Law and Justice
Vol. 8, No. 2, 2023, pp. 192-210
e-ISSN: 2549-8282
https://journals2.ums.ac.id/index.php/laj/article/view/2513

Legal Analysis on the Use of Deepfake Technology: Threats to Indonesian Banking Institutions

Indra Jaya Gunawan
Universitas Surabaya
indrajgunawan@staff.ubaya.ac.id

Sylvia Janisriwati
Universitas Surabaya

DOI: 10.23917/laj.v8i2.2513

Submission Track:
Received:
15 August 2023

Final Revision:
13 December 2023

Available online:
31 December 2023

Corresponding Author:
Indra Jaya Gunawan
indrajgunawan@staff.ubaya.ac.id

ABSTRAK

Rencana transformasi digital yang dilaksanakan oleh Otoritas Jasa Keuangan dalam industri perbankan telah memberikan dampak nyata dalam mempercepat evolusi perbankan Indonesia menuju basis teknologi informasi. Digitalisasi di sektor perbankan dengan mengadopsi penggunaan teknologi untuk setiap produk dan layanan terus dikembangkan untuk meningkatkan daya saing di antara para pelaku bisnis. Sementara itu, ada ancaman potensial yang dibawa oleh penggunaan teknologi yang disebut "Deepfake". Deepfake merupakan implementasi kecerdasan buatan (AI) untuk mereplikasi dan menghasilkan gambar palsu, suara, pola, dan/atau kombinasi dari mereka pada suatu subjek tertentu sehingga terlihat seperti aslinya. Teknologi ini berkembang tanpa disadari oleh sebagian besar orang mengenai potensi pencurian dan pemalsuan data identitas yang dapat dilakukan olehnya. Penelitian ini dilakukan untuk mengetahui ancaman potensial dari penyalahgunaan teknologi Deepfake di lembaga keuangan dan kesiapan regulasi serta lembaga keuangan untuk menghadapinya. Penelitian ini merupakan penelitian yuridis-normatif dengan pendekatan normatif dan konseptual. Hasil penelitian menunjukkan bahwa Indonesia perlu memiliki kerangka regulasi yang komprehensif dan implementasi yang akurat dari langkah-langkah pencegahan oleh lembaga keuangan terkait penggunaan teknologi dalam operasional bisnis mereka untuk menghindari bahaya penyalahgunaan teknologi. Penelitian ini dimaksudkan agar penyalahgunaan Deepfake dalam industri perbankan dapat diantisipasi dan dicegah sebelum muncul lebih banyak masalah hukum yang dapat merugikan bisnis dan pengguna.

Kata Kunci: Deepfake, Lembaga Perbankan, Kerangka Regulasi

ABSTRACT

The digital transformation plan carried out by Otoritas Jasa Keuangan

in banking industry has made real impact on accelerating the evolution of Indonesian banking towards an information-technology-basis. Digitalization on banking sector by adapting the use of technology to each line of products and services continues to be developed to increase competitiveness among business actors. At the same time, there is a potential threat brought by the use of technology called "Deepfake". Deepfake is an implementation of artificial intelligence (AI) to replicate and produce fake images, sounds, patterns, and/or combination of them on a particular subject so that it looks like the original. This technology evolved without being realized by most people regarding the potential for identity data theft and fabrication that can be carried out by it. This research conducted to find out the potential threat of Deepfake technology misuses in financial institutions and the readiness of regulations and financial institutions to deal with it. This study is juridical-normative research using statutory and conceptual approach. The results show that Indonesia needs to have a comprehensive regulatory framework and accurate implementation of preventive measures by financial institutions regarding the use of technology in their business operations to avoid the dangers of technology misuse. This study intended so that the misuse of Deepfake in the banking industry can be anticipated and prevented before more legal issues that can harm businesses and users arise.

