Jurnal Notariil

Jurnal Notariil, Vol. 10, No. 1, 2025; 1-6 P ISSN 2540 - 797X
Available Online at https://ejournal.warmadewa.ac.id/index.php/notariil E ISSN 2615 - 1545

LEGAL ANALYSIS OF THE TRANSFORMATION OF ECONOMIC CRIMES IN THE DIGITAL ERA (CYBERCRIME)

Tri Wani Andini[1]*, and Hudi Yusuf[1]
1. Universitas Bung Karno, Indonesia
*Email: angelinadinda008@gmail.com

How To Cite:
Andini, T, W., Yusuf, H. (2025). Legal Analysis of The Transformation of Economic Crimes in The Digital Era (Cybercrime). *Jurnal Notariil 10*(1), 1-6. Doi: https://doi.org/10.22225/jn.10.1.2025.1-6

Abstract

The development of digital technology has brought significant changes in various aspects of human life, including in the economic sector. Digitalization has made transactions and economic activities easier, increased efficiency, and expanded access to the global market. However, this technological advancement has also given rise to new challenges, one of which is the increase in digital-based economic crimes or what is known as cybercrime. This research aims to (1) examine the impact of economic crimes in the digital era (cybercrime) on economic stability in Indonesia and (2) analyze the effectiveness of national legal regulations in dealing with economic crimes in the digital era (cybercrime). The research method used in this study is a normative research method with the data collection method used being library data or document studies (Library Research) sourced from legal materials in the form of primary legal materials, secondary legal materials and tertiary legal materials. The conclusion obtained from this study is that economic crimes in the digital era (cybercrime) are not only a criminal problem, but also threaten the stability of the Indonesian economy as a whole. National legal regulations have provided a framework for dealing with economic crimes in the digital era (cybercrime), but their effectiveness is still limited by less-than-optimal implementation, inadequate infrastructure, and lack of cross-country cooperation. Therefore, collaboration is needed between the government, private sector, and society in increasing digital literacy, strengthening regulations, and improving digital security systems to minimize the negative impacts of this digital economic crime.

Keywords: cyber crime; digital era; economic crime

1. INTRODUCTION

The existence of the internet as a result of the development of information and communication technology is a challenge as well as an opportunity in all aspects of life considering that Indonesia has a fairly high interest in the internet. (Toni et al., 2021) The progress of computer technology integrated with the cyber world (internet) cannot be denied that it has given rise to various kinds of convenience in interacting between subjects in one country and even between the world. (Indrajit, 2000)

The development of digital technology in the current era has brought significant changes in various aspects of human life, including in the economic sector. Digitalization has facilitated economic transactions and activities, increased efficiency, and expanded access to the global market. However, this technological advancement has also given rise to new challenges, one of which is the increase in digital-based economic crimes or what is known as cybercrime.

The emergence of the information technology revolution today and in the future not only has an impact on the development of technology itself, but will also affect other aspects of life such as religion, culture, social, politics, personal life, society and even the nation and state. The global information network or internet has now become one of the means to commit crimes both domestically and internationally. The internet has become a medium for criminals to commit crimes with its mondial, international nature and beyond the borders or sovereignty of a country. All of this is a very attractive motive and modus operandi for digital criminals.(Winarno, 2015)

In some literature, cybercrime is often referred to as computer crime. The U.S. Department of Justice defines computer crime as: "…any illegal act requiring knowledge of computer technology for its preptration, investigation, or prosecution." (Hamzah 1989) means that computer crime in general can be interpreted as the illegal use of computers. (Fuady, 2005)

Cybercrime in the economic context includes various forms of crime, such as financial data theft, e-commerce fraud, money laundering through cryptocurrency, and digital-based tax evasion. These crimes not only harm individuals and institutions, but can also disrupt the economic stability of a country. According to data released by international institutions, global losses due to cybercrime are estimated to reach billions of dollars each year, and Indonesia is one of the countries vulnerable to this crime.

