International Journal of Multidisciplinary Research and Growth Evaluation.

The Impact of Digital Technology Developments on Criminal Law Enforcement in Indonesia

Moh. Anshori [1*], Nur Lailatul Musyafa'ah [2], Muh. Fathoni Hasyim [3]
[1-3] Faculty of Syariah and Law, UIN Sunan Ampel Surabaya, Indonesia

* Corresponding Author: **Moh. Anshori**

Article Info

ISSN (online): 2582-7138
Volume: 05
Issue: 06
November-December 2024
Received: 06-10-2024
Accepted: 09-11-2024
Page No: 1014-1019

Abstract
The development of technology in the era of globalization makes it very easy for perpetrators to open up opportunities for crime. This article aims to examine the impact of information technology developments on criminal law in Indonesia. This research is a literature research. Data comes from laws, books, and journals. The data were analyzed descriptively. The results of the study concluded that the crimes that occurred in the era of globalization were social media crimes such as cyber, system hacking, and electronic media crimes. For this reason, the Indonesian government amended Law Number 11 of 2008 concerning Information and Electronic Transactions, which was amended into Law Number 19 of 2016, as a form of effort to prevent information technology crimes and protect the public from these crimes. However, the law still has obstacles in dealing with electronic media crimes. Crimes occur because of opportunities and weaknesses in electronic systems, so there must be improvements by improving the professionalism of the Indonesian criminal law apparatus, increasing human resources from law enforcers, building forensic computer facilities, and taking preventive measures in cybercrime.

DOI: https://doi.org/10.54660/.IJMRGE.2024.5.6.1014-1019

Keywords: Information Technology, Criminal Law, Law Enforcement

1. Introduction

In the era of globalization, there has been a very rapid development in the field of information and technology (Edoho, 2013) [14]. These developments have a significant influence on the development of human life from childhood to adulthood (Sabadina, 2021) [33]. Technological progress is a development that every human being cannot avoid as a form of scientific development. The increasing industrial revolution has an impact on the development of law, government, and social justice (Mokyr, n.d.).

The development of technology can make it easier for everyone to carry out various activities (Nandiansyah, Aldi *et al*., 2022, p. 78) [28]. Information technology is believed to bring great benefits and importance to countries in the world. There are at least two things that make information technology so important in spurring world economic growth. First, technology drives demand for information technology products themselves, such as computers, modems, means to build internet networks, and so on. The second is to facilitate business transactions, especially financial business, in addition to other business businesses (Markus Djarawula *et al*., 2023, p. 3800) [23].

While technology offers a wide range of opportunities, there are also significant challenges to face. One of the main challenges is data privacy and security (Candiwan Candiwan & Luthfi Machdar Rianda, 2024) [9]. The use of technology in the detection and prevention of criminal acts often involves the collection and analysis of sensitive personal data, which can pose a risk of data misuse if not managed properly. In addition, the success of technology in combating evil is highly dependent on cooperation between institutions, both at the national and international levels, which often face bureaucratic constraints and policy differences (Fahamsyah *et al*., 2022) [15].

Several countries have regulated and made laws on technology, including Indonesia (Rosmaini *et al*., 2018, p. 2) [32]. In Indonesia, more than 150 million Indonesians now have access to the internet (Marwan *et al*., 2022, p. 22) [24]. In 2008, the

Indonesian now have access to the internet (Marwan *et al*., 2022, p. 22) [24]. In 2008, the Indonesian government issued Law Number 11 of 2008 concerning Information and Electronic Transactions, which was amended into Law Number 19 of 2016. This law was made to protect the public from electronic media crimes. Information, technology, and electronic laws should be mandatory to protect various cybercrimes whose scope is for legal purposes (Katyal, 2001) [22]. However,
many problems still arise in the application of criminal law in this era of globalization due to the influence of the rapid development of digital information. Based on this, this article discusses the development of information technology in the application of criminal law in Indonesia.
Several studies discuss cyber and criminal law: Criminal law regulation of cyber fraud crimes—from the perspective of citizens' information protection in the era of edge computing (Zhang & Dong, 2023) [37], the Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes (Al-Amaireh, 2024) [3], Genesis of the notion "cybersecurity" in the fuel and energy sector of the European Union: Legal analysis (A. Y. Sukharev Moscow Academy of the Investigative Committee of the Russian Federation *et al*., 2024) [1], and Illegal Online Loans in Indonesia: Between the Law Enforcement and Protection of Victim (Angkasa *et al*., 2023) [5]. Based on some of these studies, there has been no discussion about the development of information technology in criminal law enforcement in Indonesia. Therefore, this research is important to be carried out.

