Indonesian Journal of Law and Justice Volume: 2, Number 3, 2025, *Page*: 1-8

Legal Analysis Of The Handling Of M-Bangking Electronic Evidence In Bribery Cases In The Digital Era

Sudarsono Sagala*, July Esther*, Jusnizar Sinaga*

[1,2,3] Universitas HKBP Nommensen

DOI: https://doi.org/10.47134/ijlj.v2i3.3625
*Correspondence: July Esther
Email: Julyesther@uhn.ac.id

Received: 11-01-2025
Accepted: 14-02-2025
Published: 23-03-2025

Abstract: Evidence in cybercrime cases can be easily erased or eliminated, and there are challenges in detecting crimes that occur in the banking sector that utilizes computer technology. This difficulty arises due to the lack of adequate equipment, the lack of courage of some victims to report the incident to the authorities, as well as the relatively weak security system of the owner of the asset or system. In addition, the difficulty in tracking the whereabouts of the perpetrators is also a significant problem. This research aims to examine and analyze how electronic evidence derived from M-banking transactions can be used in the process of proving bribery cases, as well as the challenges faced in law enforcement in Indonesia. The research method used is a normative approach with qualitative analysis, which includes literature studies and analysis of relevant regulations, such as the Electronic Information and Transaction Act (UU ITE) and the Code of Criminal Procedure (KUHAP). In this research, it was found that although the ITE Law gives recognition to electronic documents as valid evidence, there are obstacles in its application in court. The Criminal Code has not expressly regulated the recognition of electronic documents, which causes confusion in legal practice. In addition, technical challenges and lack of understanding among law enforcement officers regarding how to handle electronic evidence are also obstacles in the proof process.

Keywords: Electronic Evidence, Criminal Law, M-Banking, Bribery, ITE Law

Introduction

Advances in technology and information have developed so rapidly that it has indirectly changed the behavior and lifestyle of people globally. This development also turns the world into borderless and causes significant and rapid social, economic and cultural changes. Information technology brings humans to a new civilization, with its social structure and values, namely a developing society towards a new global society where state barriers begin to fade which will ultimately have an impact on shifting values, norms, morals and decency.

Many cases show that the legal system in the field of information technology still has weaknesses, which can be seen from the existence of juridical and non-juridical obstacles. The juridical constraints include the lack of explicit recognition of electronic documents as evidence in KUHAP. This is reflected in Article 184 paragraph (1) of Law No. 8 of 1981, which clearly limits the types of evidence to witness testimony, expert testimony, letters, instructions, and testimony of the defendant. In addition, there is no authority for

investigators to search computer systems suspected of being involved in a crime. Meanwhile, non-juridical obstacles include the limited number and ability of police officers who have expertise in computer technology. Evidence in cybercrime is easily deleted or eliminated, and there are difficulties in detecting crimes in the banking sector that utilize computer technology. This difficulty is caused by the lack of adequate equipment, the reluctance of some victims to report to the authorities, and the relatively weak security system of the asset or system owner. In addition, it is also difficult to trace the whereabouts of the perpetrators of crimes.

Until now, Indonesia does not have a specific article that can be used to ensnare cyber criminals. For example, in the case of carding, the police can only charge the perpetrators using Article 363 of the Criminal Code on theft, because the act involves stealing other people's credit card data. Initially, internet technology was neutral in that it was defined as a value-free technology. Technology cannot be attached to its good and evil nature. However, in its development, the presence of technology tempts parties with evil intentions to misuse it. Thus technology can be said to be a criminological factor, a factor that causes people's desire to do evil or facilitates crime. One of the crimes caused by the development and advancement of information technology is crimes related to internet applications. This crime in foreign terms is often called "Cyber Crime". The world of information technology is developing so fast that it is unexpected, but this development is also followed by information technology crimes. This crime also causes many people to pay a high price to prevent it and obey existing laws.

