the ITE Law prohibits extortion or threats in cyberspace. The article explains: "Any person who intentionally and without rights distributes and/or transmits and/or makes accessible electronic information and/or electronic documents that have the content of blackmail and/or threats." Article 368 (1) of the Penal Code lists the qualifications for acts that count as extortion or threatening, namely: "Any person who intends to benefit himself or another person unlawfully (illegally), compels a person to give something belonging to that person or another person in whole or in part by force or threat of violence or creates a debt or writes off a debt, shall be punished with extortion and may be sentenced to up to 9 years prison."

e. Cyberstalking
The ITE Law in Article 29 stipulates that: "Any person who intentionally and without rights sends Electronic Information or Electronic Documents containing threats of violence or frightening directed personally". The provisions related to information and electronic transactions in Article 29 regulate acts of harassment, threats, or other behavior aimed at causing fear, including the use of certain words or actions. This rule is similar to regulations regarding cyberstalking in the United States, Canada, the United Kingdom, and several other countries. This action is carried out by utilizing information and communication technology, such as sending mail bombs, unwanted hate messages, emails containing abusive words or threats, and other methods (Suseno, 2013).

f. Spread of fake news (hoax)
The spread of fake news is regulated in Article 28 paragraph (1) of the ITE Law, which reads: "Everyone intentionally and without the right to spread false / false and misleading news, which results in consumer losses in Electronic Transactions."

g. Hate speech
Article 28 paragraph (2) of the ITE Law regulates the crime, which reads: "Everyone intentionally and without rights disseminates information designed to cause hatred or

hostility of certain individuals / groups of people based on ethnicity, religion, race, and inter-group (SARA)."

h. Illegal access

Article 30 of the ITE Law regulates illegal access as follows:

1) Anyone who knowingly, without rights or against the law (illegally) accesses another person's Computer or Electronic System in any way.
2) Anyone intentionally, without rights or unlawfully (illegally) accesses (opens) a computer or electronic system in any way with the intention of obtaining electronic information or electronic documents.
3) Anyone who violates, breaks through, exceeds, or breaks into security systems intentionally, without rights or unlawfully (illegally) accesses computers or electronic systems.

2. Law Enforcement in Efforts to Combat Cyber Crime in Indonesia

a. Application of Cyber Security in Indonesia. It is undeniable that the development of science is followed by technology. Technological developments are used to encourage rapid business growth. Information is presented in such a fast time. Only by utilizing communication technology, business between countries can be done without the need to meet face to face (Sabadina, 2021; Suparni, 2009). This is a sign that the cyber era in business has begun. In addition to benefiting business people, technological developments also make it easier to get information, and also have an impact on the economic, political, cultural, and legal sectors of a country.
b. Rapid technological advances have an impact not only in the form of positive impacts, but on the contrary also have a negative impact. The negative impact in question is related to cybercrime. In the midst of an ever-evolving digital age, cybercrime poses a serious threat to national and individual security. As a country that is increasingly dependent on information technology, Indonesia must commit to tackling cybercrime by strengthening law enforcement in cyberspace. This is the right response and step to strengthen cyber civilization in Indonesia (Riskiyadi et al., 2021; Wahid, 2002).
c. The development of computer technology, information technology, and communication technology has also led to the emergence of new criminal acts that have different characteristics from conventional crimes. Misuse of computers as one of the impacts of these three technological developments is inseparable from its nature which has its own characteristics so that it brings complicated problems to solve regarding the problem of overcoming it ranging from investigation, investigation to prosecution (Makarim, 2006). It can be said that the advancement of technology and information in addition to being able to be used by humans as an information commodity, can also have a negative impact, namely the misuse of technology which brings it to a criminal act called cybercrime. The cybercrime has its own characteristics because it is related to computer technology networks so that the handling cannot be equated with conventional crimes.

The Indonesian government has established policies related to the implementation of cybersecurity within the framework of laws and regulations, with the main foundation coming from the Law on Information and Electronic Transactions (UU ITE). In addition to the ITE Law, there are several other laws that are indirectly related to cybersecurity policy, such as Law Number 36 of 1999 concerning Telecommunications and Law Number 14 of 2008 concerning Public Information Openness. Furthermore, there are a number of laws that provide concrete support for the implementation of cybersecurity, including:

1) Law Number 8 of 1999 concerning Consumer Protection;
2) Law Number 2 of 2002 concerning the National Police of the Republic of Indonesia;
3) Law Number 3 of 2002 concerning State Defense;

4) Law Number 15 of 2003 concerning the Stipulation of Government Regulations in Lieu of Law Number 1 of 2022 concerning the Eradication of Criminal Acts of Terrorism into Law;
5) Law Number 34 of 2004 concerning the Indonesian National Army; and
6) Law Number 25 of 2009 concerning Public Services.