Method

This research is normative research with a qualitative approach. Data collection was carried out through a literature research derived from laws, books and journals which discussed the development of information technology and its relationship with criminal law enforcement. The data collected were analyzed descriptively.

Development of Digital Technology in Indonesia and Its Impact on Cybercrime

The development of technology in life starts from a very simple process, namely from daily life to the level of satisfaction of every individual and social being. From time to time, technological advances continue to develop rapidly and rapidly, starting from the agricultural era, the industrial technology era, the information technology era, and the communication and information technology era. The development of information and communication technology has a huge impact on people's lives (Danuri, 2019) [10].
Digital technology is an information technology that prioritizes the use of digital computers in its activities compared to using human labor. Digital information and communication technology development will continue to increase by being influenced by three things, namely digital transition, network convergence, and digital infrastructure. The development of technology and information has a huge impact on daily life, both in terms of education, economics, politics, and others, which makes all activities easier (Devi Tama Hardiyanti *et al*., 2023, p. 557).
In addition to having a positive impact, the development of information technology can also have a negative impact, namely, giving rise to crime. A criminal act is an unlawful act and allowing the perpetrator to be threatened with criminal penalties (*Sanctions, Perceptions, and Crime: Implications for Criminal Deterrence | Journal of Quantitative Criminology*, n.d.). In this era of globalization, criminal acts are increasingly growing because they are influenced by technological sophistication. Advances in information and communication technology make the current era a digital era (Pansariadi & Soekorini, 2023, p. 288) [29].
Crimes that arise as a result of technology are called cybercrime or crimes through the internet network (Candiwan *et al*., 2022) [8]. Among the forms of cybercrime are credit card theft, hacking of various websites, intercepting other people's data transmissions such as emails and data manipulation by preparing unwanted commands into computer programs (Besar, 2016) [6]
According to its typology, cybercrime comes from the words cyber and crime. Crime means crime, criminal acts, criminal events, or the like, while cyber means space, cyber, cyberspace (Hengki Irawan *et al*., 2024, p. 4355) [17]
Cybercrime is often equated with computer crime. Cybercrime is a crime that arises as a result of the existence of a cyber community. Cybercrime has certain characteristics that are different from the two models where this cybercrime has quite large consequences for citizens of the nation or state (Das & Nayak, n.d.).
Cybercrime is a very negative activity for many internet users. Cybercrime is said to be the activity or trying to insert the computer community devices of others to find, steal, damage, hack things that can be privacy and can cause damage to the assets of internet users. Cybercrime perpetrators also bring sufferers to large companies, internet users, digital system users, government businesses and many other cybercrime targets (Imran & Gunawan, 2024) [19].
Cybercrime can be formulated as an unlawful act that is attempted by using a computer network as a facility/equipment or a computer as an object, either to gain profit or not, or by harming other parties. Computer crime associated with hackers generally has a negative meaning. The existence of cybercrime is a threat in human life, making it difficult for government organizations to overcome crimes committed in computer technology. This crime has a bad impact on society, this is due to the lack of knowledge about crimes on the internet network and the lack of cyber protection and the security of personal data is no longer effective that during this time additional devices and ranges are not available. needed to conquer the problem of cybercrime (Indah *et al*., 2022, p. 3) [20]
Since 1983, Indonesia has experienced cybercrime, especially in the financial industry such as software piracy, encryption breaches, the use of stolen credit cards, bank fraud (Dewi *et al*., 2023) [13]. In addition to economic crimes, cybercrime also includes the spread of pornographic content, computers and other forms of cybercrime (Pansariadi & Soekorini, 2023, pp. 288–289) [29]. Throughout 2022, there have been many cybercrime cases targeting the personal data of several companies in Indonesia. Like hacker Bjorka who had gone viral because of his action of stealing personal data belonging to Bank Indonesia (BI) in early January 2022. There were at least seven major cases of data breaches carried out by Bjorka in 2022 (Hengki Irawan *et al*., 2024) [17]. In addition, on May 14, 2023, Bank Syariah Indonesia (BSI) fell victim to a cybercrime attack when hackers broke into their important data. This caused customers to not be able to access mobile banking services for 5 days. Based on information from Ministry of Communication and Information of the Republic of Indonesia, Indonesia ranks third in the country

with the highest number of cybercrime cases globally, after Ukraine (Muhammad Ghozali *et al*., 2024, p. 798) [27].