In Indonesia, the transformation of economic crimes towards the digital space is increasingly evident. Cases such as online fraud, phishing, and money laundering through blockchain technology are clear evidence of how economic crimes have adapted to technological developments. This is exacerbated by the low digital literacy of the community and limited supervision of digital economic activities.

From a legal perspective, handling digital economic crimes still faces a number of challenges. Although there are regulations such as the Electronic Information and Transactions Law (UU ITE) and the Law on the Prevention and Eradication of Money Laundering, their implementation is often less than optimal. Law enforcers are often constrained by digital forensic techniques, limited human resources, and international cooperation to deal with transnational crimes.

Based on the background of the problem above, the authors conducted research on the Legal Analysis of The Transformation of Economic Crimes in The Digital Era (Cybercrime). The purpose of this study is to understand (1) What is the impact of economic crimes in the digital era (cybercrime) on economic stability in Indonesia and (2) How effective is national legal regulation in handling economic crimes in the digital era (cybercrime).

2. METHOD

The research method used in this research is the normative research method. Normative legal research is a process to find legal rules, legal principles, and legal doctrines to answer the legal problems faced.(Marzuki, 2017) The data collection method used is library data or document studies obtained through library research sourced from data on legal materials that have been collected, namely by collecting legal materials in the form of primary legal materials, secondary legal materials and tertiary legal materials, such as laws and regulations, books, official documents, publications and research results, which data will then be analyzed with applicable laws and regulations.

3. DISCUSSION

LEGAL ANALYSIS OF THE TRANSFORMATION OF ECONOMIC CRIMES IN THE DIGITAL ERA (CYBERCRIME)

The Impact of Economic Crimes in The Digital Era (Cybercrime) on Economic Stability in Indonesia

Raharjo (2002:29) stated that cyber crime is a social phenomenon that has emerged since the beginning of human life, but is increasingly facilitated by advances in information and communication technology. If previously crimes were committed conventionally in real terms, now they can be committed by perpetrators subtly by utilizing virtual space or cyberspace.(Raharjo, 2002)

Cybercrime is a crime that requires special attention. Cybercrime is an interesting and sometimes difficult issue because cyber activities are not limited by state territory if the perpetrators are from different countries. Cyber activities are relatively intangible because the crime is carried out in cyberspace or cyberspace, the difficulty of proof because electronic data is relatively easy to change and easier to remove traces.(Muhammad Ramadhan et al., 2020)

With the existence of a virtual society, a form of criminal act will indirectly arise. What we need to remember is that a virtual society is a real society only with a different "locus", as previously stated by the opening of the constitution that "the state protects the entire nation and advances public welfare", so due to this relationship, the government must protect citizens from all criminal acts and the government must provide freedom to the community by maximizing policies for the sake of the economic growth of citizens. (Muhammad Ramadhan et al., 2020)

Crimes in high technology based on networks or can be said as cybercrime or cyber crime. What needs to be noted is that cybercrime is not a requirement to fulfill economic elements, which means that cybercrime cannot always be categorized as an economic crime, but it can be said as a special form of crime, which means that the nature of its regulation is outside the Criminal Code and its handling is carried out specifically and differently from conventional crimes in general.(Muhammad Ramadhan et al., 2020)

Skimming is a type of digital-based economic crime in which this crime is carried out by stealing other people's important data, including bank data such as account numbers, ATM data such as card numbers and PINs, even credit card data such as card numbers and types and PINs. The purpose of skimming crimes is to steal information from customers' debit or credit cards using a special tool called a Skimmer. So skimming is also called a banking crime.

