Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers

by M. Afif Hasbullah

Submission date: 26-Mar-2023 11:33AM (UTC+0700)
Submission ID: 2046575313
File name: 1_Afif_IJCC_119_130.pdf (441.04K)
Word count: 6481
Character count: 37730

Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers

M. Afif Hasbullah[1]
Universitas Islam Darul Ulum, Lamongan, Indonesia

Abstract

The current research aims to analyze the effects of cybercrime on business laws and its Implications for businesses and consumers. The purpose of conducting this study is to check the direct impact of cybercrimes on business laws and business laws on businesses and consumers. This research is conducted to focus on the several business laws prevailing in Indonesia and highlight the importance of business laws for any business. For data collection, the research has adopted secondary data collection. Reviewing previous literature from the past five years and relevant case studies is crucial for the given study. The collected data was then analyzed based on how other businesses implement the business laws and protect themselves and their consumers from cybercrimes. Lastly, this study has discussed several theoretical and practical implications and directions for future researchers.

Keywords: Cybercrime, Business Laws, law, Consumer laws, ITE.

1. Introduction

The perks and privileges of Digitalization in Business are now transforming into threats and challenges which need immediate attention by security lawmakers. Although digital developments in different sectors are increasing, the perceived threats are creating a challenging security environment (Parn & Edwards, 2019). Businesses are now exposed to serious cyber-security risks, which indeed is an alarming sign. Christiansen and Piekarz (2018) identified the gaps between the need for a modern digital environment and its prone threats. The tuned policies for cyber security dealings lack exposure in the political, social, economic, and criminological background. The dark side of the cyber-space is invading the privacy of workplaces and posing an acute business risk to the running of worldwide enterprises (Lubis & Handayani, 2022). Nowadays, effective business performance is chiefly regulated by digital competitive factors. Industries with cyber-security issues fall back and face multiple challenges in business development (Hacioglu & Sevgilioglu, 2019). Security experts claim that ASEAN countries are entering into a

[1] Faculty of Law, Universitas Islam Darul Ulum, Lamongan, Indonesia.
E-mail: afif@unisda.ac.id

new age of digital warfare due to the increasing cases of digital theft and cyber-attacks in those regions. Southeast Asia needs strict security measures and laws to curb the concentration of such crimes in those regions. The security policies and frameworks also need to be reformed through cyber diplomacy and ensure cyber resilience in Asian regional businesses (Hacioglu & Sevgilioglu, 2019). The data from APJII (Indonesian Internet Service Provider Association) highlights that the users of the internet are growing faster than ever in Indonesia. The number of Indonesian internet users was around 51.5 percent of the total population, which, on the one hand, is good as people are able to enjoy technology information, while on the other hand is dangerous because its negative impacts can't be avoided (Fahlevi et al., 2019). In this accordance, the act of Indonesian criminal procedure contains administrative law. With this idea, the act of punishing cybercrime or preventing them is enhanced. Marwan and Bonfigli (2022) state that administrative law analyzes the implementation of regulations related to cybercrime. Indonesian administrative law number 11 and 19 specify criminal offenses, which include illegal interception, gambling, defamation, and pornography. This administration figured out the implementation of the law that enforces Indonesian criminal procedure to work on a cybercrime case. Subsequently, as the digital market is increasing its impacts legal updates are becoming crucial to analyze and control the impacts of digitalization. Umanailo et al. (2019) bring forth that ever since the cybercrime has existed, and they present their worse effects in Indonesia. The country is now on a list of top countries involved in cybercrime. With the increase in crimes and continuous complaints related to it, the Indonesian wing implemented the telematics law, which is supposed to take control of worsening cybercrime situations in the country (Butkovic et al., 2019). Due to the high rate of these crimes in Indonesia, the cyber world now blacklisted the procedure of payment providers through the internet (Wiyono & Manthovani, 2019). The existing literature has highlighted that cyber-criminals who misuse technological advancements pose a serious threat to business laws and law enforcement agencies. Various countries have introduced multiple channels to control the issues of cybercrime. In this regard, practitioners proposed a request for a cyber-security bill to define the role of various institutions in dealing with the threats of cybercrimes. Although numerous studies highlight the deep impacts of cybercrime on various emerging economies, no such study has existed till far which bring forth the impact of cybercrime on the business laws of Indonesia. Therefore, this study tends to fill this gap by identifying how the business law of Indonesia is affected by cybercrime and how this serious emerging threat creates implications for businesses and their consumers. Regarding objectives, the present study aims at examining the impact of cybercrimes on ongoing business in Indonesia. The role of cyberspace trends and the effectiveness of cyber security and business laws in shaping the values of businesses and consumers. In contemporary world economies, consumers are more prone to cyber-security threats, therefore the need to address business concerns and their customers is crucial in Indonesian context. Keeping in view the fact that there are plenty of research bodies available, the present deviates from the prior studies in analyzing Indonesian cyber laws, acts and regulation.