The development of digital technology today also participates in developing technology in the field of Fintech Industry is a growing field that uses technology to improve activities in the financial sector. Article 5 and Article 6 of the Electronic Information and Transaction Law (ITE Law) regulates electronic evidence, which states that electronic information and electronic documents, as well as their printouts, are considered valid evidence if they use electronic systems in accordance with the provisions of the ITE Law. With the enactment of the ITE Law, it is increasingly emphasized that electronic documents can be used as legal evidence in Indonesian procedural law, especially in the context of criminal procedure law. Furthermore, in relation to the crime of money laundering, Law No. 8/2010 on the Eradication of the Crime of Money Laundering explicitly states that this law is the first to legalize the use of electronic evidence as valid evidence. This shows official recognition of electronic documents in the legal process, thus providing a strong foundation for the use of electronic evidence in law enforcement in Indonesia.

M-banking or mobile banking, which was originally designed to facilitate quick and efficient financial transactions, is unfortunately often misused as a tool for unlawful activities, including bribery. In the m-banking system, the ease of making transfers between accounts without face-to-face or physical presence makes the transaction process more anonymous and difficult to trace, which is exploited by parties who want to avoid detection. Technology that is supposed to bring benefits to society has become a loophole for acts of corruption that harm the state and society. The rampant misuse of m-banking in bribery transactions creates new challenges for law enforcement, which needs to adjust regulations and improve supervision to maintain the integrity and security of the digital banking system. Technological advancements in the digital era have had a major impact on various

aspects of life, including increasingly sophisticated crime patterns. One of the most common modes is bribery through electronic platforms, such as mobile banking (m-banking), which allows transactions to be carried out quickly and discreetly. This poses new challenges in law enforcement, especially in terms of handling and proving electronic evidence. Therefore, a comprehensive legal analysis is required to ensure that such evidence is admissible in court and supports a fair and transparent law enforcement process. In this context, transactions through M-banking are one form of electronic evidence that is often used in bribery cases.

Bribery is a criminal offense that harms society and the state, where the perpetrator tries to influence the decisions of public officials through the provision of rewards. With M-banking, the bribery process can be done more easily and quickly, but this also creates new challenges in terms of evidence. Therefore, it is important to analyze how electronic evidence from M-banking can be legally accounted for in the judicial process. The types of bribery include:

1. Active bribery

   Active bribery occurs when a person gives or promises something to a public official or party who has authority or influence in a particular situation with the aim of influencing the action or decision to be taken by that party. For example, a businessman gives money to a government official in order to obtain a business license or construction project.

2. Passive Bribery

   Passive bribery occurs when a person receives something from a party who wants to influence their actions, usually from the party offering the bribe. A public official or authorized party accepts a gift, money, or other reward in order to do or not to do an action that should be done in the capacity of his or her office. For example, a public official accepts money from a citizen to expedite the administrative process of producing documents.

3. Bribery

   Bribery occurs when the giving or receiving of bribes is done routinely and repeatedly in order to gain a particular advantage on an ongoing basis. This practice often takes the form of paying or receiving money periodically or in fixed amounts to ensure the continuation of a favorable relationship for both parties. For example, a businessman pays a certain amount of money to a tax officer every month to avoid being audited or penalized.

Law Number 31 of 1999 as amended by Law Number 20 of 2001 concerning Amendments to the Law on the Eradication of Corruption simplifies corruption into seven groups, including causing state losses, bribery, gratuities, conflict of interest in the procurement of goods/services, extortion, fraudulent acts, and embezzlement in office. Of the seven groups, the bribery article has the most bribes compared to other groups, including Article 5 paragraph 1 letter (a), Article 5 paragraph 1 letter (b), Article 13, Article 5 paragraph 2, Article 12 letter (a), Article 12 letter (b), Article 12 letter (c), Article 12 letter (d) Article 11, Article 6 paragraph 1 letter (a), Article 6 paragraph 1 letter (b), and Article 6 paragraph 2.

