Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 8, 7230-7239-

Criminal Policy Against Credit Card Abuse In Realising Legal Protection For Banking

Hendra Wijaya, Edy Lisdiyono, Bambang Joyo Supeno

Faculty of Law, Universitas 17 Agustus 1945 Semarang, Jalan Pemuda No.72, Semarang City, Central Java 50133, Indonesia. , Email: wijayahendra.untag@gmail.com

ABSTRACT

This study aims to analyse the construction of the current credit card abuse criminal policy model and implement the credit card abuse criminal policy model in Indonesia. The results show that credit card abuse is not explicitly regulated by banking law, so the criminal provisions contained in the law cannot be applied to criminal acts of credit card abuse. This study uses a normative legal approach. The crime of misuse of credit cards has been committed by illegal means by referring to the Penal Code or Law number 19 of 2016 amending Law number 11 of 2008 concerning information and electronic transactions. Based on the assumption that the information contained in a credit card is classified as electronic information stored in a computer or electronic system, it is included in the regime of the law on electronic information and transactions.

Keywords: criminal policy, economic law, credit card abuse, legal protection, banking, Indonesia.

INTRODUCTION

Economic development in Indonesia in the context of national development is one of the efforts to realise the welfare of a just and prosperous society materially and spiritually evenly distributed based on Pancasila and the Constitution of the Republic of Indonesia (Maryano et al., 2021; Rifai et al., 2020). The increase in development activities also increases the need for available funds, most of which are obtained by meeting the payment needs of all sectors of the economy for credit activities (Hossain, 1988; Wilson, 2012).

The rapid development of the national and international economy accompanied by increasing challenges must be followed by the development the national banking system to fulfil its functions and responsibilities towards society (Lin, 2011; Rondinelli et al., 1983). The flow of globalisation, followed by the economy, science and technology development, has both positive and negative impacts (Prasad et al., 2005; Scott & Storper, 2003). The positive impacts of rapid development include creating various quality and technological goods (Bessant & Rush, 1995). The negative impact is marked by the growing crisis of moral values in society, which can increase the number of people against criminal law in various regions. The development of the national economy is constantly changing rapidly with more and more complex challenges (Marković, 2008). Therefore, various policy adjustments are needed in the economic sector to improve and strengthen the economy, including the banking sector (Hoskisson et al., 2000).

The object of this research study is a model credit card abuse criminal policy that offers legal protection to banking institutions and does not have a deterrent effect on perpetrators. As one of the economic sub-sectors, banking affects economic life and strategically positions it as a support institution for the payment system (Babajide, 2012). So, in this case, it impacts the lack of public confidence in banking institutions, which also leads to the destruction of banking institutions due to economic crimes in the banking sector.

The Model Credit Card Abuse Penalty Policy is necessary to provide credit card protection to customers. Given the many cases of credit card counterfeiting and fraud that often occur, seeking legal reform based on the values that live in society to prevent crime as early as possible. Possible. It is using the right approach, policy-oriented and all human values-oriented.

Starting from the description of the background above, the subject of this article revolves around the criminal policy model in the crime of credit card abuse. Credit card crime is a phenomenon in people's lives that cannot be separated from space and time. In this case, therefore, criminal law reform is necessary to suppress the growth rate of the crime rate with a simple analysis scheme. However, various optimisations need to be done in its implementation because, in reality, various gaps in Indonesian law have implications for less than optimal criminal law.

RESEARCH METHODS

Peter Mahmud Marzuki (2017) formulated legal research to discover the rule of law, legal principles, and legal doctrines to answer legal problems encountered. The research in this article is legal, a process of finding laws that regulate human social activities involving state-imposed rules and commentaries. Legal research does not need to start with a hypothesis because the terms independent variable and dependent variable are not known in legal research; therefore, there is no need for a hypothesis in legal research, and the term data is unknown.