2. Literature Review

The worldwide crime investigations of recent years witnessed an extreme upsurge in cyber security issues. Holt, Bossler, and Seigfried-Spellar (2017), in "Cybercrime and Digital Forensics," provided a comprehensive insight into the nature of cybercrimes, their determinants, facilitators, and outcomes. Technology has a massive impact on human behaviors and is unluckily abused by them in the present day. The misapplication of digital natives results in cyber terrorism, cyber deviance, and cyber security threats (Suša Vugec & Stjepić, 2022). The loopholes in digital pathways are allowing criminals to establish crime forums. On the other hand, the same forums are also used for securing credential knowledge and Information. As indicated by Pastrana et al. (2018), the "CrimeBot" is used by CrimeBB to record huge datasets, which is a crude way to safeguard intellectual property rights. The surveys worldwide in recent years yielded the results that cybercrimes are among the most practiced fraud in countries with developed economies and technologies. The National Statistics in Europe located six major types of cyber crimes, including bank payments, cyber harassment, data hacking, and malware. The data revealed that the victims of online stalking stand at 1%, privacy breached by hacking at 1-6%, while issues of malware crimes are estimated at 2-15% (Reep-van den Bergh & Junger, 2018). With digital advancement, crime patterns are too changing as the increasing commoditization of cyber-crimes is declared alarming. Commoditization became a potential threat to the economies as it minimized the barrier and made digital invasion easy for aspiring criminals (Van Wegberg et al., 2018). The criminal activities facilitated by specialized customers made the global market lucid in business services. Though the prior studies found convincing evidence of commoditized forms of cyber-attacks in online markets, much research is required on the changing cyber trends in the contemporary digital world. As cyber-security is a social, political, legal, and ethical concern, the need to highlight these factors in Asia-Pacific Regions is stressed by Sarre, Lau, and Chang (2018). The past literature (Chatterjee et al., 2019; Lin & Nomikos, 2018) covers the global north and developed economies, and the scarcity of literature in the Asian region is making room for devoted researchers in the domain of digital criminology. The lack of digital awareness and cyber security investment in the Asian Region is targeting the vulnerabilities of the digital world and therefore needs to be addressed with acute consideration.

Contemporary Business policies and values are designed to keep a proper check on digital exposures and their respective threats. As the internet is a chief enabler of criminal activities, the MNEs and large organizations are more prone to cyber security threats due to their information flow across the border via digital platforms. The loss of credential information via cyber-crimes puts the organization's reputation at stake and badly influences the working units' propositions (Enderwick, 2019). Therefore, the business laws embed cybercrime laws to protect business values and citizens. UAE, in this regard, took proactive measures against cyber-attacks and designed "cyber security laws and legislation" to safeguard the values of business workspaces. Apart from cyber laws, strict penalties are proposed in curbing cyber terrorism, i.e., deportations, financial penalties, and jail terms (Younies & Al-Tawil, 2020). In combating cybercrimes, businesses and law enforcement agencies share mutual responsibility. As the countries of the Asian region, mainly ASEAN countries, became

the hub of criminal activities, Chang (2020) reviewed the legal measures taken by these countries in fighting e-commerce digital security threats. The cybercrime laws formed by Northeast Asian countries and favored by Business policymakers. Cyber security regulations, for instance, Federal Information Security Management Act (FISMA), safeguard small business interestss by developing an alignment between Federal agencies and Business lawmakers (Tracy, 2007).

Large businesses face fewer challenges in deploying cyber security measures, whereas small companies become easy targets of cyber threats. The cyber-resilience of such businesses is determined by their legal infrastructure, resource/information protection, and organizational policies maturity Tam, Rao, and Hall (2021). Consumer Privacy Protection Act (2017) and SHIELD ACT(2020) are the most recent cyber security law and regulations which reduced the cyber security threats up to two folds in the USA. Emerging US companies are successfully implementing these laws to cut down on cyber-attacks (Solove & Schwartz, 2020). Many businesses also use Third-Part Vendors, which can ensure information privacy to some extent. Still, the need for single comprehensive privacy law is the need of time in tackling the privacy risks of evolving businesses (Stark, 2022). The review of the past literature heightened the need to address cyber-related issues to maintain the integrity, privacy, values, and information of businesses worldwide, especially in Indonesia, where increased cyber-terrorism cases are becoming a potential threat to digital safety and security.

