ABSTRACT

Objective: Technological developments in the digital era are something that cannot be avoided. These significant changes have occurred in the financial industry throughout the world, including in Indonesia. Financial technology or in another language equivalent is financial technology (Fintech) as a result of exposure to technology is a new thing in Indonesia that continues to develop rapidly. This is because financial technology makes it easier for people to carry out transactions safely and more efficiently. In connection with these benefits, there are also other negative things, one of which is related to cybercrime (cyberlaw).

Methods: By using normative juridical methods with secondary sources, this paper concludes that the government does not yet have a separate law related to financial technology regulations, but the substance regarding technological developments can be found scattered in other regulations and an approach to introducing cyber law is needed. towards business people and the wider community so as to create a legal function, namely as legal certainty and justice.

Results: This development is accompanied by the development of the world of crime in the world of technology, namely cybercrime. This crime is a transnational crime and requires a more comprehensive approach to tackling this crime. In positive law, regulations related to cybercrime are regulated in Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronics and updated in Law No. 1 of 2023 concerning the Criminal Code. However, the provisions regarding cybercrime in this law are not accommodated holistically.

Suggestions: It is necessary to create a separate law regarding fintech which regulates cybercrime. It is necessary to regulate consumer protection accompanied by criminal sanctions whose elements regulate from upstream to downstream related to financial technology. Regulations at the statutory level provide legal certainty because in theory the hierarchy of statutory regulations has a higher status than regulations regarding fintech which are only regulated at the institutional regulatory level. Regulations at the statutory level also avoid overlapping regulations between state institutions, thereby creating legal certainty for fintech business actors.

Keywords: judicial review, cyber law, fintech, Indonesia.
USO DE FUNDOS HAJJ PARA DESENVOLVIMENTO DE INFRAESTRUTURA: UMA REVISÃO DE DEPÓSITO CONTRATO E USO DE FUNDOS HAJJ

RESUMO

Objetivo: A evolução tecnológica na era digital é algo que não pode ser evitado. Estas mudanças significativas ocorreram na indústria financeira em todo o mundo, incluindo na Indonésia. A tecnologia financeira ou em outro idioma equivalente é a tecnologia financeira (Fintech), como resultado da exposição à tecnologia, é algo novo na Indonésia que continua a se desenvolver rapidamente. Isso ocorre porque a tecnologia financeira torna mais fácil para as pessoas realizarem transações com segurança e eficiência. Em ligação com estes benefícios, existem também outras coisas negativas, uma das quais está relacionada com o crime cibernético (direito cibernético).

Métodos: Ao utilizar métodos jurídicos normativos com fontes secundárias, este artigo conclui que o governo ainda não possui uma lei separada relacionada às regulamentações de tecnologia financeira, mas a substância relativa aos desenvolvimentos tecnológicos pode ser encontrada dispersa em outras regulamentações e é necessária uma abordagem para introduzir a lei cibernética junto dos empresários e da comunidade em geral, de modo a criar uma função jurídica, nomeadamente como segurança jurídica e justiça.

Resultados: Este desenvolvimento é acompanhado pelo desenvolvimento do mundo do crime no mundo da tecnologia, nomeadamente do cibercrime. Este crime é um crime transnacional e requer uma abordagem mais abrangente para combatê-lo. No direito positivo, a regulamentação relacionada com o cibercrime é regulamentada na Lei n.º 19 de 2016, relativa às alterações à Lei n.º 11, de 2008, relativa à Informação e Eletrónica e atualizada na Lei n.º 1, de 2023, relativa ao Código Penal. No entanto, as disposições relativas ao crime cibernético nesta lei não são acomodadas de forma holística.