Keywords: Deepfake, Banking Institutions, Regulation Framework

INTRODUCTION

The Government of Indonesia through the 2020-2024 National Medium-Term Development Plan (RPJMN) has mapped out 41 strategic priority projects (major projects) which aim to direct the Indonesian economy towards industrial development 4.0 (Otoritas Jasa Keuangan, 2021b). In order to support this, of course, it is necessary to have a massive and continuous source of funding. Banking institutions as the main pillar in supporting the financial system and the national economy have an important role to play in supporting the realization of sustainable development. Therefore, the development of banking products and services in recent years has continued to be improved in line with market needs and the digital transformation era.

The rapid development of information technology is now giving rise to new perspectives in every aspect of life, including people's behavior and expectations in accessing financial services, namely towards practical digital financial and economic services. This is inseparable from the high penetration rate of internet users in Indonesia, which is 69.8% in 2020 and will increase to 75.47% in 2022, and is expected to continue to rise to 82.53% in

2026 (Nurhayati-Wolff, 2021). The large number of internet users in Indonesia, as many as 210,026,769 users in 2021 (Arif, 2022), also supports the development of a digitalization climate in every sector of life. In fact, the potential value of Indonesia's digital economy, measured by Gross Merchandise Value (GMV), according to research results, will be the highest in Southeast Asia in 2025, which is worth $146,000,000,000 (Hadya Jayani, 2021). This direction of growth and digitization of the national economy is becoming increasingly important because it is hoped that it can rid Indonesia of the 'middle income-trap' phenomenon.

In line with this, OJK through the 2020-2025 Indonesian Banking Development Roadmap (RP2I) has launched four strategic directions for national banking, one of which is through accelerating digital transformation (Otoritas Jasa Keuangan, 2021b). This effort is aimed at accelerating the realization of digital banking, which is currently regulated through POJK Number 12/POJK.03/2018 concerning the Implementation of Digital Banking Services by Commercial Banks (POJK No. 12/POJK.03/2018 Tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum, 2018) and POJK Number 12/POJK.03/2021 concerning Commercial Banks (POJK No. 12/POJK.03/2021 Tentang Bank Umum, 2021). OJK outlines that the future development of banking entities will prioritize the following aspects: i) strengthening information technology governance and risk management; ii) use of IT Game Changers; iii) collaboration with business actors in the field of information technology; and iv) implementation of advanced digital banking. The Indonesian banking structure is expected to undergo a change in form towards an 'internet-only bank', namely a concept of banking services with organizational tools, governance systems and business processes that are very different from existing bank services, which concept has already developed in other countries, for example: WeBank (People's Republic of China), Kakao Bank (South Korea), Bunq (Netherlands), Fidor (Germany), Atom Bank and Monzo (England).

According to POJK 12/POJK.03/2021, a digital bank is a bank that provides and carries out business activities primarily through electronic channels *without a physical office other than the Head Office or using limited physical offices*. Meanwhile, the definition of digital banking services according to POJK 12/POJK.03/2018 is a service for customers to obtain information, conduct banking communications and transactions through electronic media, by optimizing the utilization of customer data in the context of services that are faster, easier, and according to needs, and can be carried out completely independently by customers. In

the relationship between the two concepts, it can be understood that digital banking is a new form of the banking world by carrying out the office-less concept, providing full online services, and implementing process automation through network-based services and Application Programming Interface (API) technology (Wijaya, 2021).

However, like the other side of the coin, banking digitalization also carries potential risks and challenges that need to be mitigated so as not to cause problems. These threats include leakage of user data, risks of cyber-attacks, challenges to information technology infrastructure, inadequate regulatory frameworks, and risks of misuse of technology (Otoritas Jasa Keuangan, 2021a). The use of IT game-changers; such as artificial intelligence (AI), blockchain, cloud services, and APIs, pose real threats that can have a direct impact on end-users, namely consumers. OJK, in its Blueprint for Digital Banking Transformation, stated that one of the potential risks of misuse of technology in question is the misuse of technology in the form of deepfakes (Otoritas Jasa Keuangan, 2021a).