3. Acts and laws of Indonesian Cyber Crime

Cyber conduct directs the cyber laws as per rules in the entire world. As the nature of cybercrimes differs, the acts and laws are always subject to modification. The cyber security surveys demonstrated that the types of cyber-attacks are advancing with digital innovations. At the beginning of the 20th century, the initial reporting of cyber-related issues witnessed Morris Code, Malicious Code, and Advanced worm as the most notable cyber-crimes (Ngo et al., 2020). With the advent of technology, hijacking, and Cyberwarfare emerged as potential threats to organizations and Institutions (Christianto, 2020).

The Cyber laws deal with respective cyber activities and decide penalties (Sarmah, Sarmah, & Baruah, 2017). Three major areas collectively form Indonesian Cyber Law; 1)Media Law, 2) Informatics Law, and 3) The Law of Telecommunication. The three of them form the base of the implicit cyber law anatomy. The principles of these laws generate the criteria of the cyber security conditions and the limitations. Indonesia's cyber-handling legal framework is mainly based on the "Indonesian Criminal Code" and "Electronic Information and Transactions Law." The ITE law is the most widely practiced form of cyber security law, which has serious challenges and problems. Machmuddin and Pratama (2017) identified the loopholes in ITE law. Within this law, multiple acts are formed, among which Black's Law is the most problematic. The law has certain deviations in defining the nature of cyber threats and, therefore, cannot be applicable countrywide. All the cybercriminals' evaluations also fall under the UUITE, which has almost 11 articles and deals with more than 22 types of cybercriminal conducts. Article 27 of ITE defines and sets the boundaries of cyber-space activities.

According to that, the violation of ethical decency while managing the information of a third party would be subjected to cyber-crime punishment. The same article also

demonstrated that the case of intentionally transmitting or transferring the credential information comes under the charge of defamation and insult. Article 28 of UUITE sets the condition that can subject the person to a penalty. Spreading or misusing information based on regional, ethnic, and racial prejudices is also labeled a cyber-security crime (Lubis & Fajri Achmad, 2010). Article 29 deals with the leakage of residential information and threatening documents that come under micro-level security misconduct. Articles 30 and 31 deal with the security system breakage of any electronic system and invites cyber-crime law enforcement to act accordingly (Koto, 2021). The violation of these cyber-security terms under the condition of guilty would be liable to certain penalties, which are discussed under articles 45-51 (Saputra, 2016). Article 45 referred to the penalties of Article 27, where the financial payback is one billion rupiahs.

About Article 28, the penalty is set as one billion amount and a maximum of six years of imprisonment. Article 51, about article 35, sets the penalty of 12 billion rupiahs with imprisonment of 12 years (Siregar & Lubis, 2021). In 2014, the government issued Law Number 11/2008 to define the nature of cybercrimes and respective penalties. The Intellectual Property right act of 2002 was also directed with the aim of minimizing the numbers of cybercrimes. The above-discussed articles and outlined in accordance with the Law Number 11 of the 2008 (McBride, 2002). Seeing the increasing number of cyber-crime issues in Indonesia, the law-enforcement agencies facing a blow due to their inability to make the cyber law effective. Despite following Criminal code and Law Number, the security of institutions are continuously breached by the cyber criminals. However the need to revise non-penal policies are the in-time need of the hour.

4. Indonesia's business laws regarding cybercrime

The growth of technology has caused significant economic, cultural, and social advancement and changes. Although information and technology have provided several benefits to businesses and society. But the negative impacts of technology cannot be avoided (Fahlevi et al., 2019). This increasing trend of information and technology in Indonesia has caused the rapid emergence of cybercrimes over the internet (Mauladi, Laut Mertha Jaya, & Esquivias, 2022). Due to the rapid advancement and development in technological advancement and cybercrime, the government of Indonesia has made several efforts and taken many measures in order to protect against the internet or cybercrimes and has made many policies, regulations, and enacting laws (Amarullah, Runturambi, & Widiawan, 2021). In regard to the specific scope of the cyber legislation in Indonesia, the laws have been categorized into private and public areas of law (Saputra et al., 2019). The public area of cyber law covers cybercrime, data protection, and consumer privacy, and the private area of cyber law covers electronic contracts, intellectual property, cybersquatting, and e-commerce any as such. These laws have many purposes and are held accountable for how people use, communicate and interact over the internet (Koto, 2021). The cyber law or ITE law in Indonesia was built up by converging three major areas or pillars: the law of informatics, media law and telecommunications law (Riwanto, 2022). Indonesia has not recognized law informatics and media laws, and the cyber law concept in Indonesia has placed in existing positive law contestation