In addition to skimming, fraud in online buying and selling transactions is also rampant. Fraud in online buying and selling transactions is a form of cybercrime that is difficult to catch. First, handling cybercrime still faces obstacles in terms of scope. Cyberspace does not have clear boundaries, so the police need quite a long time to identify perpetrators of fraud in online buying and selling transactions because of the frequent falsification of the perpetrator's identity. Second, collecting evidence in this crime is difficult because it occurs in an electronic system. The method that can be used to collect evidence is to look for clues that indicate malicious intent, such as unauthorized access, use of fake identities during registration, device location, and devices used to commit crimes. This can be done by collecting witness statements in court, emails or printed data, or statements from the defendant in court. Third, identifying cybercrime perpetrators is difficult because of the strong network between them. Fourth, the facilities and infrastructure in the cybercrime unit in Indonesia are still not optimal, so that the law enforcement process is hampered. Obtaining clues from evidence in cybercrime will be difficult if you only rely on witness statements, letters, or statements from the defendant, although it is still possible to apply.(Fadila, 2024)

In terms of other digital-based economic crimes, the use of cryptocurrency as a tool of crime is closely related to the mode of money laundering (TPPU) and other economic crimes because the encryption of the blockchain system in crypto is difficult for outsiders to access. Although often referred to as cryptocurrency, Indonesia has not yet recognized any crypto as a currency that can be used as a means of exchange. Converting rupiah into crypto assets makes its use in crimes such as money laundering increasingly difficult to track.

Digital economic crimes, or cybercrime, have a significant impact on the stability of the Indonesian economy because the nature of this crime damages various fundamental aspects of the economy. Cybercrime can be carried out quickly and covers a wide area, beyond national borders. By utilizing technology, perpetrators can attack many victims in a short time, such as through ransomware, phishing, or online fraud, which directly disrupts large-scale economic activities.

Financial losses due to cybercrime are not only felt by individuals or companies, but also have an impact on state revenues, such as reduced taxes and investment. For example, cases of technology-based fraud or money laundering harm state finances which ultimately affect fiscal and monetary stability. Cybercrime can create economic uncertainty, which ultimately affects macroeconomic stability, such as exchange rates, inflation, and public consumption levels. At the micro level, individuals and small businesses are often the main victims, which has an impact on economic and social inequality.

It can be said that digital economic crime has a significant impact on economic stability in Indonesia. Cybercrime cases such as financial data theft, money laundering, and e-commerce fraud can cause major financial losses, both for individuals, companies, and the state. On a national scale, these losses can reduce state revenues through lost taxes due to digital-based embezzlement or hampered investment. In addition, incidents of digital economic crime can reduce public trust in technology-based economic systems, including digital wallets, e-commerce, and online payment platforms. This distrust can slow down the transformation of the digital economy in Indonesia, which is currently one of the drivers of economic growth.

Digital economic crime also has an

impact on the investment climate. The inability to overcome digital economic crime can worsen Indonesia's competitiveness in the international arena. Investors, especially foreign investors, tend to avoid countries that have a high risk of cybercrime. Economies that are vulnerable to cybercrime find it difficult to compete with other countries in attracting investors and developing technological innovation. This reduces the flow of investment needed to support national economic growth.

In addition to affecting investment, digital economic crime also affects social and microeconomic stability. Victims of digital economic crime, such as Small Medium Enterprises (MSMEs) or small communities that depend on digital platforms, often lose capital or important assets. This has an impact on economic instability at the micro level, which ultimately affects social stability. Because it is a burden on the country's legal and financial systems, handling digital economic crime requires a significant budget allocation for investigations, digital forensic technology, and strengthening regulations. This burden can affect state finances, which should be allocated for development.

The Effectiveness of National Legal Regulations in Dealing with Economic Crimes in The Digital Era (Cybercrime).

As is known, some Indonesian laws still inherit colonial law (the principle of concordance), therefore economic crimes are still regulated in Emergency Law (UUD) Number 7 of 1955 concerning the Investigation, Prosecution, and Trial of Economic Crimes (UU PTPE).

However, in discussing of economic crimes in the digital era (cybercrime), Indonesia has several national laws that specifically include:

Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) which regulates the use of information technology and electronic transactions and establishes sanctions for perpetrators of cybercrime.

Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU) which includes money laundering activities based on digital technology.

Regulation of the Financial Services Authority (OJK) which regulates the digital financial sector to prevent economic crimes in this sector.

Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) has regulated several matters related to digital-based economic crimes (cybercrime) in Indonesia. Article 31 of the ITE Law regulates the violation of tapping or intercepting electronic information or electronic documents belonging to other people. Article 48 of the ITE Law regulates the violation of transferring data belonging to other people or public property. Article 28 paragraph (1) of the ITE Law regulates the violation of distributing or transmitting electronic information or electronic documents with the intention of benefiting oneself or others unlawfully. In addition, Law Number 1 of 2024 also regulates the protection of public interests from disruption due to misuse of electronic information and electronic transactions.

The increasing scope and prevalence of digital-based economic crimes (cybercrime) encourages the government to conduct supervision. Supervision of digital economic crimes (cybercrime) is one of the key elements in efforts to prevent and eradicate these crimes. This supervision involves various parties, from the government, the private sector, to the general public. Supervision is carried out through the development and strengthening of information technology infrastructure, including early detection systems to identify potential threats. The government through institutions such as BSSN (National Cyber and Crypto Agency) has a strategic role in ensuring the protection of digital data and systems in Indonesia.

The National Cyber and Crypto Agency (BSSN) is a government agency of the Republic of Indonesia which is a transformation of the National Crypto Agency which was established on April 4, 1946 and changed its name in May 2017. Some of the authority of this agency also comes from the Directorate of Information Security and the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) which comes from the Ministry of Communication and Information. This agency is tasked with implementing cybersecurity and cryptography effectively and efficiently by utilizing, developing, and consolidating all elements related to cybersecurity and cryptography.

BSSN was formed to consolidate overlapping authorities, duties, and functions between cyber-related

institutions such as Kominfo, BIN, Ministry of Foreign Affairs, Ministry of Defense, TNI, Polri and other institutions. Previously, the forerunner of this agency was the National Cyber Information Security and Resilience Desk (DK2ICN) which was under the Coordination of the Coordinating Ministry for Political, Legal, and Security Affairs.

In addition to BSSN, the Financial Services Authority (OJK) and Bank Indonesia (BI) also oversee digital economic activities, including electronic financial transactions. This oversight involves the implementation of technology-based Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) policies. AML and CFT are a set of interrelated regulations and measures designed to combat illicit financial activity worldwide. The purpose of AML and CFT is to stop criminals and terrorists from abusing the financial system and to help track and stop financial flows linked to terrorism and serious crime.

In addition, digital-based economic crimes (cybercrime) are often transnational in nature, so supervision requires cooperation between countries. This includes the exchange of intelligence information, tracing cross-border assets, and harmonization of regulations at the international level. Supervision will be effective if followed by strict law enforcement against perpetrators of criminal acts. This involves a legal process that is fast, transparent, and in accordance with applicable procedures.

One of the major cases of digital-based economic crimes (cybercrime) that occurred in Indonesia was investment fraud through digital platforms such as "trading robots" that did not have permits. A real example is the Binomo and Quotex cases, where thousands of people were harmed with a total loss of billions of rupiah. In this case, the perpetrators used digital technology to reach victims widely. Another example of cybercrime was in 2022, where a hacker named "Bjorka" managed to leak data belonging to the Indonesian public and government on an online forum. This case shows the weak security of digital data that can be exploited for economic crimes, including illegal data trading.

This example proves that even though national legal regulations are available, there are still several challenges in their implementation, such as the interpretation of the law that is not yet uniform and the gap between the technology used by criminals and existing legal regulations. This is due to the characteristics of digital crimes which tend to be complex, cross-border, and involve technology that continues to develop. In its implementation, law enforcement related to cyber crime still faces obstacles, including: 1

Digital technology is developing very rapidly, so that criminals can easily exploit new security gaps before the legal system and surveillance technology are able to catch up. For example, as explained above, the use of blockchain technology for money laundering is difficult for authorities to track.

Limited Human Resources (HR) where our law enforcement officers often do not have the technical expertise to handle complex digital economic crimes.

Lack of technological infrastructure where handling cyber crime cases requires sophisticated technology for tracking and collecting digital evidence. However, many legal institutions in Indonesia are not yet fully equipped with this technology.