The data collected will then be analysed. The data analysis that the researchers used in this study used qualitative analysis. Researchers use this qualitative analysis to describe information that is not explained quantitatively. However, the data is deemed necessary to support the search for answers to the research questions determined by the researchers above to that be presented more systematically method and written to resolve the issues that have been identified formula.

RESULTS AND DISCUSSION

Model Criminal Policy for Credit Card Abuse in Indonesia

Law enforcement against criminal acts of credit card abuse in Indonesia refers to penal policies through penalties based on the Penal Code or Law Number 19 of 2016 regarding Amendments to Law Number 11 of 2008 concerning information and electronic transactions with the personality concerned and company law (Fuad, 2021). Through these two laws, the types of acts charged with the offence of credit card abuse are regulated in the criminal provisions relating to counterfeiting (articles 263 and 264 of the penal code), theft (article 362 of the penal code), embezzlement (Section 372 of the Penal Code) and Section 32 (2) and Section 35 as amended by Law No. 19 of 2016 amending Law No. 11 of 2008 relating to electronic information and transactions, which focuses on illegal access to electronic data.

The formulation of criminal acts in the Penal Code is still largely conventional. It has not been directly related to the development of cybercrime. Besides, there are also various weaknesses and limitations in dealing with various technological developments and crimes of high technology widely. For example, the Criminal Code has difficulties with counterfeit credit cards and electronic funds transfers because there are no specific rules on this subject (Karo & Sebastian, 2019; Nugraha et al., 2015).

Electronic Information and Transactions Act No. 11 of 2008, Chapter VII Prohibited Acts, contains penal provisions for anyone who intentionally and unlawfully resists; Disseminate false and misleading news that results in losses for consumers in electronic transactions, disseminate information aimed at causing hatred or hostility towards individuals and/or certain community groups based on ethnicity, religion, Race and Intergroup (SARA); Sending information containing threats of violence or intimidation against persons (Article 29); access other people's computers and/or electronic systems, access

computers and/or electronic systems for the purpose of obtaining electronic information and/or electronic documents, access computers and/or electronic systems by violating , violating, exceeding or breaching system security (Section 30); Modify, add, reduce, transmit, destroy, delete, transfer, hide electronic information and/or electronic documents belonging to other people or public property, transfer or transfer electronic information and/or electronic documents to 'other unauthorised electronic systems which, the disclosure of electronic information and/or electronic documents of a confidential nature so that they are accessible to the public with the integrity of the data (article 32) (Sefitrios & Chandra, 2021; Sufriadi, 2021).

Disruption of the electronic system and/or resulting in a malfunction of the electronic system (Article 33); Produce, sell, cause to be used, import, distribute, make available or hold: computer hardware or software designed or specifically developed to facilitate the actions referred to in Article 27-33, computer password, other access code, or similar other types of material for the purpose of making the electronic system accessible for the purpose of facilitating the actions referred to in Articles 27 to 33 (Article 34); Manipulate, create, modify, delete, destroy electronic information and/or electronic documents with the aim that the electronic information and/or electronic documents are considered as if the data are authentic (article 35); Perform the acts mentioned in article 27-34 causing harm to others (article 36); and Performing prohibited acts as referred to in Articles 27 to 36 outside the territory of Indonesia against the Electronic System located in the territory of Indonesian jurisdiction (article 37).

The criminalisation of cybercrime in Indonesia, especially in the Electronic Information and Transactions act, can be divided into two categories: acts that use computers as a means of crime and acts that make computers a targeted criminal. Computer-as-a-medium crime is any action that uses computer data, computer systems, and computer networks as tools to commit crimes in cyberspace instead of real space (Bunga, 2019). A computer-targeted crime is any activity using a computer that targets computer data, computer systems, computer networks, or all three together (Zakaras, 2001). The act is performed in cyberspace, not real space, so all activities prohibited by laws and regulations occur in cyberspace (Brown & Poellet, 2012).