Regulations on Cybercrime in Indonesia

Cybercrime is a crime that takes advantage of the development of computer technology, especially the Internet. Cybercrime is an unlawful act that utilizes computer technology based on the sophistication of internet technology developments. Cybercrime is divided into two categories namely, cybercrime refers to crimes against computer systems, and cybercrime includes crimes against computer systems or networks as well as crimes involving the use of computer facilities (Mohamad Revaldy Fairuzzen *et al*., 2024, p. 140) [25]

Indonesia, as a country of law, always prioritizes all state and community activities based on legal provisions. Because of this, Indonesia has always tried to reform the Criminal Law, one of which is by issuing the Electronic Information and Transaction Law (UU ITE). Because the implementation of activities in the field of computer-based technology is very important for the community and is prone to human rights violations (Markus Djarawula *et al*., 2023, p. 3803) [23].

The regulation of the form of cybercrime in the Criminal Code (KUHP) can be seen in the following articles: a. Article 282 of the Criminal Code concerning crimes against modesty; The distribution of pornography can be restricted, although in Indonesian, criminals register domains abroad, where adult pornography is allowed, making it more difficult to prosecute. Spreading vulgar photos or private videos on the Internet can be punished. Porn videos of students, workers, and public officials on the Internet. b. Article 303 of the Criminal Code concerning Gambling can be applied to internet gambling games organized by Indonesians. It regulates gambling violations. The article discusses gambling penalties. c. Article 311 of the Criminal Code concerning Defamation: Penalties for defamation through Internet media can be filed. The perpetrator sent emails to the victim's friends or mailing lists with fake stories. d. Article 335 of the Criminal Code relates to unpleasant acts, especially regarding crimes against the freedom of persons. Article 335 of the Criminal Code contains sanctions or punishments for perpetrators who have committed coercion against others. It can be applied to threats, and Criminals send emails to extort victims, which may have serious consequences if not carried out. This is often done when the perpetrator knows the victim's secret. e. Article 362 of the Criminal Code concerning theft: The perpetrator is responsible for carding, where the victim's credit card number is used to make online purchases without actually owning the card itself. Once the transaction is complete and the product has been delivered, the seller tries to withdraw funds from the bank but is rejected because the cardholder is not the same person who made the purchase. The person making the purchase does not have the card. f. Article 378 of the Criminal Code concerning fraud: You can be prosecuted for fraud if you are suspected of selling a product or service by placing an advertisement on the website to attract interest and payment. Send money to advertisers. In reality, the goods sold do not exist. After paying for the goods that never arrived, the buyer was deceived. g. Article 406 of the Criminal Code concerning Destruction; Penalties can be imposed for defacing or hacking that interferes with someone else's system, such as a website or program (Hengki Irawan *et al*., 2024) [17]

To prevent cybercrime specifically, the Indonesian government made Law No. 11 of 2008 concerning information technology and electronics (Purnama Santhi & Nuarta, 2023) [31]. This law was made as an effort by the Indonesian government to protect the internet user community. This is regulated in the information technology and electronic law in article 5, paragraph (1) and or paragraph (2) of the ITE Law (*Internet Governance by Social Media Platforms – Science Direct*, n.d.). Law No. 11 of 2008 concerning information and electronic transactions as amended by Law No. 19 of 2016 (Agustini, 2019) [2] This law regulates cybercrime for the first time, especially in Articles 27 to 37 concerning Prohibited Acts and Articles 45 to 52 concerning the threat of imprisonment, with a maximum penalty of 12 (twelve) years in prison and a maximum fine of Rp. 2,000,000,000.00 (two billion rupiah) (Hengki Irawan *et al*., 2024) [17]

In addition to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) concerning Information and Electronic Transactions, which was amended into Law Number 19 of 2016, there is a Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems (Rahmat *et al*., 2023) [31]. Both are the main laws in Indonesia that regulate the protection of personal data ("The Fading Social Trust Capital Due to Cybercrime in E-Commerce Transactions in Indonesia: The Perspective of the Electronic Information and Transaction Law," 2022). These legal protections protect victims' rights, such as the right to be notified in the event of a data leak, the right to compensation, and other rights.