Sugestões: É necessário criar uma lei separada para fintech que regule o crime cibernético. É necessário regular a proteção do consumidor acompanhada de sanções penais cujos elementos regulam de montante a jusante relacionados com a tecnologia financeira. Os regulamentos a nível estatutário proporcionam segurança jurídica porque, em teoria, a hierarquia dos regulamentos legais tem um estatuto mais elevado do que os regulamentos relativos às fintech, que são regulamentados apenas a nível regulamentar institucional. As regulamentações a nível estatutário também evitam a sobreposição de regulamentações entre instituições estatais, criando assim segurança jurídica para os intervenientes empresariais das fintech.

Palavras-chave: revisão judicial, direito cibernético, fintech, Indonésia.

1 INTRODUCTION

Mother's Nowadays, business transactions do not need to oblige or require the seller and the buyer to meet face to face and then pay and receive (ijab kabul) using demand deposits in carrying out a business transaction, business transaction kits can be carried out using cyberspace or internet facilities. One of the technological developments in the millennial era is the field of financial services. Technology-based financial innovation or what is usually called Financial Technology (fintech) has become a system that is developing in Indonesian society. Technological sophistication such as speed is
the main differentiator from other instruments, resulting in effectiveness and efficiency. Fintech has become a favorite in the wider community.

Reported on the Bank Indonesia website, Fintech is the result of a combination of financial services and technology which ultimately changed the conventional business model to a moderate one, where initially you had to meet face to face to pay and bring a certain amount of cash, now you can carry out long distance transactions by making payments which can be made in just a matter of seconds.\(^2\)

Fintech is defined as technological innovation in financial services that can produce business models, applications, processes or products with material effects related to the provision of financial services. Fintech has transformed the financial services sector. These changes occur, among others, in the areas of: retail and wholesale payments, financial market infrastructure, investment management, insurance, insurance, credit provision and capital increase. The development of Fintech in the Indonesian business world is not just random, in 2022 the Indonesian Ministry of Communication and Information revealed the value of sector transactions fintech Indonesia, with Compound Annual Growth Rate (CAGR) of 39%, the second highest among G20 developed countries. This superior performance shows that Indonesia has progressive prospects as momentum accelerates the digitalization of the financial services sector in Indonesia.\(^3\)

Based on reports from United Overseas Bank (UoB), PwC, and the Singapore Fintech Association (SFA), the number of financial technology companies in Indonesia continues to increase every year. Indonesia is recorded as having 440 companies fintech in 2017. The number then increased 32.5% to 583 companies a year after that. Number of companies fintech increased again to 691 units in 2019 and 758 units in 2020, the figure rose again by 3.56% to 785 companies fintech as of September 2021. For more detail, it is explained in the diagram as follows:\(^4\)

---

\(^3\) Bank Indonesia, "National Fintech Month, 1.5 Million People Participate and Get Fintech Education from the Government, Associations and Industry Players," Bank Indonesia, December 2022.
\(^4\) Alif Karnadi, "The Number of Fintechs in Indonesia Continues to Increase Until 2021," Data Indonesia, December 2021.
Based on reports from the Indonesian Fintech Association (Aftech), the majority of financial technology users (fintech) in Indonesia comes from individuals. This was stated by 42.7% of companies who were surveyed. According to its age, 70.8% of the main users are in the age range of 26-35 years. A total of 23.1 main users around 36-50 years old. Then, the proportion of main users in Indonesia aged 18-25 years is 6.1%. More details are depicted in the following diagram:

---

5 Febriana Sulisty Pratiwi, "The majority of Fintech users in Indonesia are aged 26-35 years," Indonesian Data, July 2023.
Display of usage data on fintech based on age, it correlates with the demographic bonus that Indonesia has. Indonesia has a period of time where the productive age has the largest portion, which is called the demographic bonus. With this connectivity, Indonesia has increasing and positive prospects for development fintech. In connection with these developments, it is crucial for the government to ensure the continuity of this growing business well. One of these guarantees is regulatory certainty. Legal instruments that provide certainty, justice and usefulness are important things to study in development fintech in Indonesia.