Long legal process where case handling procedures are often slow, so that digital criminals can exploit this gap to first eliminate traces of their crimes.

Lack of international cooperation where many cases of digital economic crime are cross-border, thus requiring close international cooperation. However, coordination between countries is often hampered by differences in law, culture, and bureaucracy.

National legal regulations have provided a framework for dealing with digital economic crimes, but their effectiveness is still limited by suboptimal implementation, inadequate infrastructure, and lack of cross-country cooperation. The effectiveness of regulations is also influenced by the level of digital literacy of the community. The low level of public understanding of the risks of digital economic crimes and how to protect themselves is one of the causes of the high number of victims of these crimes.

To increase effectiveness, several things are needed, such as:

Strengthening the capacity of law enforcement officers by providing advanced technology training to law enforcement officers.

Harmonization of regulations carried out by revising regulations to be more

relevant to more advanced/latest technological developments.

Increasing digital literacy, such as educating the public to understand the threat of cybercrime. With the steps above, it is hoped that economic crimes in the digital era (cybercrime) can be handled more effectively.

4. CONCLUSION

Based on the results of the discussion described above, the conclusions that can be drawn in this research are:

Economic crimes in the digital era (cybercrime) have a significant impact on economic stability in Indonesia, the main impact of which is significant financial losses; public distrust of the digital financial system; disruption to investment that can lead to a decline in economic competitiveness in the international arena; and can also be a burden on the country's legal and financial systems.

National legal regulations have provided a framework for dealing with economic crimes in the digital era (cybercrime), but their effectiveness is still limited by less-than-optimal implementation, inadequate infrastructure, and lack of cross-country cooperation.

Based on what described above, the suggestions that the author can convey in this research are:

Economic crimes in the digital era (cybercrime) are not only a criminal problem, but also threaten the stability of the Indonesian economy as a whole. Therefore, collaboration is needed between the government, private sector, and society in increasing digital literacy, strengthening regulations, and improving digital security systems to minimize the negative impacts of this digital economic crime.

To improve the effectiveness of national legal regulations, it is necessary to strengthen the capacity of law enforcement officers related to training on advanced technology; revise regulations to be more relevant to increasingly sophisticated technological developments; and also provide education to the public to better understand the threat of cyber crime.

REFERENCES

Fadila, Z. (2024). *TINDAK PIDANA EKONOMI DI DUNIA DIGITAL : PENIPUAN JUAL BELI ONLINE DAN REGULASI HUKUMNYA DI INDONESIA*.

Fuady, M. E. (2005). "Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia. *Mediator: Jurnal Komunikasi*, *6*(2), 255–264. https://doi.org/10.29313/mediator.v6i2.1194

Indrajit, R. E. (2000). *Pengantar konsep dasar manajemen sistem informasi dan teknologi informasi*.

Marzuki, P. D. M. (2017). *Penelitian Hukum: Edisi Revisi*. Prenada Media. https://books.google.co.id/books?id=CKZADwAAQBAJ

Muhammad Ramadhan, Ariyanti, D. O., & Nita Ariyani. (2020). Pencurian e-money pada e-commerce dalam Tindak Pidana Cybercrime sebagai Tindak Pidana Ekonomi. *Reformasi Hukum*, *24*(2), 169–188. https://doi.org/10.46257/jrh.v24i2.179

Raharjo, A. (2002). *Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi*. Citra Aditya Bakti.

Toni, H., Rolando, D. M., Yazid, Y., & Putra, R. A. (2021). Fenomena Cyber Religion sebagai Ekspresi Keberagamaan di Internet pada Komunitas Shift (Cyber Religion Phenomenon as a Religious Expression on the Internet in the Shift Community). *Jurnal Dakwah Risalah*, *32*(1), 56. https://doi.org/10.24014/jdr.v32i1.11626

Winarno, W. (2015). SEBUAH KAJIAN PADA UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE). *Jurnal Ekonomi Akuntansi Dan Manajemen*, *10*(1). https://jurnal.unej.ac.id/index.php/JEAM/article/view/1207