The criminal liability of cybercrime actors must also contain a sense of subjective censorship. It means that subjectively the perpetrator deserves to be reproached or blamed or responsible for the crime he has committed so that he deserves to be punished. In short, it is often said that there is no crime (criminal responsibility) without fault (principle of guilt). This principle of guilt must also be considered in terms of criminal liability in cybercrime. Although it may face challenges in cybercrime cases, it is not easy to prove that there is an element of guilt (dolus/culpa) in cybercrime cases (Mewengkang, 2021).

To investigate criminal acts in the field of information technology and electronic transactions. Article 42 of the ITE law stipulates that investigations into criminal acts referred to in this law are carried out based on the provisions of the criminal procedure code. This means that all provisions of the Code of Criminal Procedure and other laws relating to criminal procedure law apply in investigations to discover criminal acts in the cyber world. In addition to Indonesian National Police investigators, certain government officials whose duties and responsibilities lie in information technology and electronic transactions are granted special authority as investigators, as set out in criminal procedural law. Public Service Investigators are empowered to Receive reports or complaints. Summon any person or other party to be heard and questioned as a suspect or witness in connection with an alleged criminal act; Conduct a review of the report's accuracy or information. Conduct interviews of persons and business entities reasonably suspected of having committed a criminal act; Perform

inspections of tools and facilities related to information technology activities suspected of being used to commit criminal acts; Carry out excavations of certain places; Perform sealing and confiscation; Seek expert assistance for the investigation, and maintain the closure of the investigation.

The Electronic Information and Transactions Act stipulates that the investigation of criminal acts in the field of information technology and electronic transactions must be carried out with respect for the protection of privacy, confidentiality, the proper functioning of public (public) services, data integrity, or data integrity by the provisions of laws and regulations. Searches and confiscations of electronic systems related to suspected criminal acts must be carried out with the head of the local district court. When carrying out searches and confiscations, investigators are required to safeguard the interests of public services. When making arrests and detentions, investigators, through the Public Prosecutor's Office, are required to request a decision from the head of the local district court within twenty-four hours. In order to uncover criminal acts of electronic information and electronic transactions, investigators may cooperate with investigators from other countries to share information and evidence (Leroux, 2004). Evidence for investigation, prosecution and examination in court shall be in the form of evidence referred to in the legal provisions and evidence in electronic information and electronic documents (Dykstra, 2015; Kallil & Yaacob, 2019).

In the face of problems, whether in the form of violations or crimes, the international community sometimes uses punishment, whether in the form of States or international organisations. These facilities are used to address and prevent a situation that is considered to disturb the international community's sense of security, order and comfort, whether in violations or crimes. This penal tool can take the form of bilateral or multilateral conventions and take the form of resolutions initiated by an international organisation to be considered by its member countries to develop a new instrument to prevent and prevent international crimes. The regulations of the Draft Penal Code and the Electronic Information and Transactions Law still overlap, especially regarding the regulation or formulation of criminal acts related to cybercrimes. In most countries, cybercrime regulation (policy formulation) is incorporated into the Penal Code, although some place it in a separate law outside the Penal Code. Complex cybercrimes are often anticipated too late by law enforcement so that in the case of a new dimension, law enforcement has not been able to handle the case properly; even in some cases, it seems that the actions taken by law enforcement are reckless. For this reason, crime prevention does not have to use the criminal law as the only way out. For cybercrime prevention to be carried out more thoroughly, it goes through a legal or criminal approach and can also be carried out with a non-criminal approach (Lusthaus, 2013).