Fintech can be equated with electronic transactions which are regulated in regulations in Indonesia. Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions, in Article 1 paragraph 2 explains that electronic transactions are legal acts carried out using computers, computer networks and/or other electronic media. In the explanation of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions, it states that the virtuality characteristics of cyber space allow illegal content such as information and/or threats, the spread of false and misleading news, resulting in consumer losses in electronic transactions, as well as acts of spreading hatred. Sending
personal threats of violence or intimidation can be accessed, distributed, transmitted, copied, stored for re-dissemination from anywhere and at any time.

Crimes related to technology have become a new thing following technological developments. Term cyber crime is a criminal act committed in technological media. Computer crime or cyber crime in other words, cyber crime is a form of crime which uses the internet and computers as a medium for carrying out criminal acts. In previous similar research written by Muhammad Fachrurrary and Dirah Nurmla Siliwadi, entitled Regulation and Supervision Fintech in Indonesia: The Sharia Economic Law Perspective explains that services based on financial technology, according to its jurisprudential context, fall into the category fathu al-dzari’ah the essence of which is a breakthrough opportunity to carry out new innovations. Draft ittihad al-majeliscan get through so be it information technology, then that means basically powerful (via text/digital message) permitted by Sharia.6

In their research entitled Cybercrime and Cybersecurity on Fintech: A Systematic Review of Literature, Alexander Anggono, Tarjo, and Moh Riskiyadi In the conclusion, he explains that the problems of cybercrime in fintech include lack of regulation, theft of data and information, and theft of intellectual property, which impact on fintech reputation. Cybersecurity through proactive measures is needed to overcome cybercrime.7

Based on the explanation of the background of the problem and previous research, the author conducted inter-correlation research cyber crime Andfintech in Indonesia. How is the development of the political character of government law related to criminal law regulations in providing legal certainty for the creation of transactions fintech in Indonesia, especially the business world, has become safer. As advances in financial technology have been proven to benefit consumers, businesses and the national economy, laws must be adapted to anticipate risks that could disrupt the financial system if used properly.

2 RESEARCH METHODS

This research is normative juridical research, namely legal research carried out by reviewing the literature through secondary data or available literature. Normative legal

---

6 Muhammad Fachrurrazy and Dirah Nurmla Siliwadi, “Regulation and Supervision of Fintech in Indonesia; Sharia Economic Law Perspective,” Journal of Islamic Family Law and Humanity 02, no. 02 (December 2020): 2.
research on the normative side of law is carried out as knowledge practically normological law, can be the process of making a legal decision, including the relevant parties filling it out. empty normative law, can also explain norms of vague or biased, can also narrow the meaning or definition of something rule of law so that can be applied to a concrete legal event that requires legal settlement, or even be able to find rule of law. This paper uses a type of normative legal research to examine existing legal issues in Indonesia, particularly in the fintech sector, along with related legal regulations. To achieve the research objectives, a conceptual and comparative legal approach was used. This research uses approach rule legislation (statute approach) namely the jurisdictional rules in the Criminal Code. However, the data collection technique was carried out through literature study or library research, as well as a study of several cases that occurred in Indonesia, which was followed by qualitative data analysis. This research also uses basic law, namely law that is carried out with the aim of finding applicable positive legal standards or teachings.

3 RESULT

3.1 FINANCIAL TECHNOLOGY (FINTECH)

Financial Technology is the use of technology in the financial system that produces new products, services, technology and/or business models and can have an impact on monetary stability, financial system stability, and/or the efficiency, smoothness, security and reliability of payment systems. This understanding is the meaning stated in Bank Indonesia Regulation No. 19/12/PBI/2017 concerning the Implementation of Financial Technology. Financial Stability Board define fintech as a form of technological innovation in financial services that can produce business models, applications, processes or products with material effects related to the provision of financial services. Therefore it can be concluded that fintech is a combination of cross-understanding subjects in the fields of technology, finance and innovation management.

