LEGAL BRIEF
ISSN 2722-4643 (Online) | 1979-522X (Print)
Volume 13, No. 5, 2024, pp. 1194-1201
Published by: IHSA Institute (Institut Hukum Sumberdaya Alam)

Legal Protection for Victims of Business Email Compromise Crimes

Laksana Budiwiyono Lie

Program Magister Ilmu Hukum, Universitas Pancasila, Jakarta, Indonesia

Abstract: Business Email Compromise (BEC) is increasingly rampant in Indonesia, with significant impacts on financial losses and data security. This cybercrime exploits weaknesses in email systems and the lack of vigilance among companies to steal sensitive information. This research uses normative juridical methods and literature study to analyze the applicable legal framework, law enforcement processes, and protection efforts for BEC victims. The research results show that although Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) provide a legal basis, both have limitations in specifically addressing BEC. Law enforcement faces challenges in terms of digital evidence and perpetrators who often operate abroad. To enhance legal protection for victims, it is recommended to revise regulations, strengthen law enforcement capacities, and undertake prevention efforts through public education and cooperation with the private sector.

Keywords: Business Email Compromise, Legal Protection, ITE Law, PDP Law

1. Introduction

Information technology has come to be a major driving force of transformation in one area or the other of the economy, education and governance. Besides electronically making business processes and communication easier (Musriko & Febriansyah, 2024), (Fauzi et al., 2023). Digitalization also has great influence on financial transactions and operations in a company. Email is a clear example of a major use of communication resources in the business arena. Email is very easy way not just for the locals but also the rest of the globe to exchange info in a more or less fast and fast way. While this advancement is also accompanied by its own fair share of challenges, in this case, it's the challenges of cybersecurity (Kamal & Rafiah, 2021), (Kamariah, Rania, Harpijah, Ikhsan, & Pramuja, 2024). There are many variations (some serious) in the scope of technology-based crimes. A growing threat is Cyber Crime, such as Business Email Compromise (BEC), in which perpetrators attempt to trick someone or a company into doing one thing, and often stealing funds or information (Agazzi, 2020). BEC comes in many varieties, including takes over of email accounts, impersonating trusted parties in order to execute financial transaction manipulations (Cross & Gillett, 2020).

They have consistently caused financial and reputational losses to BECs. The losses due to BEC are reported on a global scale to be in the billions of dollars per year. This threat is not just confined to Indonesia as well. BEC is a hard crime to measure accurately because the crime is complex and hard to detect, and many small to large companies have fallen prey to the crime (Scanio, 2024), (Fauzi et al., 2023) (Sudarmanto, 2023). In addition, the public and business actors' lack of knowledge on the value of being cybersecured increases the risk of becoming a victim of this crime. The legal instruments used by Indonesia normatively on the regulation and protection of Indonesian society from cybercrime threats, including BEC (Azzani, Purwantoro, & Almubaroq, 2023). The Information and Electronic Transactions (ITE) Law or Law No. 1 of 2024 is the fundamental legal foundations for any matter concerning information technology (from breach in the transmission of data to e-transactions). Aside from that, the Personal Data Protection Law Number 27 / 2022 (PDP Law) has also mandated personal data protection in any of information crime, including BEC. However, these laws exist on paper rather than in

Correspondence:
Name: Laksana Budiwiyono Lie
Email : laksana@ieee.org

Received: Nov 07, 2024;
Revised: Nov 17 2024;
Accepted: Nov 25, 2024;
Published: Dec 30, 2024;

practise. Despite allowing the prosecution of cyber criminals, the ITE Law does not expressly criminalise BEC. The current regulations are usually formulated based and do not cover any special protection mechanisms for this victim's crime. Like the PDP Law, which is intended to protect personal data, it actually puts more emphasis in data governance rather than directly protecting the victim of cybercrime (Kalesaran, 2022).