(Amin & Huda, 2021). Law informatics and media laws in Indonesia are associated with intellectual property rights, and these are also associated with press laws and telecommunication laws (Rohayati et al., 2022). Formed its basis on the major pillars of cyber law in Indonesia, it must be inherited into the ITE law, but in reality, it is not inherited into such. According to Anggono and Firdaus (2020), the principle of law that only considers and runs specific laws and regulations is the sectorial law principle. Therefore, the ITE law is held unaccountable for the cybercrimes occurring in Indonesia. Besides having a systematic and legal interpretation, the urgency of the cyber regulation law presented in 2008 is extremely high and required in the country because there is a lack of proper law for cyber-related crimes (Mutiarin, Pribadi, & Rahmawati, 2022).

Consequently, the ITE law has lost its focus on information and technology and digital transactions (Octora, Sewu, & Sugiono, 2021). Although, from its name, it is interpreted that the ITE law must have its major focus on information and electronic transactions and not regulate any other aspect, such as hate speech, defamation, gambling, and an interception. There is some problem in the cyber law of Indonesia (Sefitrios & Chandra, 2021). Legal experts disagree the cyber terminologies prevailing in Indonesia due to many reasons. Its major reason is the cyber terminology used in the law (Setiyawan & Satria, 2021). Its differences are reflected in the legislation. The concept of cyber was considered as virtual or something illusion or imaginary. In response to this situation, the court judge of the Indonesian Constitutional Court has decided that it is crucial to understand that cyber is media that has been utilized in order to perform any activity and task that has an impact on people's lives in the real world (Christianto, 2020). The legislation and laws prevailing in Indonesia related to the protection of data are way far behind international cyber laws and legislation. Indonesia still has to pass a comprehensive cyber law to reduce and stop the number of cybercrimes in the country. Currently, data protection's primary regulations are being concerned under the law of the Government Regulation Concerning Electronic Systems and Transaction Providers (82/2012) and the law of Electronic Information Technology (11/2008). As there are many legislations in the legal framework of Indonesia related to cybersecurity and cybercrime and those regulations have passed many standardized checks and depend upon different areas of laws and specific incidents. Still, after many efforts, Indonesia needs a proper cyber law (Marwan & Bonfigli, 2022).

5. Influence of cybercrime and Indonesia's business laws on businesses and consumers

Cybercrime can cause many issues for individuals as a customer, consumers, and businesses (Abdullah, 2020). They can lead to severe financial damages. In today's world, and especially after the Covid-19 pandemic, most businesses have made their online presence apart from having a physical presence (Gryllakis & Matsiola, 2022). Although online businesses are so much in trend and have many potential benefits for the consumers and the firms, for instance, it reduces costs, saves time and effort, etc. But it has brought many negative impacts, and one of the major among them is cybercrimes over the internet networks. Online businesses have emerged many challenges for Indonesia's businesses (Setyowati, Widayanti, & Supriyanti, 2021). In

this regard, customer trust is crucial for any business to earn revenues and gain higher market shares and competitive advantage over its competitors. The fear of perceived risk and cybercrime associated with the business has become a challenge for consumers. And it has been seen that Indonesian businesses (specially e-businesses) have an emerging challenge to prevent them from cybercrimes and gain the trust of the consumers (Anggusti, 2022). Suppose any business is found to be included in any cybercrime activity and breaches personal security and harms the personal data of its customers. In that case, this may cause a serious problem for the business as the customers will no longer trust such business. Also, the business could lose its reputation and customers, too. Cybercrimes tend to harm the long-term stability of businesses. So, the businesses that ensure the cyber laws and regulations and always tend to keep the data and privacy of their customers secure are more sustainable and competitive than others (Odhomi, 2021). According to Anggusti (2022), cybercrime has a strong and direct impact on business laws and customers. Cybercrimes affect the purchasing intentions and purchasing decisions of Indonesian customers. Customers' intentions and purchase decisions are influenced greatly when they know businesses are not following legal practices or being involved in any unethical and unlawful acts. Thus, the customers' modified attitudes negatively impact the business growth and profitability, resulting in business failure and huge losses. According to Li, Yao, and Chen (2021), consumers tend to purchase goods and services from reliable and secure businesses that follow legal regulations and laws.