Implementation of Criminal Credit Card Abuse Policy Model in Indonesia

Credit card abuse consists of stealing the credit card data belonging to the cardholder, using various methods, either by committing fraud on the cardholder or by obtaining the card data directly without through the cardholder, such as breaking into the database to steal credit card data. Inside, the data is used to transact with merchants to obtain goods/services that can be sent directly to the debtor or sent to another party for resale and the profits obtained are shared between the debtor and a third party. In this act of abuse, it can be imposed in the Criminal Code as an effort to criminalise the crime of carding, namely: Article 362 and Article 363 of the Criminal Code regarding theft can be explained by a carder who steals data from the cardholder or from the database where the credit card data is stored; Article 363 may apply if the flight is conducted in a group; Article 378 of the criminal code regarding fraud, which is explained by phishing by carders, can be carried out by different methods

via e-mail, SMS, or telephones, such as the offer of goods/services, or d other forms of fraud; Articles 378 and 362 of the penal code may apply to cases of carding because the carder commits fraud as if he wants to buy an article and pays with a credit card whose credit card number is stolen; Article 263 of the Penal Code relating to counterfeiting applies if the debtor falsifies a credit card, even if the credit contains data from the original credit card; Articles 112, 113 and 114 of the penal code relating to state security apply to acts of breaking into database data; Section 322 and Section 323 are applied when there is an act of data leakage that should be protected by some officials/professions.

Carding is a form of cybercrime proliferating in Indonesia (Adhi & Soponyono, 2021). Therefore, the Indonesian police have responded by establishing a particular unit to combat cybercrime, namely the Cybercrime Directorate, Criminal Investigation Agency, Republic of Indonesia police. Members of the Special Division are trained to handle cybercrime cases and conduct investigations, and collect electronic evidence using special techniques. The phenomenon of cybercrime should be monitored because this crime is very different from criminal acts in general. Cybercrime can be perpetrated regardless of temporal and spatial boundaries and can be perpetrated without direct interaction with victims or potential victims. On the other hand, this crime has the potential to grow beyond other crimes; considering the rapid development of technology, when juxtaposed with available facts, the Indonesian National Police has formed a special division to deal with cybercrimes (Pratiwi, 2020).

Managing the crime of credit card abuse starts with understanding how the crime works (which in general has been depicted in the image above), then the critical point in law enforcement for the act of criminal credit card abuse lies in the policy of criminalising an act that was not originally a crime. Criminal acts (cannot be punished) becomes a criminal act. This policy of criminalisation is integrated into the criminal policy, which is exercised through penal law or can be stated as a penal policy. The problem of criminalisation arises because actions have new dimensions, so a legal question arises that applies to these actions; the next impression is a legal vacuum for these actions, which ultimately underlies the criminalisation of these actions (Westen, 2007). Basically, in cybercrime issues, there is no legal vacuum; it happens when a method of interpretation known in legal science is used, which should be used as a guide for law enforcement officials in the treatment of acts that have a new dimension that has not been regulated explicitly in law (Brenner, 2006; Holt, 2018). It will be different if there is a political decision to stipulate cybercrime in separate legislation apart from the Penal Code or other special laws. Judging from the definition of criminalisation does not have to take the form of special laws outside of the Criminal Code; it can also be done in the halls of the Criminal Code through amendments. The indecisiveness of the Indonesian legal system, which does not adhere to a complete codification system, has led to the emergence of various special laws (Butt & Parsons, 2014; Juwana, 2003).

The execution of criminal acts in Indonesia, apart from relying on the Penal Code, also refers to Law No. 19 of 2016 Amending Law No. 11 of 2008 Regarding Electronic Information and Transactions, in particular Article 31, paragraphs (1) and (2) which involves the act of interception or wiretapping of information in the form of credit card data, including card number, date of validity, CCV, name of cardholder and others. The act was committed to using technology in the form of software to extract data from the database; in addition to being classified as an illegal act, the act also threatens state security.

Enforcement of the law against credit card abuse is identical to the method used by the authors. However, it is generally strongly linked to electronic information and transactions law because authors are highly dependent on technology, especially the

Internet, by committing crimes. Using this technology, perpetrators commit fraud, forgery, and theft with a credit card as the primary container. Law enforcement officials enforce these criminal acts through penitentiary institutions based on the Penal Code and the Electronic Information and Transactions Act, the police, prosecutors and courts. The following is an analysis of decisions in handling criminal cases related to credit cards, namely South Jakarta District Court Decision No. 1193 / Pid. B/2013/PN. Jkt.