The limitations leave holes that criminals can take advantage of. Where victims are cheated out of their BEC, they often cannot seek justice because of problems in the law enforcement process like not having enough evidence or not being able to prove electronic evidence. On top of that, perpetrators are often transnational, complicating efforts at tracking and law enforcement. In addition, law enforcement faces a slew of challenges. Significant obstacles are the lack of deep understanding of cybercrime, poor digital forensic technology and poor coordination between law enforcement agencies. Unfortunately, in many cases victims do not only lose material but are not indemnified in adequate measure. The level of these developments reveals that the protection of BEC victims in Indonesia is still very serious. In addition to developing more effective regulations focused on this crime, we also need to strengthen law enforcement capabilities and increase awareness by the public on issue of cybersecurity. It is hoped these measures can minimise the threat of BEC and give justice to the BEC victims according to Indonesian laws.

2. Materials and Methods

This view of protection through the legal means takes a normative juridical method by analysing legal provisions for a protection of Business Email Compromise (BEC) victims. The objective of this method is primarily an overview of some primary legal texts similar to Information and Electronic Transactions Law No. 1 of 2024 and Personal Data Protection Law No. 27 of 2022. In addition, the approach looks at secondary (books, journals, scholarly articles) and tertiary (legally produced materials such as court rulings, jurists' opinions etc.) legal materials in order to fully understand some legal concepts that are used. This research through literature study examines effectiveness and limitation of legal protections for BEC victims based on various regulations, doctrines, and legal literature in Indonesia. It is analysed qualitatively using a descriptive analytical approach of the collected data. How far can these procedural legal provisions contained in the ITE Law and PDP Law bring BEC perpetrators to trial and protect victims of BEC is the focus of the researcher. The analysis also includes making legal in gaps, law enforcement obstacles and international comparative studies to adopt best practises from other countries. By adopting this approach, the study seeks to offer an overall picture of the strengths and deficits of Indonesian legal framework in prosecuting BEC crimes and to suggest measures to improve the legal protection of victims.

3. Results and Discussion

3.1. Analysis of the Applicable Legal Framework and Its Limitations

Business Email Compromise (BEC) is a major cybercrime that is being committed more now than ever before, costing companies and individuals thousands of dollars (Bahri, 2023). In fact, the regulation, which is the main legal framework to protect BEC cases in Indonesia, is Law No. 11 Year 2008 concerning Information and Information Transactions (ITE Law), as amended by law Number 19 Year 2016. This law controls different forms of cyber crime such as a crime concerning the manipulation of electronic information (Febriansyah, 2023). Indeed, related provisions of the ITE Law, which are relevant for prosecution of BEC perpetrators, include Article 30 on illegal access into electronic systems as well as Articles 35 and 36 on manipulation of electronic data to harm someone else. Article 45A, paragraph (1), further provides criminal sanctions for persons who use data in a fraudulent manner to achieve unlawful economic gain.

Business Email Compromise (BEC) is a major cybercrime that is being committed more now than ever before, costing companies and individuals thousands of dollars

(Bahri, 2023). In fact, the regulation, which is the main legal framework to protect BEC cases in Indonesia, is Law No. 11 Year 2008 concerning Information and Information Transactions (ITE Law), as amended by law Number 19 Year 2016. This law controls different forms of cyber crime such as a crime concerning the manipulation of electronic information. Indeed, related provisions of the ITE Law, which are relevant for prosecution of BEC perpetrators, include Article 30 on illegal access into electronic systems as well as Articles 35 and 36 on manipulation of electronic data to harm someone else. Article 45A, paragraph (1), further provides criminal sanctions for persons who use data in a fraudulent manner to achieve unlawful economic gain.Business Email Compromise (BEC) is a major cybercrime that is being committed more now than ever before, costing companies and individuals thousands of dollars (Bahri, 2023). In fact, the regulation, which is the main legal framework to protect BEC cases in Indonesia, is Law No. 11 Year 2008 concerning Information and Information Transactions (ITE Law), as amended by law Number 19 Year 2016. This law controls different forms of cyber crime such as a crime concerning the manipulation of electronic information. Indeed, related provisions of the ITE Law, which are relevant for prosecution of BEC perpetrators, include Article 30 on illegal access into electronic systems as well as Articles 35 and 36 on manipulation of electronic data to harm someone else. Article 45A, paragraph (1), further provides criminal sanctions for persons who use data in a fraudulent manner to achieve unlawful economic gain.