Deepfake, which comes from a combination of the terms '*deep learning*' and '*fake*', is a technology that can electronically manipulate a text, image, audio, video, and/or a combination of all, to swap or imitate the face, expression, pattern or expression and voice of another person, so that it seems as if the impersonator is making expressions, gestures, and sounds like the appearance of the targeted person, including uttering sentences that the person being imitated has never actually uttered (Uddin Mahmud & Sharmin, 2020). Looking at the implementation of the use of deepfakes, OJK is aware of the potential threats that can be brought to banking institutions. Deepfakes can easily be used to avoid applying KYC principles, falsifying other people's profiles, abusing consumer privacy, and even breaking into consumer accounts. In the broader picture, the misuse of deepfakes can lead to criminal acts, namely bullying, extortion and fraud, pornography, identity forgery, forgery of electronic evidence, disinformation and influencing public opinion, propaganda, political polarization, and so on (Europol Innovation Lab, 2022). This condition is become more complicated by the limitations for the human eye and understanding in general to be able to easily distinguish original content from content that has been manipulated using deepfakes.

Real examples of the dangers of using deepfakes can be seen in the phenomenons that have occurred in recent years. In late 2022, Americans were shocked by a video clip showing Joe Biden, the current President of the United States, singing the children's song 'Baby Shark' as the national anthem in one of his public speeches (Goldin, 2022). It was later discovered that the video was edited by a British citizen with the help of deepfake

technology. Another case that resulted in material losses occurred in 2019, where one CEO of a UK-based subsidiary transferred amounts of up to $243,000 on orders from an insider who ‘had the exact same voice, accent and melody’ as his boss from the German parent company (Stupp, 2019). The calls were later found to be made by criminals who used AI technology to clone the voices of company executives to impersonate and commit fraud (spoofing). Similarly in Indonesia, there was a case involving the head of state and government, Joko Widodo, where a circulated video in October 2023 seemingly showed fluency in Mandarin during a state speech (Fransisca Lahur, 2023). However, upon investigation, it was revealed that the video's distribution was based on false information. Considering the growth of awareness and utilization of deepfakes among the Indonesian, it is also crucial to acknowledge their potential for misuse, which without prompt regulation and constraints, unrestricted use of deepfake can lead to significant negative consequences. Additionally, as part of Indonesian banking digitalization strategies, Bank Indonesia itself intends to integrate AI into its data centers and payment services (Aprilia, 2023), which potentially raises concerns about the misuse of AI within the banking sector.

Discussion regarding the legal aspects of deepfakes has been described in several previous studies; namely research by Sayid Muhammad RN (2019), Edvinas Meskys, et.al. (2020), Heny N. and Pudji A. (2021), and by Hafsha AA (2022). Research by Sayid Muhammad RN focuses on discussing alternatives to preventing deepfake abuse through legal instruments as a form of legal protection for victims of personal data abuse, with conclusions in the form of efforts to limit the publication of documentation and data selection, as well as the use of the ‘right to be forgotten’ as stipulated in Republic of Indonesia Law Number 11 of 2008 concerning Information and Electronic Transactions and its amendments (UU ITE), in the event that publication is not under the control of the data subject (Muhammad Rifki Noval, 2019). Furthermore, research by Hafsha A. A. discusses legal protection against falsification and misuse of personal data using deepfakes and their connection when used for peer-to-peer loan applications, and it is concluded that regulations governing deepfakes at the statutory level do not yet exist (Amalia Afnan, 2022). In Edvinas Meskys, et.al.’s research, it was concluded that ethical issues and the legitimacy of deepfakes will be determined by market influences and regulatory responses will not be able to compete with the speed of their use within social structures, although in the end the need for developing AI to detect deepfakes with harmful content is still needed (Meskys et al., 2020). Meanwhile, in the research by Heny N. and Pudji A., it was concluded that the misuse of

deepfakes fulfills the elements of criminalization and is a criminal offense under the ITE Law and Republic of Indonesia Law Number 44 of 2008 concerning Pornography (Novyanti & Astuti, 2021). Among the four previous articles, none specifically addresses the threat of deepfakes within banking institutions, despite their profound economic impact on the state. This marks the necessity for regulations adjustment regarding the use of Deepfake AI in the banking sector, aligning with the government's proposed digitalization strategies. The difference in the object of study examined is the focus of issues related to regulatory readiness in Indonesia regarding the potential misuse of deepfakes in the banking industry in the era of banking digitalization, which has the potential to disrupt digital bank operations and affect customers, and how digital banks themselves can prevent it.