Defendant's Misuse of Credit Cards; through South Jakarta District Court Decision No. 1193/Pid.B/2013/PN.Jkt.Sel, it can be seen that criminal sanctions were issued by sentencing Suri Anni with a term of imprisonment of 2 (two) years and Thiam Kim with imprisonment for 1 (two) years, one year.

The verdict above shows that the type of crime used is the major crime with the type of imprisonment and a fine. Credit card abuse is still not considered a severe consequence crime that must be considered. The implementation of the criminal provisions in the case mentioned above shows that the criminal (criminal) law was used to deal with the credit card crimes committed by the defendant. The application of the article of the Penal Code should bring benefits to the victim, namely that, although it cannot return the goods or materials belonging to the victim, it can at least bring a feeling of inner satisfaction to the victim. Victims, in the form, punish the accused. Criminal law is the ultimate recourse (last means), and criminal law with penal means limits the fight against crime. Penitentiary institutions are considered to operate after the crime has been committed, so the criminal law cannot function optimally as a deterrent before the crime occurs, therefore, to prevent crime or credit card fraud.

As the holder of the supervisory authority for the banking sector in Indonesia, Bank Indonesia is interested in improving the protection of customers vis-à-vis banks or, in this case, card issuers. Therefore, Bank Indonesia, about this protection, established the Indonesian Banking Architecture (API), which the Governor of Bank Indonesia launched on January 9, 2004, which is a national banking system master plan consisting of 6 (six) pillars to realise the vision of a healthy, sound and efficient banking system to create stability in the financial system to encourage national economic growth. The six pillars are a sound banking structure, an effective regulatory system, an independent and effective control system; a strong banking sector; adequate infrastructure; and customer protection.

The legal basis used by Bank Indonesia to develop regulations and implement policies is Banking Law No. 7 of 1992 as amended by Law No. 10 of 1998 and Law No. 23 of 1999 concerning Bank Indonesia, as amended by Law No. 3 of 2004, where the aspect of legal protection in the banking world lies in the prudence of the banks.

The legal protection of cardholders refers to the Consumer Protection Act number 8 of 1999. This consumer protection law has resulted in the expansion of banking regulations to protect and empower customers as consumers who use banking services. Considering the effective period of the consumer protection law, it can be seen that Bank Indonesia is less responsive to the enactment of the law. However, this does not mean that Bank Indonesia does not consider customer protection and empowerment.

Cardholders, under Section 1 of the Consumer Protection Act Number 8 of 1999, maybe classified as consumers, having regard to the definition of consumers under the act, persons who use goods and services that exist in society, both for themselves, their families, as well as other people who are not trafficked (Syahril, 2021). The customer is a who is a person or business with a current account or a deposit account or other similar savings account in a bank (Cheney & Rhine, 2006). Thus, it is clear that credit cards are banking products to qualify cardholders as consumers.

The existence of the Consumer Protection Act provides a legal basis and framework for banking activities through credit cards so that cardholders can feel safe and protected. In addition, it also enables the government and

related institutions to organise, encourage and educate consumers/cardholders so that the role of consumers in the world of commerce, banking and the like can work smoothly optimal (Barkatullah, 2019).