A comparative analysis of China's experience with other countries shows that defining and making the measures to fight BEC cases even more specific and exhaustive can improve the efficiency of combating this crime. For instance, the United States equally uses the Computer Fraud and Abuse Act (CFAA) as legal backing in apprehending cyber criminals and offenders of BEC inclusive. The CFAA also provides specific sections on unauthorised computer access, computer fraud, and consequences of computer crime together with legal remedy for victims. Also, in response to BEC crimes, the United States has created an organisation called the Cybersecurity and Infrastructure Security Agency that offers recommendations and leadership to those who own businesses to shield against BEC crimes (Hoshmand & Ratnawati, 2023). Criminal justice comparisons with other countries suggest that increased clear and expansive rules for considering BEC instances can increase the efficiency of handling this crime. For instance, the United States through the Computer Fraud and Abuse Act (CFAA) has strong legal framework through which it prosecutes cybercrimes inclusive of BEC.

The CFAA describes specific provisions for the unauthorised access, electronic fraud, and the consequences arising from computer crime schemes together with the remedies for the survivors. Also, the United States has put in place the Cybersecurity and Infrastructure Security Agency (CISA) that helps organisations prevent BEC crimes by offering direction and training to them (Muhammad Rifqi Noval, 2024). In the EU digital single market regulation, the GDPR provides tighter control of data protection for individuals, regulations and reporting of cyber incidents within a certain period, and penalties for the failure of protecting data (Ramadhani, 2022). This regulation goes a long way in reducing the likelihood of cybercrime, which is in turn reduces BEC. Furthermore, as it will be recalled from earlier sections, the GDPR entitles victims to seek compensation where misuse occurs or when losses are incurred. These practises can be a benchmark for Indonesia to enhance its legal architecture (Yurizal & others, 2018). Some changes or supplements of the provisions of the ITE Law are required to pertain to the BEC crimes or to contain the provisions regarding the compensation for the victims. In addition, there is a need to enhance capacity in digital forensics of law enforcement, as well as enhancing public awareness of the modus operandi of the BEC criminals. Consequently, Indonesia may establish a legal environment that is more sensitive to cybsercriminal threats and ensure the appropriated safeguard of BEC victims at the same time.

3.2. Law Enforcement against BEC Crimes and Its Challenges

To fight BEC an elaborated process with several stages must be executed, which starts from victim's report and ends with court decisions. This kind of cybercrime, which commonly involves the breaking into business email accounts in order to perform fraudulent financial transactions, is particularly problematic for police agents in many countries around the world. The flow starts from when the victim or those affected by the criminal conduct including corporations or ay other person who has incurred a financial loss, report the commission of the crime to the police, a prosecutor or any other law enforcement agency. These reports are normally accompanied by some form of preliminary material such as electronic copy, e-mails and/or bank statements and the like that give rise to an investigation. Police are supposed to gain further evidence and bring to light the culprits. . This investigative phase may employ enhanced electronic evidence to analyse servers, user mail logs and header information, the hardware in connexion with this. They assist in mapping the trails that the offenders create by following them, and revea[ing the processes used in the crime. After collecting sufficient material, the record of the case is sent back to the prosecutor, who draws up the legal part of the case for trial. An attorney has to draw a charge depending on the evidence that is at his or her disposal and also make sure that he or she present the sides case before the judiciary in proper manner. The court in particular assess all evidence and arguments of the prosecution and the defence before delivering judgment.