Through this regulation, the government seeks to create a legal framework that supports the implementation and enforcement of cybersecurity policies in Indonesia. Although the handling of cybersecurity in the framework of national defense is still sectoral, it has not been well coordinated and integrated. Likewise, the concept of cyber defense applied by the Ministry of Defense and the TNI is still temporary, sectoral, not comprehensive as a unit (Budiman, 2022).

3. Strengthening Cybersecurity in Indonesia

Strengthening cybersecurity in Indonesia is a very important effort considering the development of information technology and people's dependence on the internet. The state through the government must be able to create a safe and trustworthy digital environment. Effective law enforcement, supported by strong regulation and cross-sector collaboration, lays the foundation for eradicating cybercrime and protecting the country's society and digital infrastructure. Several steps that can be taken to strengthen cybersecurity in Indonesia can be done by involving various parties, namely the government, the private sector, and the general public. These steps include:

a. Legal Capacity Building
   Increased cyber legal capacity is critical to protecting people, businesses, and information infrastructure from cyberattacks. Actions that can be taken to strengthen cyber legal capacity are by involving policy stakeholders, especially related to the preparation of laws and regulations, law enforcement, and international cooperation (Putri, 2021). Drafting clear and comprehensive laws and regulations related to cybercrime, including strict sanctions and punishments is a priority step to take. Moreover, cybercrime is dynamic, so regular rule updates are also important to do in order to keep up with the development of new cybercrime technology and tactics.
b. Policy Formation and Cybersecurity Infrastructure Development
   Policy formation and the development of cybersecurity infrastructure are two interrelated and crucial aspects in an effort to protect a country or organization from threats in cyberspace. Amid the rapid development of information technology, governments and the private sector must take strategic steps to protect sensitive data and critical infrastructure from increasingly sophisticated cyber threats. The process of establishing cybersecurity policy should involve coordination between governments, regulatory agencies, and relevant stakeholders. Furthermore, the development of cybersecurity infrastructure is an integral part of policy implementation. This infrastructure includes technology, personnel, and procedures that support protection against cybersecurity threats.
c. Capacity Building and Community Awareness
   In the midst of the rapid development of information technology, increasing public capacity and awareness in cybersecurity is an urgent need. People who have a good understanding of cyber threats and countermeasures can be at the forefront of protecting themselves and their communities from various risks that arise in cyberspace. A more educated and aware society of cybersecurity risks can be a powerful layer of defense.
   Public awareness of cybersecurity can be increased through various methods. Social media campaigns are becoming an effective means of disseminating cybersecurity information and tips. The public can be invited to actively participate in this campaign by disseminating safety information, voicing their experiences, and asking questions about things that are not yet understood. In addition, local workshops and seminars can also be a place to interact with the community. By bringing in cybersecurity experts, the public

can gain insight, ask questions, and discuss relevant security issues. The establishment of a cybersecurity community at the local level can also provide a platform for sharing experiences and knowledge.

d. Partnership Between Government, Private Sector, and Academia

Strong partnerships between governments, the private sector, and academic institutions are a very important foundation in efforts to improve a country's cybersecurity. This collaboration not only strengthens defenses against cyber threats, but also encourages innovation and knowledge exchange between these sectors.

Governments have a central role to play in shaping the frameworks, regulations, and policies that support cybersecurity. By involving stakeholders from the private and academic sectors, the government can ensure that the regulation is in line with the needs of industry and society. In addition, the government can be a prime mover in establishing national cybersecurity centers and providing resources for training and skill development in this area.

The private sector is not only a prime target for cyberattacks, but also has an important role to play in protecting digital infrastructure. Through partnerships with governments, companies can share up-to-date information on cyber threats and contribute to the development of more effective policies. Meanwhile, the private sector can also provide the financial and technological support needed for critical cybersecurity projects.

Furthermore, academic institutions bring technical and research expertise that can help identify new threat trends and develop innovative solutions. Partnerships with academic institutions enable up-to-date education and training programs, creating the next generation of cybersecurity experts. In addition, academic institutions can also be valuable sources of research to inform cybersecurity policies and practices.

e. Monitoring and Quick Response

The importance of monitoring cannot be underestimated. Sophisticated monitoring systems allow us to proactively detect suspicious or unusual activity within networks and systems. Using behavioral analysis and threat detection technologies, any suspicious changes can be identified early. However, detecting threats alone is not enough. Quick response is key to stopping an attack before it causes significant damage. Every threat detection must be followed by fast and precise action. Having a detailed cybersecurity response plan that is regularly tested is a must.