Customers' intentions have changed over time, and they also realized the importance and significance of purchasing the product from a regulated business. Astuti, Khasanah, and Yoestini (2020) have described that Indonesian consumers are not pleased and satisfied with online purchasing, so cybercrime is much more challenging for businesses in Indonesia. Tawalbeh et al. (2020) further added that consumers are less likely to purchase from businesses that compromise their personal information and breach privacy concerns. Moreover, according to Babić Rosario, De Valck, and Sotgiu (2020), businesses that do not follow the legislation and do unlawful acts will create a negative word of mouth that negatively affect the business's profitability, revenues, and goodwill. It has been reported by Yuan and Peluso (2020) that a business must be bound legally and follow the country's business laws. If not, the customers will develop a negative attitude and behavior towards such businesses, and may avoid purchasing from the, resultings in the failure of a business. It has been noticed that the legal problems between the consumers and businesses have shifted their association in a negative way, as a consequence of which the businesses lost their market shares (Anggusti, 2022).

6. Conclusion

The purpose of the present study was to investigate the effects of cybercrime on business laws and the Implications for businesses and consumers. In this regard, the study has discussed the importance of business and cyber laws for businesses, consumers, and society. The study has analyzed the impact of cybercrimes on business laws, specifically in Indonesia. The paper has further discussed several business laws, including ITE law, laws for intellectual property rights, e-commerce-related laws, and cyber regulation laws. The article has discussed the importance of

the implementation of business laws in their business practices in necessary because they contain all the relevant sections of the legislation that are either directly or indirectly related to the businesses, their establishment, agreement, growth and development, logistic management, transactions, and several multinational business operations and dealings. Business laws are vital because they protect businesses and consumers from any unlawful act or misconduct in the corporation (Parella, 2021). It is a crucial component for running a business, so any market or business requires its unique business laws. The paper has further analyzed the emergence of cybercrimes in the Indonesian markets because the country has no such comprehensive and active cyber law, and the existing laws that deal with crimes are not very active and effective in dealing with crimes that are occurring through the internet. That is why the paper has suggested that it requires an hour to have a comprehensive and active cyber law in Indonesia so that the cybercrimes can be eradicated or lessened.

6.1 Theoretical and Practical Implications

The current study has several practical and theoretical implications that make it both worthy and creditable. Firstly, this study has discussed the research gap not discussed before in the body of knowledge. Secondly, the study enhanced the existing literature on the knowledge of cybercrime and business laws, both generically and specifically in Indonesia. The study has also demonstrated that the Indonesian government should develop modern business laws and cybercrime-related laws, especially for the smooth and secure running of e-businesses because, with the predefined laws and regulations, Indonesian businesses and consumers are not much satisfied and experiencing cybercrimes that are harming both the businesses and the consumers.

6.2 Limitations and Future Directions

The study also has a few limitations that give future directions to the researcher. First, the study has selected the country of investigation Indonesia, so the research is of narrower scope and cannot be applied globally. So, it is advised for future researchers to select any other nations like UAE, MENA region, South Asian countries, etc., to study these variables. Another limitation of this study is that this study has adopted the mechanism of reviewing the existing literature regarding business acts and laws implemented in Indonesia, so for the analysis, the data has been collected quantitatively, but it could be done as a mixed research method including both perspectives, i.e., quantitative and qualitative so it would give a more detailed analysis of the observed variables.

References

Abdullah, H. (2020). Proposition of a framework for consumer information privacy protection. In *2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems* (pp. 1-6). IEEE. https://doi.org/10.1109/icABCD49160.2020.9183822

Amarullah, A. H., Runturambi, A. J. S., & Widiawan, B. (2021). Analyzing cyber crimes during Covid-19 time in Indonesia. In *2021 3rd International Conference on Computer Communication and the Internet (ICCCI)* (pp. 78-83). IEEE. https://doi.org/10.1109/ICCCI51764.2021.9486775

Amin, M. E., & Huda, M. K. (2021). Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia. *International Journal of Cyber Criminology, 15*(1), 79-94. https://doi.org/10.5281/zenodo.4766534