However, and as stated above, there are structured stages that need to be followed when dealing with BEC crimes and its laws face a number of formidable hurdles. One of the main challenges is the fact that these are transnational offences. Criminals often act simultaneously in different jurisdictions to use servers and networks in several states to hide their tracks. This hampers detection and arrest because the police go through various legal matters, which they recognise are not easy because they involve dealing with foreign law enforcement. Also, there is the permanently advancing use of intelligent anonymization methods and encrypted contacts that complicate tracking activities. As acknowledged by law enforcement experts, BEC crimes pose challenges, not the least because the nature of the evidence usually consists of digital information indicated in the study by Situmeang (2020). The new forms of data, which are critical in constructing a legal case, may be erased, altered or encoded. Such evidence usually needs recovery and authentication which is a complex technicality that sometimes may not be easily provided by the police. Also, the technological trend of cybercrime activities and products makes the improvement of officers' knowledge and instrument highly important.

Nationwide, the allocation of resources makes it almost impossible to manage the emerging BEC cases. Some of the factors common to many police organisations including the Indonesian police force are inadequate physical infrastructure, and disparate human resources specialised in computer crime investigation. Due to the constantly increasing advancement and occurrence of these crimes, the specialised units assigned to enforcement of these laws and handling of these crimes, for instance the Cybercrime Directorate (Dittipidsiber) within the Indonesian National police, are sometimes overwhelmed. On the prosecution front too there are some challenges as well. Some of the prosecutors, who are supposed to draw up sensible charges and also plead the case in court, may lack the adequate backstage knowledge to make sense of technology-intensive proofs. This gap can eros the legal arguments and bring down the prospects of a successful conviction(Mahendra, 2022). The judiciary also has a number of challenges of its own. It means that judges are to consider complex evidence and arguments where many aspects involve sort of intricate technical peculiarities that contribite to cybercrime processes and, thus, call for a polymath decision.

Nationally as well as internationally, there is need for better coordination amongst the law enforcement agencies as a result of these challenges. At the national level, governments have not built efficient cooperation between police, prosecutors, and the judiciary organs leading to delay or even a gap in legal processes. The structures from these institutions need to improve on the handling of cases hence the need for improvement in

the collaboration and communication. Internationally, this is even more so given that most of the BEC crimes are international in nature. There are other international agencies for example Interpol and regional agencies like ASEANAPOL that help in cross border cooperation, sharing of intelligence and helping track and nab the cross border criminals. These objectives can, of course, be complemented by bilateral treaties between countries that adjust rules for extradition and mutual legal assistance. Nevertheless, the main obstacle in international cooperation still lies in the synchronisation of the jurisdictional criteria and the legal norms(Hutabarat et al., 2023).

Only in this way is it possible to overcome the named obstacles and enhance the efficiency of law enforcement activity in the sphere of BEC crimes. First, improvement of equipment overhauls of law enforcement agencies is the primary need. This includes purchase of better forensic equipment and creation of post graduate courses in forensic science to acts as a reference to investigators, prosecutors, judges, magistrates and other judicial persons. Such skills should be given to these professionals so that they are well equipped to deal with digital evidential and cybercrime investigations. Second, dissemination of public awareness awareness programmes to ensure that the members of the public and the business entities known of how BEC crimes work. Analysing how these crimes are committed will enable potential victims avoid falling prey to them by practising good security measures and to confirm any transactions. Besides, the support of international cooperation has to be enhanced. For example, Indonesia could also develop more intense cooperation with the international organisations and increase the volume of the bi-lateral agreements seen with other countries. These partnerships should concern the coordination and synchronisation of legal provisions governing the exchange of intelligence information and the number of years it generally takes to extradite an individual. Other international organisations such as ASEAN can also help to build coherent action plans to transform cybercrime. Prior to the national level there should be specialized BEC task forces in concern with the police, prosecutors and judicial representatives. These task forces should tasks with the responsibility of facilitating proper communication and coordination of the various stakeholders.