Bribery cases involving m-banking often require in-depth legal analysis to ensure that electronic evidence is processed in accordance with the Electronic Information and Transaction Law (ITE Law), the Criminal Procedure Code (KUHAP) and other relevant regulations. In addition, the existence of electronic evidence must be supported by adequate technological understanding in order to be used as valid evidence in court. Therefore, based on this background, the author wants to analyze the strength of M-bangking electronic evidence in bribery cases in the digital era and how to prove M-bangking electronic evidence in bribery cases in the digital era which will aim to help practitioners, law enforcement in law enforcement against bribery cases in the digital era.

Methodology

In the context of the object of this research, it refers to the systematic ways used to identify, analyze, and evaluate how the applicable law enforcement in Indonesia deals with corruption in the handling of m-banking electronic evidence. The data sources in this research are primary legal materials such as Law number 11 of 2008 concerning electronic information and transactions, our criminal law law, and our criminal procedure law, secondary legal materials such as books, legal journals and articles and tertiary legal materials in the form of large Indonesian dictionaries and legal dictionaries.

Based on the types and sources of data used by the author in analyzing this research, the data collection technique applied is normative qualitative research method. This research focuses on literature review, using various sources such as laws, books, journals, theses, and legislation relevant to the research problem formulation. With this approach, the author seeks to obtain systematic results regarding criminal acts of connexity.

This research uses perspective analysis, which means the process of evaluating an issue or phenomenon by considering different points of view and a form of data analysis that not only predicts future results, but also provides recommendations for actions or decisions to achieve desired results or prevent undesirable results This helps in understanding the complexity of the problem and how various factors affect a person's perspective. Data analysis in this research uses normative legal research methods by examining various materials in the literature related to law enforcement against corruption in handling m-banking electronic evidence in the digital era.

Result and Discussion

The Power of M-banking electronic evidence in bribery cases in the digital era

In the context of Indonesian law, the strength of electronic evidence, including transactions through M-banking, is becoming increasingly important, especially in cases of crimes such as bribery. The process of evidence in criminal procedure law has a very crucial role, because the investigation aims to find material truth, which is the core of criminal procedure law itself. Evidence serves as a benchmark to determine whether someone is guilty or not in court. If the evidence presented in court is strong enough to show a person's guilt, then the individual will be sentenced in accordance with the applicable legal provisions. Conversely, if the evidence presented is insufficient to prove the defendant's guilt, then no punishment will be imposed.

Judges have the responsibility to carefully assess and consider each piece of evidence presented. In the evidentiary system, it is stipulated that the judge cannot impose a sentence on a defendant unless there are at least two valid pieces of evidence. This is regulated in Article 183 of the Criminal Procedure Code, which emphasizes the importance of the judge's belief that a criminal act actually occurred and that the defendant is the perpetrator. Therefore, the evidentiary process is not just a formality, but a fundamental step to achieve justice in every criminal case. The existence of valid evidence and the judge's belief are key in determining the final outcome of a case.

Electronic money transaction systems have the potential to facilitate the concealment of funds originating from crime, so they can be categorized as money laundering through digital media. Article 3 of the Law on Eradication of Money Laundering (PPTPPU) describes in detail the acts of money laundering, including placement, transfer, payment, expenditure, donation, overseas expenditure, change of form, and exchange for foreign currency or securities. Money laundering activities often utilize electronic-based transactions. Regulations regarding electronic evidence have been regulated in special laws such as the PPTPPU Law. However, despite these arrangements, there are no formal rules that fully regulate electronic evidence. In practice, judges still consider the existence of electronic evidence when deciding money laundering cases. The development of technology that is often misused as a means of money laundering must be taken seriously.