Based on the explanation above, this study specifically discusses the potential threat of deepfakes to the digitization of financial institutions, especially to banks, where there are additional potential technology risks (technology risks) that banking institutions must be aware of. The security of consumers' personal data, including financial information and customer deposits, can become a target for crime if regulations and preventive instruments in the banking sector against deepfakes are not regulated immediately. Therefore, this research will discuss the potential threat of deepfakes that can be posed to banking institutions and the current readiness of Indonesian regulations to prevent this problem. The purpose of this study is to analyze the level of deepfake threat in banking institutions in Indonesia and obtain effective preventive solutions to minimize it.

RESEARCH METHOD

This writing made based on legal research in a normative-juridical research, namely by examining the laws and regulations related to the subject matter. In order to support the intended legal research, this writing use the statute approach and conceptual approach. The statute approach is used to determine the legal provisions in Indonesia that apply or may apply to deepfakes and its relationship to digital banking, while conceptual approach is used to compare the existence of deepfakes and its relationship to digital banking with existing legal concepts and principles, so that it can be determined whether the use of deepfakes is a legal problem. The legal materials used in this writing are primary legal materials, such as Republic of Indonesia Law Number 7 Year 1992 concerning Banking and its amendments (including Law Number 10 Year 1998 concerning Banking and Law Number 4 Year 2023

concerning Development and Strengthening of the Financial Sector), POJK 12/POJK.03/2018, and POJK 12/POJK.03/2021, as well as secondary legal materials, namely opinions, views, explanations and/or doctrines of legal experts contained in books, journals, papers, comments, and other forms of literacy. Analysis of legal material is carried out by examining laws and regulations, theories and views of legal experts to solve the problems studied. The legal material obtained will be described descriptively and systematically, so that an appropriate conclusion can be found along with a solution that is the answer to the problem in question.

RESULTS & DISCUSSION

Deepfakes and its applications

Deepfake is a technological advancement that uses AI intelligence and machine learning to create content (both images, audio and video) that is fake (synthetic) through the following methods: altering, swapping, merged, or superimposing original content (Thi Nguyen et al., 2022). The purpose of using a deepfake is to create, replicate, imitate, or change someone's appearance (both in the form of appearance or expression in the form of images or videos or imitation of voice in the form of audio recordings; voice cloning). The result of using a deepfake is in the form of a fake (engineered) appearance of the subject and being manipulated to do or say things that the intended subject does not actually do in reality.

Deepfake content can be created with the help of a technology called Generative Adversarial Networks (GAN), which is a technology in machine learning classification that was first created by Ian Goodfellow, et. al. in 2014 (Alattas & Bayoumi, 2020). This technology consists of two main components, namely a generator (producer), an algorithmic system for generating images from random data, and a discriminator (separator), which is a component for assessing and distinguishing whether an image that is processed is original (authentic) or the result of production manipulation (C. Helmus, 2022). Both have contradictory roles, where the generator will continue to produce images in an effort to trick the discriminator, and conversely the discriminator will continue to study the structure and form of the image and train its understanding and processing skills for the resulting image (Meskys et al., 2020). Through trial-and-error learning methods over a long period of time, AI will have a large enough database to be able to generate fake images in less time and with better results.

One of the earliest applied technologies for generating deepfake content is 'real-time face capture and reenactment of RGB videos' devised by Justus Thies, et al. in 2016, which aims to manipulate and control the facial expressions of the target subject in the video to then be processed and re-imaged into a photo-realistic new video output. In simple terms, Justus Thies in his writings explains the steps for video image reprocessing are carried out by identifying and tracking the target facial structure, image deformation, transferring data from source to target, adjusting facial expressions and curves (mouth, facial expressions, etc.), initial reenactment trials, and finally re-rendering to produce a fake image that blends smoothly (Thies et al., 2020). In everyday life, unknowingly this technology has also been widely used by people, including in Indonesia. This can be seen from the many visual effects features (filters) and applications that can be accessed freely on the internet and social media, such as DeepFaceLab, FaceApp, Faceswap, Reface, and so on.