Apart from structural and procedural changes, it is imperative to have embracing concerns focusing on victims in policing. Those who fall prey to BEC crimes face the prospect of major financial losses and the long time before they can get justice. If the agencies learn to handle the cases as quickly as possible then the victim will suffer the least and the society will regain its confidence in the legal system. Looking at the consequences of the crime, special help systems, including legal, psychological, and social, should be also created to help victims. That is why it is also necessary to contemplate the possibilities of combating BEC crimes and their underlying difficulties in the future. Strategy 2021 mentions that cyber threats are dynamic, and hence the law enforcement apparatus has to be battling those threats proactively(Sirait et al., 2024). This entails persistent study of new and developing trends of cybercrime and encouraging the cooperation between ministries, universities and corporations. In the system of fighting cybercrime, and for the invention of special tools and approaches, P3 is most efficient. For example, the tech companies can offer their tact in protecting against security threats in order to help police organisations evaluate and seek out vulnerabilities in cyberspace. Last but not the least, legal and regulating requirement need to be made dynamic in order to meet the emerging trends and challenges of cybercrimes. It was also recommended that legislative provisions regulating digital evidence, data protection and cross border cooperation should be reconsidered and updated. In Indonesia, therefore there is need to strengthen laws on cybercrime as well as its implementation: this will serve as a good foundation in the fight against BEC and other related crimes. Policy makers need to consider whether they should invite the creation of separate courts or tribunals for the determination of cyber crimes issues as this shortens the judicial systems and improves the quality of the decision made.

3.3. Efforts to Enhance Legal Protection for BEC Victims

Enhancing legal protection for victims of Business Email Compromise (BEC) crimes has become an urgent necessity amidst the rising prevalence of cybercrimes that harm various sectors. Efforts to achieve this can be pursued through multiple approaches, including revising existing laws, strengthening law enforcement capacity, preventive measures, and involving other institutions to provide more effective protection. Combining these strategies aims to fortify the legal framework, enhance the capabilities of law enforcement, and minimize the risks and impacts suffered by victims.

a. Legal Reform

META therefore seeks to explore how legal protection to BEC crimes victims has become necessary amidst increasing incidence of cybercrimes affecting several industries. Of course, it is possible here to continue the list of initiatives for attaining this goal, but to do this one might utilise the following strategies: legislative changes, to enhance the Law enforcement capabilities, the Agency might implement the concept of preventative measures, or invite other institutions to provide alternative forms of protection. Implementing these approaches' purpose is to strengthen the legal basis, increase the efficiency of the police work, and reduce as much as possible threats and consequences for the victims.

b. Strengthening Law Enforcement Capacity

However, the analysis of the BEC cases suggests that it is equally essential to enhance an operational capacity of the police. Officers need enough technical capabilities to investigate BEC crimes and produce digital evidence that is frequently used by these offenders. Admiral Kistijono also explained that an advanced digital forensic training model increases officers' knowledge in terms of the latest technologies such as tracking footprints, identifying servers involved in crimes, and authenticating electronic data (Wahyudi, 2022). Further, apart from professional knowledge in fighting cybercriminality, the police needs to gain legal awareness concerning the international legislation regulating such offence. Because BEC crimes imply that offenders work globally, officers should know how, for example, the MLAT and extradition treaties work (Maringka, 2022). These competencies help in cooperation with other countries to arrest culprits in other countries. Enhancing this capacity also entails ensuring there is adequate human resource capacity in terms of numbers in particular the personnel dealing with cybercrime within police, prosecution and judiciary and ensuring that their caseloads are reasonably balanced.