Anggono, B. D., & Firdaus, F. R. (2020). Omnibus law in Indonesia: A comparison to the United States and Ireland. *Lentera Hukum, 7*(3), 319-336. https://doi.org/10.19184/ejlh.v7i3.19895

Anggusti, M. (2022). Cybercrime Change Consumers' Purchase Intention in Indonesia: A Moderating Role of Corporate Social Responsibility and Business Law. *International Journal of Cyber Criminology, 16*(1), 20–39. https://doi.org/10.5281/zenodo.4766554

Astuti, S. R. T., Khasanah, I., & Yoestini, Y. (2020). Study of impulse buying on Instagram users in Indonesia. *Diponegoro International Journal of Business, 3*(1), 47-54. https://doi.org/10.14710/dijb.3.1.2020.47-54

Babić Rosario, A., De Valck, K., & Sotgiu, F. (2020). Conceptualizing the electronic word-of-mouth process: What we know and need to know about eWOM creation, exposure, and evaluation. *Journal of the Academy of Marketing Science, 48*, 422-448. https://doi.org/10.1007/s11747-019-00706-1

Butkovic, A., Mrdovic, S., Uludag, S., & Tanovic, A. (2019). Geographic profiling for serial cybercrime investigation. *Digital Investigation, 28*, 176-182. https://doi.org/10.1016/j.diin.2018.12.001

Chang, L. Y. C. (2020). Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 327-343). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_6

Chatterjee, S., Kar, A. K., Dwivedi, Y. K., & Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: from a citizen's perspective. *Information Technology & People, 32*(5), 1153-1183. https://doi.org/10.1108/ITP-05-2018-0251

Christiansen, B., & Piekarz, A. (2018). *Global cyber security labor shortage and international business risk*. IGI Global. https://doi.org/10.4018/978-1-5225-5927-6

Christianto, H. (2020). Measuring cyber pornography based on Indonesian living law: A study of current law finding method. *International Journal of Law, Crime and Justice, 60*, 100348. https://doi.org/10.1016/j.ijlcj.2019.100348

Enderwick, P. (2019). Understanding cross-border crime: the value of international business research. *critical perspectives on international business, 15*(2/3), 119-138. https://doi.org/10.1108/cpoib-01-2019-0006

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime business digital in Indonesia. *E3S Web of Conferences, 125*, 21001. https://doi.org/10.1051/e3sconf/201912521001

Gryllakis, N., & Matsiola, M. (2022). Digital audiovisual content in marketing and distributing cultural products during the COVID-19 pandemic in Greece. *Arts and the Market*. https://doi.org/10.1108/AAM-09-2021-0053

Hacioglu, U., & Sevgilioglu, G. (2019). The evolving role of automated systems and its cyber-security issue for global business operations in Industry 4.0. *International Journal of Business Ecosystem & Strategy, 1*(1), 01-11. https://doi.org/10.36096/ijbes.v1i1.105

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics: An introduction*. Routledge. https://doi.org/10.4324/9781315296975

Koto, I. (2021). Cyber Crime According to the ITE Law. *International Journal Reglement & Society (IJRS), 2*(2), 103-110. https://doi.org/10.55357/ijrs.v2i2.124

Li, Y., Yao, J., & Chen, J. (2021). The negative effect of scarcity cues on consumer purchase decisions in the hospitality industry during the COVID-19 pandemic. *International Journal of Hospitality Management, 94*, 102815. https://doi.org/10.1016/j.ijhm.2020.102815

Lin, L. S. F., & Nomikos, J. (2018). Cybercrime in East and Southeast Asia: The Case of Taiwan. In A. J. Masys & L. S. F. Lin (Eds.), *Asia-Pacific Security Challenges: Managing Black Swans and Persistent Threats* (pp. 65-84). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-61729-9_4

Lubis, M., & Fajri Achmad, M. (2010). Information and electronic transaction law effectiveness (UU-ITE) in Indonesia. In *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010* (pp. C-13-C-19). IEEE. https://doi.org/10.1109/ICT4M.2010.5971892

Lubis, M., & Handayani, D. O. D. (2022). The relationship of personal data protection towards internet addiction: Cyber crimes, pornography and reduced physical activity. *Procedia Computer Science, 197*, 151-161. https://doi.org/10.1016/j.procs.2021.12.129

Machmuddin, D. D., & Pratama, B. (2017). Some of Indonesian Cyber Law Problems. *Journal of Physics: Conference Series, 801*(1), 012089. https://doi.org/10.1088/1742-6596/801/1/012089