Victims of personal data leaks have several rights that are protected by these legal protections. First, they have the right to be notified in the event of a data leak involving personal information. This obligation helps electronic system operators become more transparent and accountable. Second, victims are entitled to compensation for losses caused by the dissemination of data. Victims can usually seek damages through adequate legal process, where they can sue the party responsible for negligence in protecting personal data. In addition, the right to file a complaint and get protection from the competent authorities is part of the legal protection for victims.

In Indonesia, the Ministry of Communication and Information Technology is responsible for receiving and handling complaints about personal data breaches. The Ministry of Communication and Informatics also has the authority to conduct investigations and take necessary actions against these violations. Victims will feel safer and have a way to seek justice if there is this mechanism (Alfi Salsabilah Idriansyah & Nur Afifah, 2024, p. 464) [4].

Obstacles in Cyber Crime Law Enforcement in the Digital Era

In general, the UU-ITE (Act No.14/2008) has the main objective to manage information and transactions electronically as well as to stipulate prohibited acts without specifying the principle of privacy. The role of this regulation is to tackle the growing of cybercrime (Hakim *et al*., 2018) [16]. Although cybercrime has been regulated in the law, its implementation still faces many challenges and obstacles. The ITE law does not explain in detail the description of the crime using computers. In this case, the perpetrator can look for an opening to commit a crime. In addition, the birth of the

ITE law has not been accompanied by regulations that control its formal law. Legal features in Indonesia are not enough to criminalize social media crimes (Broadhurst, 2006) [7].

Another challenge is the difficulty of identifying criminal evidence of cybercrime. This identification is very complicated because the crime is on social media. The problem of prosecuting cybercrime cases often encounters obstacles, especially in the arrest of suspects and the confiscation of evidence. In the arrest of suspects, law enforcement often cannot determine exactly who the perpetrators are because they do so simply by starting with a computer that can change its location without anyone knowing so that no witness knows directly. Meanwhile, in the confiscation of evidence, often the problem arises. Usually, the reporter is very slow in reporting, which means the attack data in the server log has been deleted; usually, it occurs in deface cases, so investigators have difficulty identifying (Sugiswati, 2011, p. 64) [35].

Identifying in the previous stage is very difficult because if identification is carried out, it will also affect the next stage in the examination stage of the victim and witnesses (*Identification and Application of Requirements and Their Impact on the Design Process: A Protocol Study | Research in Engineering Design*, n.d.)Obstacles in settling case files occur in the issue of evidence, which is not the same perception among law enforcement officials. This happens because of different interpretations of the content of the ITE law. In addition, the collection of digital evidence in cybercrime cases requires special expertise from computer experts.

Mohamad Revaldy Fairuzzen explained that the main obstacles in reducing cybercrime in Indonesia are: 1) Weak cyber legislation system in Indonesia: Cybercrime perpetrators cannot be fully prosecuted due to the weak cyber legislation system in Indonesia. 2) Limited human resources and infrastructure: Cybercrime perpetrators come from various countries, and limited human resources and infrastructure are the main obstacles. 3) Personnel limitations: Personnel limitations such as IT and cyber forensic experts are an obstacle for the National Police in tackling cybercrime. 4) Lack of understanding and lack of knowledge among the public contributes to obstacles in efforts to overcome cybercrime (Mohamad Revaldy Fairuzzen *et al*., 2024, p. 151) [25].

To overcome these challenges, improvement efforts are needed, including through: 1) Training and improvement of cybersecurity skills. 2) Establishment of a Special Law on Cybercrimes. Where the laws and regulations in the field of information technology that currently apply in Indonesia have not yet accommodated all cybercrimes, so several cybercrimes are currently a problem for security and defense that have not been regulated in national regulations. 3) Improvement of Human Resources. 4) Enhance global collaboration in the advancement and strengthening of cybersecurity capabilities. This includes developing and expanding the capacity of cybersecurity capabilities on a global scale, both in terms of infrastructure and resources (Muhammad Ghozali *et al*., 2024, p. 806) [27].

Strengthening cyber law in Indonesia is very important in order to fight for the country's defense. Therefore, this is a shared responsibility between interested subjects, namely the government, law enforcement officials, and all elements of society to combat cybercrime turmoil (Purnama Santhi & Nuarta, 2023, p. 24) [31].