The lack of understanding regarding access and guarantees of the integrity of electronic evidence in accordance with Article 6 of the ITE Law can affect the judge's confidence in assessing the validity of the evidence. Evidence is a practice carried out by related parties to prove facts and rights related to their interests. Evidence in a criminal trial basically aims to show that the defendant has committed a criminal act. Therefore, law enforcers are obliged to gather the necessary evidence to prove the truth of the accusation.

A. Evidence of M-banking electronic evidence in bribery cases in the digital era

In criminal cases involving electronic data, law enforcement cannot be ignored simply because of difficulties in the evidentiary process. Moreover, if the criminal act can be subject to conventional offenses that have clear and firm provisions. The effort that can be made is to trace the evidence related to the actions of the perpetrators of the crime through the criminal procedure law (KUHAP). This means that we continue to use evidence such as witness testimony, expert testimony, letters, clues, and testimony of the defendant. The perpetrator's guilt can be proven with a minimum of two valid pieces of evidence. These pieces of evidence must be able to show that an act has occurred and prove the existence of the consequences of the criminal act.

Regarding the types of evidence that are valid and allowed to be used in evidence, as stipulated in Article 184 paragraph (1) of the Criminal Procedure Code, there are five main categories, namely witness testimony, expert testimony, letters, clues, testimony of the defendant.

When compared to the evidence listed in Article 295 HIR, there are some significant differences. These differences include: Confession: In the HIR, a confession is considered a separate piece of evidence, whereas in KUHAP, the confession is expanded to become the

testimony of the accused, which includes more than just the confession itself. Addition of Evidence: KUHAP introduces new evidence that was not previously recognized in the HIR, namely expert testimony, which is important given the development of science and technology that affects the modus operandi of crime.

As such, this distinction demonstrates an evolution in Indonesia's legal evidentiary system, where KUHAP seeks to be more responsive to complex evidentiary needs in the modern context. And overall, electronic evidence from M-banking plays an important role in proving bribery cases in the digital age. With clear regulations in the ITE Law and court practice, electronic evidence can be effectively used to prove corruption crimes. However, special attention should be paid to the procedures for collecting and presenting evidence to ensure its validity in the eyes of the law.

Conclusion

In the growing digital era, the handling of electronic evidence, especially those from M-banking transactions, has become a crucial aspect in the law enforcement process, especially in bribery cases. The Electronic Information and Transaction Law (ITE Law) provides a clear legal basis regarding the recognition of electronic evidence as valid evidence. Article 5 and Article 6 of the ITE Law emphasize that electronic information and documents can be used in legal proceedings, including in bribery crimes. To increase the effectiveness of the use of electronic evidence in bribery cases, further efforts are needed to strengthen regulations and improve the technical capacity of law enforcement officials. Training on how to handle and analyze electronic evidence should be increased so that they can be better prepared for the challenges of the digital age.

Overall, this analysis shows that while electronic evidence from M-banking has great potential in proving bribery cases in the digital era, special attention must be paid to the procedures for collecting and presenting the evidence to ensure its validity in the eyes of the law. As such, improved understanding and skills in this area are essential to support more effective law enforcement.

References

Angela Gabriela Bupu, dkk. *Analisis Yuridis Cyber Crime Pembobolan Dana Nasabah pada Aplikasi Mobile Banking dengan Modus Pembobolan Jalur Undangan Pernikahan Palsu*. Vol. 2 No. 2, Jurnal Ilmu Hukum dan Sosial, Mei (2024)

Horsman, G. (2022). Defining principles for preserving privacy in digital forensic examinations. *Forensic Science International: Digital Investigation*, *40*, ISSN 2666-2825, https://doi.org/10.1016/j.fsidi.2022.301350

Indonesia, *Mengenal penyuapan: Defenisi, jenis, dan dampak negatifnya.* (2024). https://grc-indonesia.com/mengenal-penyuapan-definisi-jenis-dan-dampak-negatifnya/.