Marwan, A., & Bonfigli, F. (2022). Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia. *Bestuur, 10*(1), 22-32. https://doi.org/10.20961/bestuur.v10i1.59143

Mauladi, K. F., Laut Mertha Jaya, I. M., & Esquivias, M. A. (2022). Exploring the link between cashless society and cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy, 10*(3), 58-76. https://doi.org/10.18080/jtde.v10n3.533

McBride, M. S. (2002). Bioinformatics and intellectual property protection. *Berkeley Technology Law Journal, 17*(4), 1331. https://www.jstor.org/stable/24116745

Mutiarin, D., Pribadi, U., & Rahmawati, D. E. (2022). Overseeing Cyber-Neighborhoods: How Far the Indonesian National Police Effort in Handling Cybercrime? In *International Conference on Public Organization (ICONPO 2021)* (pp. 549-555). Atlantis Press. https://doi.org/10.2991/aebmr.k.220209.070

Ngo, F. T., Agarwal, A., Govindu, R., & MacDonald, C. (2020). Malicious Software Threats. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 793-813). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_35

Octora, R., Sewu, P. L. S., & Sugiono, J. A. (2021). Regulation on electronic system security for E-wallet in order to protect consumers from financial loss due to cyber fraud based on Indonesian law. *International Journal of Social Science And Human Research, 4*(9), 2272-2279. https://doi.org/10.47191/ijsshr/v4-i9-01

Odhomi, E. E. (2021). *The Operative Level Perception of Cyber crime (Threats and Prevention) in a Logistic Company.* (Bachelor's thesis). Satakunta University of Applied Sciences. https://urn.fi/URN:NBN:fi:amk-202105138657

Parella, K. (2021). Protecting third parties in contracts. *American Business Law Journal, 58*(2), 327-386. https://doi.org/10.1111/ablj.12184

Parn, E. A., & Edwards, D. (2019). Cyber threats confronting the digital built environment. *Engineering, Construction and Architectural Management, 26*(2), 245-266. https://doi.org/10.1108/ECAM-03-2018-0101

Pastrana, S., Thomas, D. R., Hutchings, A., & Clayton, R. (2018). Crimebb: Enabling cybercrime research on underground forums at scale. In *Proceedings of the 2018 World Wide Web Conference* (pp. 1845-1854). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland. https://doi.org/10.1145/3178876.3186178

Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime Science, 7*(1), 1-15. https://doi.org/10.1186/s40163-018-0079-3

Riwanto, A. (2022). Construction of Legal Culture Model for Corruption Prevention Through Social Media in Indonesia. *Jurnal Hukum dan Peradilan, 11*(3), 385-404. http://dx.doi.org/10.25216/jhp.11.3.2022.385-404

Rohayati, Y., Bangkara, B. A., Fkun, E., Iskandar, A., & Jacob, J. (2022). Understanding the Roles and Challenges of Local Government in the Era of Technological Transformation in Indonesia: A Study of Public Policy Literacy. *ARISTO, 10*(3), 566-590. http://dx.doi.org/10.24269/ars.v10i3.6303

Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP). *Central European Journal of International & Security Studies, 13*(4), 104–120. https://doi.org/10.51870/CEJISS.XKVV3716

Saputra, R. W. (2016). A survey of cyber crime in Indonesia. In *2016 International Conference on ICT For Smart Society (ICISS)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICTSS.2016.7792846

Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cyber crime and cyber laws of India. *International Research Journal of Engineering and Technology (IRJET), 4*(6), 1633-1640. https://www.southcalcuttalawcollege.ac.in/Notice/50446IRJET-V4I6303.pdf

Sarre, R., Lau, L. Y.-C., & Chang, L. Y. C. (2018). Responding to cybercrime: current trends. *Police Practice and Research, 19*(6), 515-518. https://doi.org/10.1080/15614263.2018.1507888

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. http://dx.doi.org/10.15408/sjsbs.v8i4.21795

Setiyawan, R., & Satria, U. (2021). Indonesian Online Shopping Practices in the COVID-19 Pandemic Era: A Study of Culture and Cyber Security Law. *Jurnal Hukum Novelty, 12*(1), 29-44. http://dx.doi.org/10.26555/novelty.v12i01.a16944

Setyowati, W., Widayanti, R., & Supriyanti, D. (2021). Implementation of E-business Information System in Indonesia: Prospects and Challenges. *International Journal of Cyber and IT Service Management, 1*(2), 180-188. https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/49

Siregar, G., & Lubis, M. R. (2021). Juridical Analysis of Religious Blasphemy Crimes Through Smartphone Application Based on the Information and Electronic Transaction. *Journal of Contemporary Issues in Business and Government, 27*(2), 1006-1012. https://doi.org/10.47750/cibg.2021.27.02.120

Solove, D. J., & Schwartz, P. M. (2020). *Information privacy law*. Aspen Publishing.