The existence of legal protection through the Consumer Protection Act cannot solve abuses. Misuse of credit cards can lead to material and immaterial losses (Tejomurti et al., 2018). This abuse can be committed by other parties not involved in the credit card agreement or by parties directly involved in the agreement. This implies that the legal protection in the credit card agreements encounters many obstacles; several factors become obstacles to the legal protection of the credit card agreements, in particular, the holder of the credit card, namely :

1. The commercial actor factor, the problem that may arise on this site is the possibility that the author has made a mistake occurred in the credit card transaction, such as not receiving transfer proof from the actor commercial or the problem of transferring funds that do not reach the credit card user.
2. The credit card owner factor is due to the negligence of the card user, which can be caused by many factors, including the owner's inability to use credit cards properly, as stated in the 'OK'.
3. Other factors include misuse of technology by irresponsible parties; technological constraints due to system incapacity; VSAT (vertical satellite network) conditions; insufficient human resources; the absence or inability of the role of the parties who should be responsible for a valid credit card agreement.
4. Legal factors so far, there has been no legislation that regulates credit cards and their misuse explicitly. However, Law Number 11 of 2008 regarding Electronic Information and Transactions considers that many criminal acts of credit card abuse are related to electronic transactions while the legal instruments used deal specifically with the issue. Under Article 51 of the Information and Electronic Transactions Act No. 11 of 2008, it can only regulate credit card abuse through the modus operandi of card re-embossing, courier delivery/consignee, or the customer) and use.

The legal protection against misuse of credit cards by Indonesian law has not been able to cover all forms/methods of misuse. This certainly can cause tangible and intangible losses to consumers/customers/cardholders and cause similar losses and more to card issuers and merchants. Especially in Indonesia, it may further impact Indonesia's economic, security, and legal issues. Apart from that, people will lose their sense of security and protection to use credit cards, one of the banking products.

The criminal policy model of credit card abuse in Indonesia is enforced through a criminal approach through litigation using the Penal Code and the Electronic Information and Transactions act for charges of forgery, theft or fraud, or illegal access to the data of others. Via computers or Internet networks. This can be observed in the District Court decision no. 1193/ Pid.B/ 2013/ PN.Jkt.Sel, District Court decision no. 673/ Pid.B/2017/ PN.Jkt.Sel, and District Court Decision No. 1570/Pid.B/2016/PN.JKT.PST, respectively, use Section 363, Section 378 and Article 263 of the Penal Code. From the three rulings, it can be seen that the three cases received only relatively favourable rulings, such as in District Court ruling no. 673/ Pid.B/2017/ PN.Jkt.Sel declared that the defendant was guilty and was only sentenced to a prison term of 2 (two) years, while the maximum prison term provided in article 378 of the Penal Code is three years.

CONCLUSION

The implementation of the criminal policy model of credit card abuse in Indonesia relates

to the implementation of credit card activities that are not regulated by the banking law so that the misuse of credit cards cannot be charged with criminal provisions in the law. As in the act of misuse of credit cards for cash transfer business, which is actually through Bank Indonesia regulations: 11/11/PBI/2009 regarding implementation card payment instrument activities, it is prohibited to do so because basically credit cards are provided for the purchase of goods/services, even if withdrawals are made. Cash on the card is allowed, and withdrawal is limited to a specific limit. The criminal policy model for enforcing the criminal acts of credit card abuse has been enforced through penitentiary institutions with types of sanctions in the form of criminal penalties, including prison sentences. Imprisonment or fines are executed alternately or cumulatively and with different penalties.

Enforcement of the law against credit card abuse is identical to the method used by the authors. However, it is generally strongly linked to electronic information and transactions law because authors are highly dependent on technology, especially the Internet, by committing crimes. Using this technology, perpetrators commit fraud, forgery, and theft with a credit card as the primary container. Law enforcement officials enforce these criminal acts through penitentiary institutions based on the Penal Code and the Electronic Information and Transactions Act, the police, prosecutors and courts.

Penal means as a model of criminal policy. The practical implications of this research are a contribution for legislators in order to be able to reform the banking law or the penal code for the future, given that credit card crimes are not explicitly regulated by any law, in particular those who use credit cards. Also, for the public, this research can bring thoughts and insights related to the concept of punishment in Indonesia, especially regarding credit card abuse in Indonesian laws and regulations.