9 Soerjono Soekanto and Sri Mamudji, Normative Legal Research (Jakarta: Rajagrafindo Persada, 2009), 6.
11 Bachtiar, Legal Research Methods (South Tangerang: Unpam Press, 2018), 69.
12 Muhammad Afdi Nizar, "Financial Technology (Fintech): Concept and Implementation in Indonesia" (Jakarta, December 2017), 6.
In History and Development fintech in the world can be divided into three periodic timelines from the point of view of periodic functions as follows:  

1. Fintech 1.0 (1866-1967). When the initial financial globalization occurred, that was the first period fintech 1.0 started. It was marked by the first trans-Atlantic cable connection between Europe and America in 1866, before the first ATM system was invented by Barclays in 1967. During this period, the financial sector had adopted traditional analog technologies such as the telegraph, railroads, canals, and steamships, which supports cross-border financial linkages, enabling rapid transmission of financial information, transactions and payments worldwide.

2. Fintech 2.0, period 1967–2008. Most people believe that the invention of the Barclays ATM in 1967 marked the beginning of the era of digitalization in the financial industry. Wells Fargo started the first internet banking via the World Wide Web (WWW) in 1995 to give financial customers a first-time experience using the internet. Conventional financial companies such as banking conglomerates and insurance companies are usually called fintech 2.0.

3. Fintech 3.0 and 3.5 (2008-present). Regarding the stages of development of the period fintech 3.0, some believe that geographic location may have played a big role in determining the evolutionary phase of a startup fintech. The Global Financial Crisis (GFC) of 2008 was a critical transition from fintech 2.0 sometime fintech 3.0 in the western hemisphere.

Fintech technology first appeared in Indonesia in 2015. The Indonesian Fintech Association (AFI) was founded to provide facilities to capable business partners in the financial technology industry. Indonesian fintech companies began to emerge in 2016. The increasing use of the internet and social media in Indonesia every year is one of the factors that encourages the government to develop new products in the financial services sector. Presence fintech has had a lot of impact on various industries, especially the financial industry. As reported by Forbes, Sorrentino (2015), stated that the banking industry will experience changes with the presence of fintech and the increasing popularity of new technologies such as blockchain, artificial intelligence, and the dominance of millennials.

---

13 Padjadjaran University Faculty of Economics and Business, “Fintech in Indonesia” (Bandung, February 2022), 4–8.
Usage financial technology in the financial industry has a big impact on players in the financial industry. As is fintech can shorten the service flow in the financial industry to be efficient and effective. Fintech making these services easier with technology that allows the financial industry to automate services, predictive analysis, digital banking and digital banking, blockchain, and others. Carney explained that financial technology started from the financial sector of the economy, which has become an important sector and continues to develop to meet society's needs. Financial technology has developed not only in developed countries, but also in developing countries, such as Indonesia. Financial technology provides new hope for convenience in various financial transactions in various industries.\(^{14}\)

Classification Financial technology (Fintech) according to Bank Indonesia is divided into 4 types, including the following:\(^{15}\)

1. **Peer-to-Peer (P2P) Lending**. And **Fundraising**. Fintech this one is like market financial. This platform is able to bring together parties who need funds with parties who can provide funds as capital or investment. In the UK, the provision of funds through P2P Lending has doubled in a relatively short period of time. The provision of P2P Lending loan funds was recorded at 1 billion pounds sterling and 2 billion pounds sterling in 2014 and 2015 respectively. In 2021, the total amount will be 25.7 billion in the first half-year period of 2021. Indonesia itself is no less interested in fintech this one. As of May 2021, there were 118 organizing companies fintech loans conventional and 9 companies fintech loans registered sharia.\(^{16}\) In the Financial Services Authority (OJK) Regulation No 77/POJK.01/2016 it is stipulated that the OJK is the institution that regulates, grants permits and supervises fintech P2P Lending registered.

2. **Investment Risk Management**: Types Fintech This can be used to monitor financial conditions and carry out financial planning more easily and practically. They can usually be accessed via smartphone and only need to provide the data necessary to keep an eye on finances.