In relation to the discussion above, the misuse of technological advances in the field of machine learning, including deepfake AI, can pose a threat to the law enforcement system, the socio-political situation, and the business world (Awah Buo, 2020). In law enforcement, for example, in 2020 in a trial at a British court there was a submission of evidence by one of the parties which, after being traced, was fake, namely in the form of an audio recording that was fabricated using deepfake software. In fact, the abuse of deepfakes also generally leads to acts of bullying and pornography, for example the behavior of revenge porn and celebrity deepfakes (Meskys et al., 2020). Meanwhile in the business world, deepfake abuse combined with social engineering attacks such as phishing, baiting, ransomware, and so on, can easily be used as a tool of crime to deceive and manipulate others to gain economic advantage.

Thus, it can be understood that deviant behavior from using deepfakes is included in one type of cyber-crime. The characteristics of criminal behavior using, through or targeting data in an electronic device or internet connection in a borderless manner, in this case deepfake technology, can also be classified as a crime because it fulfills the elements of criminalization. In the view of criminal law, according to Moeljatno, the criminalization of an act must be based on three criteria: i) the determination of an act as a criminal act must be in accordance with the legal feelings that live in society; ii) criminal threats and imposition of criminal penalties are the main way to prevent violations of these prohibitions; and iii) in the event that there is a violation in the form of committing the said act, the government is really capable of enforcing the criminal threats regulated against it (Luthan, 2009). Furthermore, quoting the writings of Heny Novianti and Pudji Astuti, deepfake abuse is a crime because it actually

causes harm to society (especially for the victims) and if done repeatedly can lead to subsequent victims if enforcement is not immediately regulated (Novyanti & Astuti, 2021).

As Indonesian banking digitalization develops, deepfake abuse is a structural challenge that must be addressed immediately, both at the regulatory and implementation levels. Based on information from the National Cyber and Crypto Agency (BSSN), in 2021 there will be 1.6 billion traffic anomaly cases in the national banking sector (Ibrahim, 2023). There are at least 1,924 cases of cyber-attacks every month against banking institutions, with the most recent case in 2023 being a ransomware cyber-attack against Bank Syariah Indonesia (BSI) by a group of hackers in an international network who stole BSI customer data and demanded ransoms (Setyo Wardani, 2023). This does not rule out the fact that other technological risks that can occur in the banking sector in relation to the implementation and transformation of information technology, namely in the form of theft of personal data (customers and consumers of financial services), data leakage, unpreparedness of bank resources, third party risks, network infrastructure, and regulations related to products and institutions in the application of information technology in banking are not yet perfect.

Based on existing threats to the banking industry and the characteristics of criminalization of an act according to Moeljatno as previously explained, the misuse of deepfakes can be categorized as a criminal act that can threaten the existence of banking institutions, if in fact: i) it is carried out to obscure a reality and influence the perception of a subject which may causing losses (generally in material terms) for both victims, customers, banking institutions, and relevant third parties; ii) aims to obtain a reaction, namely in the form of economic benefits for the perpetrators of abuse; and iii) requires clear legal sanctions for acts of abuse in order to guarantee legal protection for society in a broad scope. First, for national banking institutions which are still in the early stages of transformation towards digitalization, they are very vulnerable and unfamiliar with the use of deepfakes. As a comparison, at the beginning of 2023 there was a fraud case with the mode of falsifying identity to withdraw some money from a BCA account even though the perpetrator physically visited the bank office and met face to face with bank employees (Perdana Kurniaputra, 2023). This is one of the potential threats in banking due to the weak application of the Customer Due Diligence principle which still involves the human element. If later banking digitalization is fully operational, while the technological infrastructure for anticipating cyber-crimes is inadequate, an increase in crime against the banking sector has the potential to occur. Second, crimes against the banking sector, with or without the use of deepfakes, are aimed at obtaining economic benefits for the

perpetrators. Along with this, the position of customers and/or consumers who use banking services is the party most vulnerable to being harmed, considering that their personal data and savings funds are fully managed by the bank. Therefore, banking digitization transformation must be carried out while still paying attention to data security and the interests of customers and consumers who use financial products and services.