Javed, A.R. (2022). A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. *IEEE Access*, *10*, 11065-11089, ISSN 2169-3536, https://doi.org/10.1109/ACCESS.2022.3142508

Keumala Ulfah A, et al, 2022. *Ragam Analisis Data Penelitian.* Jawa Timur: IAIN Madura Press. law, June (2003).

Khan, A.A. (2022). Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction. *International Journal of Electronic Security and Digital Forensics*, *14*(2), 124-150, ISSN 1751-911X, https://doi.org/10.1504/IJESDF.2022.121174

Khashashneh, T. (2023). The Importance of Digital Technology in Extracting Electronic Evidence: How Can Digital Technology be used at Crime Scenes?. *Pakistan Journal of Criminology*, *15*(4), 69-85, ISSN 2074-2738

Kumar, S. (2022). A comprehensive study of XSS attack and the Digital Forensic Models to gather the evidence. *ECS Transactions*, *107*(1), 7153-7163, ISSN 1938-6737, https://doi.org/10.1149/10701.7153ecst

Modesta Anen M. Batmomolin, dkk, *Keabsahan Bukti Elektronik Dalam Tindak Pidana Pencucian Uang di Pasar Modal Beserta Akibat Hukumnya,* Vol. 6 No. 2, jurnal of notarial

Nasya Ardhani Subarzah, dkk. *Kekuatan Pembuktian Alat Bukti Elektronik Dalam Tindak Pidana Pencucian Uang Pada Kasus Putusan Nomor 844/Pid.Sus/2019/Pn.Ptk.* Juranl Krisna Law. Vol. 5 No. 1. Feb (2023).

Pandoe Pramoe Kartika. *Data Elektronik Sebagai Alat Bukti Yang Sah Dalam Pembuktian Tindak Pidana Pencucian Uang. Indonesia Journal of Criminal Law.* Vol. 1 No. 1. Jun (2019)

Prakash, V. (2022). Cloud-Based Framework for Performing Digital Forensic Investigations. *International Journal of Wireless Information Networks*, *29*(4), 419-441, ISSN 1068-9605, https://doi.org/10.1007/s10776-022-00560-z

Pusat Edukasi Anti Korupsi, *Memahami suap- menyuap dalam delik Korupsi,* https://aclc.kpk.go.id/aksi-informasi/Eksplorasi/20231017-memahami-suap-menyuap-dalam-delik-korupsi. Diakses pada tanggal 17 Okt 2023.

Rana, S.K. (2023). Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain. *IEEE Access*, *11*, 83289-83300, ISSN 2169-3536, https://doi.org/10.1109/ACCESS.2023.3302771

Ridwan Karim, *Pengertian Objek Penelitian: Jenis, Prinsip dan Cara Menentukan,* Deepublish Store. 2023. https://deepublishstore.com/blog/pengertian-objek-penelitian/

Somaerin Saputra, Tesis. *Analisis Pembuktian Hukum Perkara Tindak Pidana Penggelapan Melalui Elektronik Sistem* (Studi Perkara Nomor 118/Pid.B/2021/PN Cbn). (Semarang: UNISSULA, 2022).

Stoykova, R. (2022). Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation*, *40*, ISSN 2666-2825, https://doi.org/10.1016/j.fsidi.2022.301351

Tok, Y.C. (2023). Identifying threats, cybercrime and digital forensic opportunities in Smart City Infrastructure via threat modeling. *Forensic Science International: Digital Investigation*, *45*, ISSN 2666-2825, https://doi.org/10.1016/j.fsidi.2023.301540

Tsai, F.C. (2021). The application of blockchain of custody in criminal investigation process. *Procedia Computer Science*, *192*, 2779-2788, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.09.048

UU No. 8 Tahun 1981 tentang Kitab Undang-undang Hukum Acara Pidana (KUHAP)

Valentino Wenno, dkk. *Pertanggung Jawaban Hukum Pelaku Tindak Pidana Penyuapan*. Jurnal Ilmu Hukum. Vol. 1 No. 9. Nov (2021).