In the face of evolving cyber threats, all parties must be able to work together. Collaboration and partnerships between governments, the private sector, and cybersecurity agencies are key to building a solid security ecosystem. The exchange of information on current threats and attack techniques can enrich insights and detection capabilities. In a changing and connected world, monitoring and rapid response is not just a strategy, but a necessity. Creating a resilient cybersecurity environment requires a combination of advanced technology, proven response strategies, and cross-sector collaboration. With this approach, each party is expected to prepare for cyber threats with the confidence and resilience needed in the tireless digital era.

The steps mentioned above are expected to be taken into consideration and reference in the formulation of policies that can increase the resilience of existing cybersecurity in Indonesia to face cybersecurity challenges and protect information and critical infrastructure from attacks that can be detrimental from all sides.

D. Conclusion

Currently, Indonesia does have several laws and policies that regulate cybersecurity. However, existing rules and/or policies are still general and non-specific. As a result, cybersecurity implementation has not been effective. In order to run effectively, in this case the government through policy makers needs to establish rules or policies that specifically regulate cyber security. Including establishing partnerships and collaborations with the private sector and academia to

strengthen the ecosystem in order to increase the level of cyber security.

In addition, the government needs to be more serious in responding to and anticipating cyber attacks. Indonesia does not yet have a special institution that has full authority to manage and handle cybersecurity. However, even though there is no or no special institution, the government can still assign one of its structures or institutions to become a leading sector in handling this cyber problem. So that the handling of cybersecurity is not spread and cyber defense can become stronger and more solid.

Based on the results of the research that has been described, it can be seen that indeed the condition of cyber defense in Indonesia is still weak. Therefore, researchers suggest several things as follows. First, regulations related to cyber policy need to be specific. Second, harmonization and synchronization of related rules must be carried out so that the handling of cybercrime becomes integrated. Third, the establishment of a special institution for handling cyber problems is important to be confirmed, so that Indonesia has a strong cyber defense.

References

Akub, M. S. (2018). Pengaturan Tindak Pidana Mayantara (Cyber Crime) Dalam Sistem Hukum Indonesia. *Al-Ishlah: Jurnal Ilmiah Hukum*, *21*(2), 1–26.

Anam, K., & Syahputra, E. (2023, November 2). Indonesia Darurat Serangan Siber, Pemerintah Harus Apa? *CNBC Indonesia*. https://www.cnbcindonesia.com/tech/20231102140604-37-485824/indonesia-darurat-serangan-siber-pemerintah-harus-apa

Chazawi, A. (2020). *Hukum Pidana Positif Penghinaan*. Media Nusa Creative.

CNN Indonesia. (2023, June 19). 35 Kebocoran Data 2023, Kominfo Akui Cuma Beri Rekomendasi dan Teguran. *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/20230619141948-192-963776/35-kebocoran-data-2023-kominfo-akui-cuma-beri-rekomendasi-dan-teguran

Farid, A. (2022). *14 Kasus Cyber Crime di Indonesia Yang Menggemparkan Warganet*. Exabytes. https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/

Goce, A. N. R., & Adhari, A. (2023). Pertanggungjawaban Pidana Korporasi PT. Aneka Bintang Gading Dalam Tindak Pidana Penistaan Agama Melalui Media Sosial Holywings. *Syntax Literate: Jurnal Ilmiah Indonesia*, *8*(2), 810–820.

Ibrahim, M. (2023, June 20). Waspada! Ini Modus Serangan Siber Teranyar di Indonesia. *Infobanknews.Com*. https://infobanknews.com/waspada-ini-modus-serangan-siber-teranyar-di-indonesia/

Idy, M. Y. (2022). Implementasi Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Di Bidang Komputer. *Pleno Jure*, *11*(2), 142–158. https://doi.org/10.37541/plenojure.v11i2.818

Jati, W. R. (2013). *Pengantar Kajian Globalisasi: Analisa Teori dan Dampaknya di Dunia Ketiga*. Mitra Wacana Media.

Koto, I. (2021). Cyber Crime According to the ITE Law. *IJRS: International Journal Reglement & Society*, *2*(2), 103–110.

Lesmana, H. S. J. (2020). *Pengantar Ilmu Hukum*. Bidara Cendekia Ilmi Nusantara.