\(^{15}\) Ratnawaty Marginingsih, "Financial Technology (Fintech) in National Financial Inclusion During the Covid 19 Pandemic," *Journal of Accounting and Finance* 08, no. 01 (April 2021): 58.

3. Payment, Clearing and Settlement There are several financial startups that fall into this fintech category, such as payment gateways or fintech payment gateway digital wallets, which connect e-commerce businesses with various banks so that both parties can carry out transactions. The term "electronic money" is often used for this type. There are many new fintech companies in Indonesia, such as OVO, Linkaja, Brizzi, Gopay, and many more.

4. Market Aggregator. His presence fintech this refers to a portal that collects various types of information related to the financial sector to present to its users. Usually fintech This type includes information related to finance, tips, credit cards and other financial investments. His presence fintech This type is expected to be able to absorb a lot of information before making financial decisions.

The development of the fintech industry can be considered as a result of the process of integrating technology with various economic activities around the world through digitalization. These developments are part of a strong current of digital transformation that has occurred over the last ten years. There are two legal bases or rules of the game at the relevant level of governing authority fintech, namely Bank Indonesia Regulation No. 19/12/PBI/2017 concerning the Implementation of Financial Technology and Regulation of the Financial Services Authority of the Republic of Indonesia No. 13/POJK. 02/2018 concerning Digital Financial Innovation in the Financial Services Sector.

In the PBI, Article 2 states that Bank Indonesia regulates the implementation of financial technology to encourage innovation in the financial sector by applying the principles of consumer protection as well as risk management and prudence in order to maintain monetary stability, financial system stability and an efficient, smooth, safe and reliable payment system. Article 15 in the PBI states that financial technology operators who are included in the category of Payment System Service Providers must obtain permission from Bank Indonesia in accordance with Bank Indonesia regulations governing the implementation of payment transaction processing.

Financial Technology Operators receive sanctions based on the PBI, including: a) written warning; b) termination of business activities; c) certain actions related to organizers, payment system activities; and/or; d) recommendation to the competent authority to revoke the business permit granted by the said competent authority. In the OJK Regulations mentioned previously, it is known as Digital Financial Innovation,
hereinafter abbreviated to IKD. Activists for updating business processes, business models and financial instruments that provide new added value in the financial services sector by involving the digital ecosystem is the meaning of IKD.

Article 3 of the POJK explains the scope of IKD, which includes: a) Settlement of transactions; b) Capital raising; c) Investment management; d) Collecting and distributing funds; d) Insurance; e) Market support; f) Other digital financial supporters; and/or; f) Other financial services activities.

Article 4 explains the criteria for IKD, namely as follows: a) Innovative and forward-oriented; b) Using information and communication technology as the main means of providing services to consumers in the financial services sector; c) Support financial inclusion and literacy; d) Useful and can be used widely; e) Can be integrated into existing financial services; f) Using a collaborative approach; And g) Pay attention to aspects of consumer protection and data protection.

Data protection and confidentiality is essential in the running of the business. OJK guarantees that organizers are obliged to maintain the confidentiality, integrity and availability of personal data, transaction data and financial data that they manage from the time the data is obtained until the data is destroyed. Not only that, organizers are also required to apply basic principles in consumer protection such as transparency, fair treatment, reliability, confidentiality and security of consumer data/information and handling complaints and resolving consumer disputes in a simple, fast and affordable manner.

3.2 JURIDICAL REVIEW OF CYBER CRIME IN FINTECH

Cyber crime is one of the fruits of technological progress. But unfortunately this fruit actually has a negative result that has a broad impact on life in today's modern era. Volodymyr Golubev calls it “new forms of anti-social behavior”. Several other well-known nicknames/names have been given to this new type of crime in various writings, including cybercrime (cyber/cyberspace violations), a new dimension of “hitech crime”, new dimension of "transnational crime”, and new dimensions of “white collar crime.”