REFERENCES

1. Adhi, M. I. P., & Soponyono, E. (2021). Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law. Law Reform, 17(2), 135–144. https://doi.org/10.14710/lr.v17i2.41736
2. Babajide, A. A. (2012). Effects of microfinance on micro and small enterprises (MSEs) growth in Nigeria. Asian Economic and Financial Review, 2(3), 463–477.
3. Barkatullah, A. H. (2019). Hukum Transaksi Elektronik di Indonesia: Sebagai pedoman dalam menghadapi era digital Bisnis e-commerce di Indonesia. Nusamedia.
4. Bessant, J., & Rush, H. (1995). Building bridges for innovation: The role of consultants in technology transfer. Research Policy, 24(1), 97–114. https://doi.org/10.1016/0048-7333(93)00751-E
5. Brenner, S. W. (2006). Cybercrime jurisdiction. Crime, Law and Social Change, 46(4), 189–206. https://doi.org/10.1007/s10611-007-9063-7
6. Brown, G., & Poellet, K. (2012). The Customary International Law of Cyberspace. Strategic Studies Quarterly, 6(3), 126–145. JSTOR.
7. Bunga, D. (2019). Legal Response to Cybercrime in Global and National Dimensions. PADJADJARAN Jurnal Ilmu Hukum (Journal of Law), 6(1), 69–89. https://doi.org/10.22304/pjih.v6n1.a4
8. Butt, S., & Parsons, N. (2014). Judicial Review and the Supreme Court in Indonesia: A New Space for Law? Indonesia, 97, 55–85. JSTOR. https://doi.org/10.5728/indonesia.97.0055
9. Cheney, J. S., & Rhine, S. L. (2006). Prepaid cards: An important innovation in financial services. Citeseer.

10. Dykstra, J. (2015). Seizing electronic evidence from cloud computing environments. In Cloud Technology: Concepts, Methodologies, Tools, and Applications (pp. 2033–2062). IGI Global.
11. Fuad, A. N. (2021). Misuse of Credit Cards or Carding in Indonesia: How is the Law Enforced? Law Research Review Quarterly, 7(1), 83–96. https://doi.org/10.15294/lrrq.v7i1.43165
12. Holt, T. J. (2018). Regulating Cybercrime through Law Enforcement and Industry Mechanisms. The ANNALS of the American Academy of Political and Social Science, 679(1), 140–157. https://doi.org/10.1177/0002716218783679
13. Hoskisson, R. E., Eden, L., Lau, C. M., & Wright, M. (2000). Strategy in Emerging Economies. Academy of Management Journal, 43(3), 249–267. https://doi.org/10.5465/1556394
14. Hossain, M. (1988). Credit for alleviation of rural poverty: The Grameen Bank in Bangladesh (Vol. 65). Intl Food Policy Res Inst.
15. Juwana, H. (2003). Dispute resolution process in Indonesia. Institute of Developing Economies.
16. Kallil, M. K., & Yaacob, A. (2019). The integration of digital forensics science and Islamic evidence laws. International Journal of Law, Government and Communication, 4(17), 61–70.
17. Karo, R. K., & Sebastian, A. (2019). Juridical analysis on the criminal act of online shop fraud in Indonesia. Lentera Hukum, 6, 1.
18. Leroux, O. (2004). Legal admissibility of electronic evidence. International Review of Law, Computers & Technology, 18(2), 193–220. https://doi.org/10.1080/13600860420000223508
19. Lin, J. Y. (2011). New Structural Economics: A Framework for Rethinking Development. The World Bank Research Observer, 26(2), 193–221. https://doi.org/10.1093/wbro/lkr007
20. Lusthaus, J. (2013). How organised is organised cybercrime? Global Crime, 14(1), 52–60. https://doi.org/10.1080/17440572.2012.759508
21. Marković, M. R. (2008). Managing the organizational change and culture in the age of globalization. Journal of Business Economics and Management, 9(1), 3–11. https://doi.org/10.3846/1611-1699.2008.9.3-11
22. Maryano, Mulyadi, L., & Ogan, M. (2021). Adat Penal Decision in The Indonesia Legal Practice. Proceedings from the 1st International Conference on Law and Human Rights, ICLHR 2021, 14-15 April 2021, Jakarta, Indonesia.
23. Marzuki, P. M. (2017). Penelitian Hukum. Prenada Media.
24. Mewengkang, I. B. (2021). Kajian Yuridis Cyber Crime Penanggulangan Dan Penegakan Hukumnya. Lex Crimen, 10(5), 26–35.
25. Nugraha, E., Akub, S., Rifai, B., & Arie, M. (2015). Renewal of Criminal Law Against Abuse of Credit Cards. Journal of Humanity, 3(2), 92956.
26. Prasad, E., Rogoff, K., Wei, S.-J., & Kose, M. A. (2005). Effects of Financial Globalization on Developing Countries: Some Empirical Evidence. In W. Tseng & D. Cowen (Eds.), India's and China's Recent Experience with Reform and Growth (pp. 201–228). Palgrave Macmillan UK. https://doi.org/10.1057/9780230505759_9
27. Pratiwi, E. I. (2020). Law Enforcement Efforts against the Crime of Body Shaming Through Mediation.