Stark, R. (2022). The Role of Digital Technology Vendors. In R. Stark (Ed.), *Virtual Product Creation in Industry: The Difficult Transformation from IT Enabler Technology to Core Engineering Competence* (pp. 465-506). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-64301-3_19

Suša Vugec, D., & Stjepić, A.-M. (2022). Digital Literacy of Digital Natives. In C. Machado (Ed.), *Technological Challenges: The Human Side of the Digital Age* (pp. 61-91). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-98040-5_3

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Computers & Security, 109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

Tawalbeh, L. a., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences, 10*(12), 4102. https://doi.org/10.3390/app10124102

Tracy, R. P. (2007). IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards. *Information Systems Security, 16*(2), 114-122. https://doi.org/10.1080/10658980601051706

Umanailo, M. C. B., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., Daulay, P., Meifilina, A., Alamin, T., & Fitriana, R. (2019). Cybercrime Case As Impact Development Of Communication Technology That Troubling Society. *International Journal of Scientific & Technology Research, 8*(9), 1224-1228. https://www.ijstr.org/final-print/sep2019/Cybercrime-Case-As-Impact-Development-Of-Communication-Technology-That-Troubling-Society.pdf

Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Ganan, C. H., Klievink, B., Christin, N., & Van Eeten, M. (2018). Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets. In *Proceedings of the 27th USENIX Security Symposium* (pp. 1009-1026). USENIX Association. http://resolver.tudelft.nl/uuid:fc38dcc0-c3b9-404e-8c12-f71ac5b4130d

Wiyono, P., & Manthovani, R. (2019). Nationalization as a Threat to the Economy Market in Visa and Mastercard Business in Indonesia. *Journal of Critical Reviews, 7*(1), 159-166. http://dx.doi.org/10.22159/jcr.07.01.28

Younies, H., & Al-Tawil, T. N. e. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime, 27*(4), 1089-1105. https://doi.org/10.1108/JFC-04-2020-0055

Yuan, B., & Peluso, A. M. (2020). The impact of electronic entrepreneur-related word of mouth on brand evaluation. *Journal of Brand Management, 27*(5), 579-592. https://doi.org/10.1057/s41262-020-00200-y

Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers

ORIGINALITY REPORT

9%	6%	6%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	journals.publicknowledgeproject.org Internet Source	2%
2	Anum Khan, Muhammad Shujaat Mubarik, Navaz Naghavi. "What matters for financial inclusions? Evidence from emerging economy", International Journal of Finance & Economics, 2021 Publication	1%
3	Submitted to Old Dominion University Student Paper	1%
4	kjss.sports.re.kr Internet Source	1%
5	M Afif Hasbullah. "Legal Policy of Independent Learning Independent Campus (MBKM) Program in Indonesia: Tracing the Literature", AL-ISHLAH: Jurnal Pendidikan, 2022 Publication	<1%
6	digitalcommons.csumb.edu Internet Source	<1%

7	Submitted to University of Maryland, University College Student Paper	<1%
8	tel.archives-ouvertes.fr Internet Source	<1%
9	link.springer.com Internet Source	<1%
10	Mochammad Fahlevi, Mohamad Saparudin, Sari Maemunah, Dasih Irma, Muhamad Ekhsan. "Cybercrime Business Digital in Indonesia", E3S Web of Conferences, 2019 Publication	<1%
11	jhcls.org Internet Source	<1%
12	bradscholars.brad.ac.uk Internet Source	<1%
13	Enrique Bigne, María Lilibeth Fuentes-Medina, Sandra Morini-Marrero. "Memorable tourist experiences versus ordinary tourist experiences analysed through user-generated content", Journal of Hospitality and Tourism Management, 2020 Publication	<1%
14	fe2fbe8f-93c0-40a9-b260-f48c7e108fa6.filesusr.com Internet Source	<1%

15	www.legalbites.in Internet Source	<1%
16	www.tdx.cat Internet Source	<1%
17	www.tisc.rs Internet Source	<1%
18	www.crimejusticejournal.com Internet Source	<1%
19	journalppw.com Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		