Development of cyber crime which can be seen so quickly from the emergence of various terms, such as economic cyber crime, EFT (Electronic Fund Transfer Crime) Cyberbank Crime, Internet Banking Crime, On-line Business Crime, Cyber/Electronic

---

17 Dwi Haryadi, Integral Policy for Combating Cyberporn in Indonesia (Semarang: Lima, 2012), 44.
Money Laundering, Hitech WWC (White collar crime), Internet Fraud, Cyber terrorism, Cyber stalking, Cyber sex, world pornography cyber (child), cyber defamation, cyber criminals, etc.  

Based on several literatures and practices, cyber crime has a distinctive character compared to conventional crimes, including:

1. Actions carried out illegally, without rights or unethically occur in virtual space/territory (cyberspace), so it cannot be ascertained which country's legal jurisdiction applies to it;
2. This act is carried out using any equipment that can be connected to the internet;
3. These acts result in material and immaterial losses (time, value, services, money, goods, self-esteem, dignity, confidentiality of information) which tend to be greater than conventional crimes;
4. The perpetrators are people who master the use of the internet and its applications;
5. These actions are often carried out in person/transnational/cross national borders.

In general, the following is a division of forms of cyber crime, including:

1. Unauthorized access to Computer Systems and Services.

Mistakes committed by entering or infiltrating a computer network system illegally, without the permission or knowledge of the owner of the network system. Criminals, also known as hackers, usually do this with the aim of sabotage or theft of important and confidential information. However, some people do it simply because they feel challenged to try their skills to bypass highly protected systems. With the development of internet/intranet technology, this crime is increasingly widespread.

2. Illegal Content

Posting data or information about something that is incorrect or unethical on the internet is a crime that can be considered unlawful or disturbing public order. For example, spreading false news or slander that lowers a person's dignity or self-esteem; pornography; dissemination of information or information that is kept secret by the state; agitation and propaganda to fight against the legitimate government; etc.

---

3. **Data Falsification**

It is a crime to falsify data on important documents stored as unscripted documents through the internet. This crime is usually aimed at documents by making it appear as if there was a “typo” which will ultimately benefit the perpetrator.

4. **Cyber Espionage**

It is a crime to utilize the internet network to carry out spying activities against other parties, by entering the target party's computer network system (also known as the computer network system). This crime is usually directed at business rivals who have important documents or data stored in computer systems.

5. **Cyber Sabotage and Extortion**

This type of violation is committed by disrupting, destroying or destroying data, computer programs or computer network systems connected to the internet. Most of these crimes are committed by inserting logic bombs, viruses, or certain programs into computers so that data, programs, or computer network systems cannot be used, do not work properly, or function as desired by the perpetrator. After the incident, criminals sometimes ask victims to repair the data, computer programs, or network systems that have been sabotaged for a fee. Crimes like this are often called "cyber-terrorism".

6. **Violation of Intellectual Property**

This crime focuses on the intellectual property rights of other parties on the internet. For example, displaying content on a website that is owned by someone else illegally or spreading information that apparently belongs to someone else on the internet.

7. **Privacy Breach**

This crime exploits highly sensitive personal information, such as provided health information, credit card numbers, ATM PIN numbers, and so on.

Various types of cybercrime attacks that are often carried out by perpetrators in relation to fintech are fintech attacks. Exploiting cybersecurity gaps in multi-factor authentication or application connection protection by perpetrators are examples of frequent attacks. A mobile banking Trojan that breaks the mobile banking security code so that it can spread to the public domain Ransomware, which infects malicious applications and locks user data to demand ransom. Magecarting is a cybercrime attack that targets payment systems via the internet. As technology and network speed continue to develop, the risk of other cybercrimes increases. Fintech development is a professional
development that requires technical and ethical skills to reduce emerging risks, usually related to cybercrime.\textsuperscript{20}