Lintasarta Cloudeka. (2023, July 26). 10 Contoh Kasus Cyber Crime yang Bisa Menjadi Pelajaran. *Lintasarta Cloudeka*. https://www.cloudeka.id/id/berita/web-sec/contoh-kasus-cyber-crime/

Mahzar, A. (1999). *Spiritualitas Cyber Space: Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagamaan Manusia*. Mizan.

Makarim, E. (2006). *Pengantar Hukum Telematika Suatu Kompilasi Kajian*. Raja Grafindo Persada.

Marzuki, P. M. (2017). *Penelitian Hukum*. Kencana.

Mewengkang, I. B., Warong, R. N., & Kuntag, M. (2021). Kajian Yuridis Cyber Crime

Penanggulangan Dan Penegakan Hukumnya. *Lex Crimen*, *10*(5), 26–35.

Prabowo, G. (2020, December 21). Perkembangan Teknologi Informasi dan Komunikasi di Indonesia. *Kompas.Com*. https://www.kompas.com/skola/read/2020/12/21/164007469/perkembangan-teknologi-informasi-dan-komunikasi-di-indonesia?page=all

Putri, K. V. K. (2021). Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime. *Jurnal Hukum Lex Generalis*, *2*(7), 542–554. https://doi.org/10.56370/jhlg.v2i7.90

Rais, N. S. R., Dien, M. M. J., & Dien, A. Y. (2018). Kemajuan Teknologi Informasi Berdampak Pada Generalisasi Unsur Sosial Budaya Bagi Generasi Milenial. *Jurnal Mozaik*, *10*(2), 61–71.

Riskiyadi, M., Anggono, A., & Tarjo. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Manajemen Dan Organisasi*, *12*(3), 239–251. https://doi.org/10.29244/jmo.v12i3.33528

Rizal, M., & Yani, Y. M. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *Journal of ASEAN Studies*, *4*(1), 61–78. https://doi.org/10.21512/jas.v4i1.967

S, L. A. (2017). Perlindungan Hukum UMKM dari Eksploitasi Ekonomi Dalam Rangka Peningkatan Kesejahteraan Masyarakat. *Jurnal Rechts Vinding*, *6*(3), 387–402.

Sabadina, U. (2021). Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online. *Jurnal Lex Renaissance*, *6*(4), 799–814. https://doi.org/10.20885/jlr.vol6.iss4.art11

Sabardi, L. (2014). Peran Serta Masyarakat Dalam Pengelolaan Lingkungan Hidup Menurut Undang-Undang Nomor 32 Tahun 2009 Tentang Perlindungan dan Pengelolaan Lingkungan Hidup. *Yustisia*, *3*(1), 67–79.

Sari, U. I. P. (2022). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Mimbar Jurnal Hukum*, *2*(01), 58–77. https://doi.org/10.61084/jsl.v2i01.7

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *Sasi*, *27*(1), 38. https://doi.org/10.47268/sasi.v27i1.394

Supanto. (2016). Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy. *Yustisia Jurnal Hukum*, *5*(1), 52–70. https://doi.org/10.20961/yustisia.v5i1.8718

Suparni, N. (2009). *Cyberspace: Problematika dan Antisipasi Pengaturannya*. Sinar Grafika.

Suseno, S. (2013). *Yurisdiksi Tindak Pidana Siber*. Refika Aditama.

Tim Penulis Pusiknas. (2023). *Kejahatan Siber di Indonesia Naik Berkali-Kali Lipat*. PUSIKNAS. https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

Tomalili, R. (2015). *Hukum Pidana*. Deepublish.

Ubaidillah, Dani Noval Kurnia, A., & Octaviany, R. V. (2022). Kejahatan Cybercrime di Era 4.0. *Universitas Negeri Surabaya*, *1*(10), 776–783.

Vitayanti, N. M. R., & Santosa, A. A. G. D. H. (2015). Tinjauan Yuridis Pertanggungjawaban Pidana Pelaku Tindak Pidana Prostitusi Secara Online Berdasarkan Perspektif Cyber Crime. *Kertha Semaya*, *4*(3), 1–5.

Wahid, A. (2002). *Kriminologi dan Kejahatan Kontemporer*. Lembaga Penerbitan Fakultas Hukum Unisma.

Wahid, A., & Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime)*. Refika Aditama.

Yakhamid, R. Y. (2023). *Waspada Kejahatan Siber di Era Serba Daring*. LAN RI. https://lan.go.id/?p=13415

Yulianto, A. (2021). Cybersecurity Policy and Its Implementation in Indonesia. *Law Research Review Quarterly*, *7*(1), 69–82. https://doi.org/10.15294/lrrq.v7i1.43191