Pancasila and Law Review, 1(2), 101–110. https://doi.org/10.25041/plr.v1i2.2127

28. Rifai, A., Syamsuddin, M. M., & Maharani, S. D. (2020). Pancasila as foundation and goals of Indonesia's human development in the President Jokowi era. Research, Society and Development, 9(8), e258985177. https://doi.org/10.33448/rsd-v9i8.5177
29. Rondinelli, D. A., Nellis, J. R., & Cheema, G. S. (1983). Decentralization in developing countries. World Bank Staff Working Paper, 581, 13–28.
30. Scott, A., & Storper, M. (2003). Regions, Globalization, Development. Regional Studies, 37(6–7), 579–593. https://doi.org/10.1080/0034340032000108697a
31. Sefitrios, S., & Chandra, T. Y. (2021). The Process and Performance of Combating Cyber Crimes In Indonesia. SALAM: Jurnal Sosial Dan Budaya Syar-i, 8(4), 975–986. https://doi.org/10.15408/sjsbs.v8i4.21795
32. Sufriadi, Y. (2021). Prevention Efforts Against E-Commerce Fraud Based on Indonesian Cyber Law. 2021 9th International Conference on Cyber and IT Service Management (CITSM), 1–6. https://doi.org/10.1109/CITSM52892.2021.9588900
33. Syahril, Muh. A. F. (2021). Perlindungan Hukum Terhadap Nasabah Pengguna Kartu Automatic Teller Machine. JUSTISI, 7(1), 52–65. https://doi.org/10.33506/js.v7i1.1159
34. Tejomurti, K., Hadi, H., Imanullah, M. N., & Indriyani, R. (2018). Legal Protection for Urban Online-Transportation-Users' Personal Data Disclosure in the Age of Digital Technology. Padjadjaran Journal of Law, 5(3), 485–505. https://doi.org/10.22304/pjih.v5n3.a5
35. Westen, P. (2007). Two Rules of Legality in Criminal Law. Law and Philosophy, 26(3), 229–305. JSTOR.
36. Wilson, T. A. (2012). Supporting Social Enterprises to Support Vulnerable Consumers: The Example of Community Development Finance Institutions and Financial Exclusion. Journal of Consumer Policy, 35(2), 197–213. https://doi.org/10.1007/s10603-011-9182-5
37. Zakaras, M. R. (2001). International computer crimes: General report. Revue internationale de droit pénal, 72(3–4), 813–829. Cairn.info. https://doi.org/10.3917/ridp.723.0813