A study shows that hacking, phishing, and malware impact cybersecurity suitability in the financial sector. Because a lot of personal and credit card data is stored and processed in e-commerce applications, cybercriminals prefer to commit crimes there.\textsuperscript{21} To overcome the risks of actioncyber crimeTherefore, legal sanctions are needed that can provide a deterrent effect on the perpetrators. Criminal law as last choice implementing sanctions, they have a big responsibility in resolving problems related tocyeber crimein the world of fintech. In the regulations at the applicable legal level, there are several criminal provisions related to cyber crime, including the following:

\subsection*{3.2.1 Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronics}

Article 45 paragraph 4 (four): Every person who intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents which contain extortion and/or threats as intended in Article 27 paragraph (4 ) shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah). Article 45A paragraph 1 (one): Every person who deliberately and without right spreads false and misleading news which results in consumer losses in Electronic Transactions as intended in Article 28 paragraph (1) shall be punished with imprisonment for a maximum of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah).

Article 45B: Any person who intentionally and without authorization sends Electronic Information and/or Electronic Documents containing threats of violence or intimidation aimed at a person as intended in Article 29 shall be punished by imprisonment for a maximum of 4 (four) years and/or a maximum fine of IDR 750,000,000.00 (seven hundred and fifty million rupiah).

\textsuperscript{20} Edris, 13.
\textsuperscript{21} Rahadiyan, “Development of Financial Technology in Indonesia and the Regulatory Challenges Faced,” 19.
3.2.2 Law No. 11 of 2008 concerning Information and Electronics

Article 30:
(1) Every person intentionally and without authority or unlawfully accesses another person's computer and/or electronic system in any way.
(2) Any Person intentionally and without right or against the law accesses a Computer and/or Electronic System in any way with the aim of obtaining Electronic Information and/or Electronic Documents.
(3) Every person intentionally and without authority or unlawfully accesses a computer and/or electronic system in any way by violating, breaching, surpassing or breaching the security system.

Article 31
(1) Every Person intentionally and without right or against the law intercepts or intercepts Electronic Information and/or Electronic Documents on a Computer and/or certain Electronic System belonging to another Person.

Article 32
(1) Every person intentionally and without right or against the law in any way changes, adds, reduces, transmits, damages, deletes, moves, hides electronic information and/or electronic documents belonging to other people or public property.
(2) Any Person intentionally and without right or against the law in any way transfers or transmits Electronic Information and/or Electronic Documents to another Person's Electronic System without authorization.
(3) For actions as intended in paragraph (1) which result in the disclosure of confidential Electronic Information and/or Electronic Documents being accessible to the public with data integrity that is not as it should be.

Article 33
(1) Every person intentionally and without right or against the law carries out any action which results in disruption of the Electronic System and/or causes the Electronic System to not work properly.

Article 34
(1) Every person intentionally and without right or against the law produces, sells, procures for use, imports, distributes, provides, or possesses:
a. Computer hardware or software designed or specifically developed to facilitate actions as intended in Articles 27 to Article 33;
b. password via computer, access code, or something similar intended to make the Electronic System accessible with the aim of facilitating actions as intended in Articles 27 to Article 33
(2) Article 35: Every person intentionally and without right or against the law manipulates, creates, changes, deletes, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are treated as if they were authentic data.

3.2.3 Law No. 1 of 2023 concerning the Criminal Code (even though it only comes into effect in 2026)

Article 332
(1) Every person who intentionally and without right or against the law accesses another person's computer and/or electronic system in any way, shall be punished with a maximum imprisonment of 6 (six) years or a maximum fine of category V. 
(2) Every person who intentionally and without right or against the law accesses a computer and/or electronic system in any way with the aim of obtaining electronic information and/or electronic documents, shall be punished by imprisonment for a maximum of 7 (seven) years or a fine, at most category V.
(3) Every person who intentionally and without authority or unlawfully accesses a computer and/or electronic system in any way by violating, breaching, surpassing, or breaching the security system, shall be punished by imprisonment for a maximum of 8 (eight) years or a fine, at most category VI.