Conclusion

The development of digital technology in today's society continues to increase very rapidly. Various new tools and technologies that have been discovered are very effective and efficient in helping and facilitating people's daily lives and activities. The development of digital technology also has an impact on the emergence of cybercrime. Cybercrime is increasingly developing in various fields such as economic, social, political, pornographic, and other fields. In Indonesia, cybercrime is regulated in the Criminal Code, law 11 of 2008 concerning Information and Electronic Transactions, which was amended into Law Number 19 of 2016 and a Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems. However, many challenges exist in enforcing cybercrime criminal law, such as a weak cyber legislation system in Indonesia, limited human resources and infrastructure, personnel limitations, and a lack of understanding and knowledge among the public in efforts to overcome cybercrime. For this reason, the support of various parties, both from the government, law enforcement, and the community, is needed to reduce cybercrime in Indonesia.

References

1. Sukharev AY, Shestak VA, Savenkova PG, LLC FINMARSH. Genesis of the notion “cybersecurity” in the fuel and energy sector of the European Union: Legal analysis. Vestnik of Saint Petersburg University. Law. 2024;15(3):866–881. doi: 10.21638/spbu14.2024.320.
2. Agustini P. Undang Undang Informasi dan Transaksi Elektronik. Ditjen Aptika. 2019 Aug 13. Available from: https://aptika.kominfo.go.id/2019/08/undang-undang-ite/.
3. Al-Amaireh MAA-M. The Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes. Revista de Gestão Social e Ambiental. 2024;18(8):e06508. doi: 10.24857/rgsa.v18n8-124.
4. Idriansyah AS, Afifah N. Perlindungan Hukum Terhadap Korban Cyber Crime di Indonesia dalam Aliran Hukum Pada Kasus Pencurian Data Pribadi. Media Hukum Indonesia. 2024;2(4):463–469. doi: 10.5281/zenodo.14209512.
5. Angkasa A, Wamafma F, Juanda O, Nunna BP. Illegal Online Loans in Indonesia: Between the Law Enforcement and Protection of Victim. Lex Scientia Law Review. 2023;7(1):119–178. doi: 10.15294/lesrev.v7i1.67558.
6. Besar. KEJAHATAN DENGAN MENGGUNAKAN SARANA TEKNOLOGI INFORMASI. Business Law. 2016 Jul 31. Available from: https://business-law.binus.ac.id/2016/07/31/kejahatan-dengan-menggunakan-sarana-teknologi-informasi/.
7. Broadhurst R. Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management. 2006;29(3):408–433. doi: 10.1108/13639510610684674.
8. Candiwan C, Azmi M, Alamsyah A. Analysis of Behavioral and Information Security Awareness among Users of Zoom Application in COVID-19 Era. International Journal of Safety and Security Engineering. 2022;12(2):229–237. doi: 10.18280/ijsse.120212.
9. Candiwan Candiwan, Machdar Rianda L. Transactions