c. Preventive Measures

However, prevention remains a critical component of minimising BEC crime risks. The first and major step in addressing the issue of the lack of effective BEC schemes is to raise awareness of the population. Several media can be used to run Cyber awareness campaigns in order to educate the public about indicators that may prove that email fraud is ongoing such as sudden transfer of funds, changes of account details among others or receipt of emails from strange email addresses. Such programmes should be developed for businesses, organisations and persons of interest, especially those in the financial industry, to enhance their alertness on BEC attacks. Consequently, efforts to increase awareness about cybersecurity have to be supported by material training in how to use technological defence mechanisms, including two-factor authentication, data protection, and password management. At the corporate level, it is crucial to enhance internal communication safety and cheque the results of transactions. Further, raising awareness and working together with stakeholders such as the IT industry and providers of email services improves the security of the information systems commonly utilised by the public (Daeng et al., 2023). These companies can begin spending in awareness technologies to identify BEC attack patterns and create better andstronger software against cyber threats.

d. Role of Other Institutions

To enhance legal protection for the BEC victims, enforcement of law is not enough; other institutions like the Indonesian Financial Services Authority (OJK) has some proactive parts too. OJK as a supervisor of the financial sector must make sure that financial institutions had good enough security measure for customer data and prevent misuse of such data through cyber fraud. OJK can provide technical directives towards the banks and other financial companies to enhance the security of electronic transactions and to fast track the process of handling the BEC similar cases related to bank accounts. Other stakeholders such as the Ministry of Communication and Information Technology of Indonesia also have several strategic responsibilities for developing national cybersecurity framework. The solution identified is Kominfo can coordinate with Internet Service Providers to blackout recognised servers or domains that are utilised in carrying out BEC scams. Besides, Kominfo may enhance the regulation of data handlers to address compliance with Law No. 27 of 2022 on the Protection of Personal Data (PDP Law).

One final factor is public–private partnerships The available literature on innovation has revealed collaboration between the private sector and the public sector as being important to the development of innovation. Technology companies and organisations providing email service, for instance, can help by designing other forms of security for instance identification of the emails that are suspicious or offering activity reports to the users on the safety of the content being received. They can also get involved by ensuring that, institutions offer courses in digital literacy to teach the younger generation correct conducts to embrace. Thus, promoting BEC-related legal protection can only be multi-focused and multipronged in nature, involving both legal and social strategies along with capacity development for law enforcement, preventive measures for other institutions, and legal reform. If theseelements arerefined, the legalenvironment of the country can be enhanced; thefacilities of policemeet these cases withsuccess; and overall, the harmful effects and dangers on victims may bediminished. To that end, it is crucial that protective measures applied today remain capable of responding to a threat that continues to advance over time.

4. Conclusions

The findings of this work show that BEC offences are a real threat in the digital age and call for multi-faceted solutions. Although the former Law Number 11 of 2008 on Electronic Information and Transactions (EIT Law) and the latter Law Number 27 of 2022 on Personal Data Protection (PDP Law) form the legal basis for accout, both contain weaknesses in addressing BEC crimes and providing the best protection for the victims. Therefore, there is the need to adapt the legal frameworks to meet the above-cited legal defects.As discussed by CostTF, the actual problem is the impossibility of effective enforcement of the laws against BEC crimes due to several factors, including the nature of digital evidence and the difficulties in identifying the criminals, let alone those operating from other countries. Improving the ability of LEA and encouraging cooperation and linkages between agencies is one of the important areas. Also, there are secondary measures by raising public awareness and engaging private companies, which can help reduce the threats connected with BEC. Other institutions such as Financial Services Authority (OJK) also need to contribute in the victimisation side of minimising losses from cybercrimes. The above mentioned steps are the essential for increasing legal protection of BEC victims in Indonesia.

References

Agazzi, A. E. (2020). Business Email Compromise (BEC) And Cyberpsychology. ArXiv Preprint ArXiv:2007.02415.

Azzani, I. K., Purwantoro, S. A., & Almubaroq, H. Z. (2023). Urgensi Peningkatan Kesadaran Masyarakat Tentang Kasus Penipuan Online Berkedok Kerja Paruh Waktu Sebagai Ancaman Negara. NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 10(7), 3556–3568.