Article 334
Any person who:
a. without the right or exceeding their authority to use or access a computer or electronic system with the intention of gaining profit or obtaining financial information from a central bank, banking or financial institution, credit card issuer or payment card or otherwise contains customer report data;
b. without the right to use data or access in any way another person's credit card or payment card in electronic transactions to obtain profits;
c. without right or exceeding his/her authority to use or access a computer or electronic system of a central bank, banking institution or protected financial institution, with the intention of abusing it, or to gain profit from it; or
d. distribute, trade, or utilize Access Codes or information similar to this that can be used to break into computers or electronic systems with the intention of misuse which as a result can affect the electronic systems of central banks, banking institutions or financial institutions, as well as domestic and foreign commerce

In the regulations that have been explained, from a juridical perspective it is illustrated that there are several normative rules of criminal law related to cyber crime in this world. However, the author encourages the publication of regulations at the statutory level, specifically regulating fintech, for the following reasons: 1) There are several articles that have been revoked in Law No. 11 of 2008 concerning Information and Electronics and replaced in the new Criminal Code which will only come into effect in 2026, namely Article 30 and Article 31. And if you look further at the substance of Law 1 of 2023 which directly related to the world fintech, in quantity it is only regulated in 1 Article, namely Article 334. In terms of quality, the sound of the article elements contained in Article 334, which consists of 4 (four) letters, is more or less the same. For example, the elements in Article 334 letters a and c are both without rights or beyond authority, into the financial institution system, and with the intention of abusing or gaining profit. 2) Provisions are required regarding criminal sanctions give organizers fintech who commits a violation in terms of failing to carry out their obligations. And this section must also regulate the sanctions given to owners of activities who carry out illegal practices.

Regulations at the statutory level provide clearer legal certainty to the industry fintech. Because the current regulations governing this matter are mostly regulated at the level of certain institutional regulations. It is clear that these regulations are below the level of law in the hierarchy of statutory regulations. Another advantage is that if fintech regulated at the statutory level, the tendency to change these regulations becomes more difficult because it requires two institutions to change them, namely the DPR and the President and avoids overlapping regulations between state institutions, this of course provides greater legal certainty. One example of regulations regarding legal protection of consumer data in business fintech regulated at the level of ministerial or institutional regulations, such as
Minister of Communication and Information Regulation no. 20 of 2016 concerning Protection of Personal Data in Electronic Systems, POJK No. 13/POJK.02/2018 concerning Digital Financial Innovation in the Financial Services Sector, POJK No. 77/POJK.01/2016 concerning Information Technology-Based Money Lending and Borrowing Services, POJK No. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services

4 CONCLUSION

Business industry financial technology (fintech) is an industry that is and will continue to grow in Indonesia. the law lags behind the facts (the law is running slowly behind concrete events) and legal regulations are a must to ensure the continued growth of the business for the better. Two state institutions, namely Bank Indonesia and the Financial Services Authority, have responsibility for regulating this business, so Bank Indonesia Regulation No. 19/12/PBI/2017 concerning the Implementation of Financial Technology and Regulation of the Financial Services Authority of the Republic of Indonesia No. 13/POJK were issued. 02/2018 concerning Digital Financial Innovation in the Financial Services Sector.

This development is accompanied by the development of the world of crime in the world of technology, namely cyber crime. This crime is a transnational crime and requires a more comprehensive approach to tackling this crime. In positive law, regulations are related to cyber crime regulated in Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronics and updated in Law No. 1 of 2023 concerning the Criminal Code. However, the provisions regarding cyber crime in this law it is not accommodated holistically.
REFERENCES


Fachhrurazy, Muhammad, and Dirah Nurmila Siliwadi. “Regulasi Dan Pengawasan Fintech Di Indonesia; Perspektif Hukum Ekonomi Syariah.” Jurnal Hukum Keluarga Islam Dan Kemanusiaan 02, no. 02 (December 2020).