at Your Fingertips: Influential Factors in Information Security Behavior for Mobile Banking Users. International Journal of Safety and Security Engineering. 2024;14(3):795–806. doi: 10.18280/ijsse.140312.
10. Danuri M. PERKEMBANGAN DAN TRANSFORMASI TEKNOLOGI DIGITAL. Jurnal Ilmiah Infokam. 2019;15(2).
11. Das S, Nayak T. IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES. International Journal of Engineering Sciences. 2019;6(2).
12. Hardiyanti DT, Harefa B, Bakhtiar HS, Supardi. Grooming Offences Againts Children in Indonesia. UUM Journal of Legal Studies. 2023;14(2):557–579. doi: 10.32890/uumjls2023.14.2.6.
13. Dewi Y, Suharman H, Koeswayo PS, Tanzil ND. Factors influencing the effectiveness of credit card fraud prevention in Indonesian issuing banks. Banks and Bank Systems. 2023;18(4):44–60. doi: 10.21511/bbs.18(4).2023.05.
14. Edoho FM. Information and communications technologies in the age of globalization. African Journal of Economic and Management Studies. 2013;4(1):9–33. doi: 10.1108/20400701311303131.
15. Fahamsyah E, Taniady V, Rachim KV, Riwayanti NW. Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention. De Jure: Jurnal Hukum dan Syar'iah. 2022;14(1):140–159. doi: 10.18860/j-fsh.v14i1.15731.
16. Hakim L, Kusumasari TF, Lubis M. Text Mining of UU-ITE Implementation in Indonesia. Journal of Physics: Conference Series. 2018;1007:012038. doi: 10.1088/1742-6596/1007/1/012038.
17. Irawan H, Paamsyah J, Feprizon H, Fatullah AP. Pengaturan Tindak Pidana Mayantara (Cybercrime) Dalam Sistem Hukum Indonesia. INNOVATIVE: Journal Of Social Science Research. 2024;4(1):4358–4369.
18. Identification and application of requirements and their impact on the design process: A protocol study. Research in Engineering Design. Available from: https://link.springer.com/article/10.1007/s00163-003-0033-5.
19. Imran MF, Gunawan H. The role of digital distrust, negative emotion and government policy on cyber violence during the digital era in Indonesia. International Journal of Data and Network Science. 2024;8(4):2581–2590. doi: 10.5267/j.ijdns.2024.5.001.
20. Indah F, Sidabutar A, Annisa N. Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum. 2022;1(1):77–87. Available from: https://ejournal.kreatifcemerlang.id/index.php/jbpi/article/view/78.
21. Internet governance by social media platforms. ScienceDirect. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0308596115000592.
22. Katyal NK. Criminal Law in Cyberspace. University of Pennsylvania Law Review. 2001;149(4):1003–1014. doi: 10.2307/3312990.
23. Djarawula M, Alfiani N, Mayasari H. Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) di Indonesia Ditinjau dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Jurnal Cakrawala Ilmiah. 2023;2(10):3799–3806. doi: 10.53625/jcijurnalcakrawalailmiah.v2i10.5842.
24. Marwan A, Garduño DO-C, Bonfigli F. Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia. BESTUUR. 2022;10(1):22. doi: 10.20961/bestuur.v10i1.59143.
25. Fairuzzen MR, Putra AA, Reihan A, Prihatini LH. Perkembangan Hukum dan Kejahatan Siber "Cybercrime" di Indonesia. Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory. 2024;2(1):139–153. doi: 10.62976/ijijel.v2i1.372.
26. Mokyr J. The Institutional Origins of the Industrial Revolution.
27. Ghozali M, Liana N, Afra C, Siregar Z, Nurfahni. Kejahatan Siber (Cyber Crime) dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI). CENDEKIA: Jurnal Hukum, Sosial & Humaniora. 2024;2(4):797–809. doi: 10.5281/ZENODO.13883603.
28. Nandiansyah A, Raihana, Raihana, Cheny B. Kesadaran Hukum Perlindungan Hak Cipta Bagi Pengguna Karya Cipta Sinematografi Pada Media Internet. SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum. 2022;1(2):77–87. doi: 10.55681/seikat.v1i1.235.
29. Pansariadi RSB, Soekorini N. Tindak Pidana Cyber Crime dan Penegakan Hukumnya. Binamulia Hukum. 2023;12(2):287–298. doi: 10.37893/jbh.v12i2.605.
30. Santhi NNP, Nuarta IN. Penguatan Penegakan Hukum Polri dalam Rangka Optimalisasi Penanggulangan Cybercrime di Indonesia. SCIENTIA: Journal of Multi Disciplinary Science. 2023;2(1):15–27. doi: 10.62394/scientia.v2i1.40.
31. Rahmat RF, Aziira AH, Purnamawati S, Pane YM, Faza S, Al-Khowarizm, Nadi F. Classifying Indonesian Cyber Crime Cases under ITE Law Using a Hybrid of Mutual Information and Support Vector Machine. International Journal of Safety and Security Engineering. 2023;13(5):835-844. doi: 10.18280/ijsse.130507.
32. Rosmaini E, Kusumasari TF, Lubis M, Lubis AR. Study to the current protection of personal data in the educational sector in Indonesia. Journal of Physics: Conference Series. 2018;978:012037. doi: 10.1088/1742-6596/978/1/012037.
33. Sabadina U. Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online. UII Yogyakarta. 2021;6.
34. Sanctions, Perceptions, and Crime: Implications for Criminal Deterrence. Journal of Quantitative Criminology. Available from: https://link.springer.com/article/10.1007/s10940-012-9170-1.
35. Sugiswati B. Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi di Era Informasi. Perspektif. 2011;16(1):59. doi: 10.30742/perspektif.v16i1.70.
36. The fading social trust capital due to cybercrime in e-commerce transactions in Indonesia: The perspective of the electronic information and transaction law. Edelweiss Applied Science and Technology. 2022;8(5):348-358. doi: 10.55214/25768484.v8i5.1692.

37. Zhang Y, Dong H. Criminal law regulation of cyber fraud crimes—From the perspective of citizens' personal information protection in the era of edge computing. Journal of Cloud Computing. 2023;12(1):64. doi: 10.1186/s13677-023-00437-3.