Bahri, I. S. (2023). Cyber Crime dalam Sorotan Hukum Pidana. Bahasa Rakyat.

Cross, C., & Gillett, R. (2020). Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. Journal of Financial Crime, 27(3), 871–884.

Daeng, Y., Levin, J., Karolina, K., Prayudha, M. R., Ramadhani, N. P., Noverto, N., Imanuel, S., & Virgio, V. (2023). Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia. Innovative: Journal Of Social Science Research, 3(6), 1135–1145.

Fauzi, A. A., Kom, S., Kom, M., Budi Harto, S. E., MM, P. I. A., Mulyanto, M. E., … Kom, S. (2023). PEMANFAATAN TEKNOLOGI INFORMASI DI BERBAGAI SEKTOR PADA MASA SOCIETY 5.0. PT. Sonpedia Publishing Indonesia.

Febriansyah. (2023). FINANCIAL IDENTITY THEFT : DARI TINDAK PIDANA INFORMASI ELEKTRONIK KE KEJAHATAN DATA PRIBADI. Jurnal Hukum Samudra Keadilan, 18(2), 359–375. https://doi.org/10.33059/jhsk.v18i2.8783

Hoshmand, M. O., & Ratnawati, S. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. Jurnal Sains Dan Teknologi, 5(2), 679–686.

Hutabarat, S. A., Praja, S. J., Suhariyanto, D., Paminto, S. R., Kusumastuti, D., Fajrina, R. M., Saragih, I. I. M., Budihartono, E., & Abas, M. (2023). CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0. PT. Sonpedia Publishing Indonesia.

Kalesaran, A. (2022). Akibat Hukum Digitalisasi Perdagangan Saham Menurut Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia. Lex Privatum, 10(6).

Kamal, I., & Rafiah, K. K. (2021). Bisnis di Era Digital, Why Not? Yrama Widya.

Kamariah, H., Rania, T. S., Harpijah, D., Ikhsan, F., & Pramuja, I. A. (2024). Disparitas Pendapatan Pelaku Usaha Digital Vs Konvensional Di Kota Pontianak. Inovasi Makro Ekonomi (IME), 6(3).

Maringka, J. S. (2022). Ekstradisi Dalam Sistem Peradilan Pidana. Sinar Grafika.

Muhammad Rifqi Noval, S. (2024). HUKUM SIBER Kebangkitan Kembali Metaverse Beserta Permasalahan Hukumnya.

Musriko, M., & Febriansyah, F. (2024). Disparity in the Application of Legal Rules to Gambling Crimes Through Electronic Media. Pena Justisia: Media Komunikasi Dan Kajian Hukum, 22(2). https://doi.org/10.31941/pj.v22i2.4731

Ramadhani, S. A. (2022). Komparasi Perlindungan Data Pribadi di Indonesia dan Uni Eropa. Jurnal Hukum Lex Generalis, 3(1), 73–84.

Scanio, S. (2024). Liability of the Beneficiary's Bank for Cybercrime Involving Fraudulent Funds Transfers. The Business Lawyer, 79.

Sirait, T. M., SH, M. H., & others. (2024). Cyber Law dalam Teori dan Perkembangannya (Cyber Crime, Privacy Data, E-Commerce). Deepublish.

Situmeang, S. M. T. (2020). Cyber law. CV Cakra.

Sudarmanto, E. (2023). Pencegahan Fraud Dengan Manajemen Risiko Dalam Perspektif Al-Quran. Zahir Publishing.

Wahyudi, R. (2022). Kekuatan Keterangan Saksi Ahli Digital Forensik Dalam Penyidikan Tindak Pidana Di Wilayah Direktorat Reserse Kriminal Umum Kepolisian Daerah Riau. Universitas Islam Riau.

Yurizal, D. R., & others. (2018). Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia (Vol. 1). Media Nusa Creative (MNC Publishing).