Deepfake threats to banking institutions in Indonesia

Banks have the primary responsibility for customers or consumers who use their products and services. This is due to the existence of the principle of trust in the banking business between the bank and the consumer which is called a fiduciary relationship (Plato-Shinar, 2019). So, in carrying out its operational activities, the bank risks the trust placed in it by the public. Therefore, banks must always be careful in running their business (Sjofjan, 2015). Banks must base its business activities on relevant guidelines based on prudential banking principles to minimize bank operational business risks that may arise. The ability of a bank to be able to maintain these two variables is an important benchmark for measuring the reliability of the bank, and at a larger level it is also used as a supporting factor in strengthening the structure of the National banking system.

Referring to POJK Number 18/POJK.03/2016 concerning the Implementation of Risk Management in Commercial Banks (POJK No. 38/POJK.03/2016 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum, 2016), in article 4 it is stated that in carrying out bank business activities, banking institutions are primarily faced with 8 (eight) types of risks, namely: i) Credit Risk; ii) Market Risk; iii) Liquidity risk; iv) Operational Risk; v) Legal Risk; vi) Reputation Risk; vii) Strategic Risk; and viii) Compliance Risk. However, with regard to the development of information technology, regulators also do not close their eyes to the possibility of risks arising from the use of information technology. Therefore, initially POJK Number 38/POJK.03/2016 was issued concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks, which integrates the eight risks for Banks in relation to the use of information technology. Banks are hinted that it is necessary to implement information technology governance, so that in the future the Bank can manage the risks it faces effectively in each of its operational activities that have used information technology.

Article 2 POJK 12/POJK.03/2018 states that banks can provide electronic banking services or digital banking services. According to the provisions of Article 1 number 3,

electronic banking services are services for Bank customers to obtain information, communicate, and carry out banking transactions through electronic media. Furthermore, the output product of these electronic banking services is in the form of digital banking services, which according to the provisions of Article 1 number 4 are described as electronic banking services that are developed by optimizing the utilization of customer data in order to produce services that are more independent, fast, easy, and in accordance with customer needs, or what is then known as digital banking. In the provisions of Article 10, it is explained that digital banking services that can be provided by Banks include:

a. account administration, including opening and closing accounts, as well as updating customer data;
b. transaction authorization, both for financial and non-financial transactions;
c. financial management, namely banking services to assist customers in analyzing and planning the use of funds, including financial planning, implementation of financial transactions, as well as financial management consulting; and/or
d. other financial product services based on OJK approval.

In contrast to digital banks, Article 1 number 22 *jo.* Article 23 Paragraph (3) POJK 12/POJK.03/2021 describes it as a bank that provides and carries out business activities primarily through electronic channels without a physical office (other than for the needs of the head office) or by using a limited physical office. So that in digital banks, it is hoped that the implementation of banking operations can be fully carried out digitally, minimizing the presence and face-to-face between customers and the bank physically, as well as ease of transactions and use of financial products and services only through the platform provided. Article 24 Paragraph (1) POJK 12/POJK.03/2021 stipulates that Digital Banks must meet the following requirements:

a. having a business model using innovative and safe technology to serve customer needs;
b. have the ability to manage a prudent and sustainable digital banking business model;
c. have adequate risk management;
d. fulfill governance aspects including the fulfillment of directors who have competence in the field of information technology and other competencies in accordance with OJK regulations regarding the fit and proper test for the main parties of financial service institutions;
e. carry out the protection of customer data security; and

f. provide efforts that contribute to the development of a digital financial ecosystem and/or financial inclusion.

When viewed from the provisions of letter b and letter e, OJK requires that the implementation of digital banks must still prioritize prudent banking principles or prudence in banks and ensure the protection of customer data security. This is important considering the magnitude of the risks posed by the implementation of digital banking (or digital banking), so that comprehensive risk mitigation and guarantees for the protection and security of customer data must be carried out by banks. Therefore, it is specified in letter c that in practice, digital banks are required to have adequate risk management, both for the implementation of bank operations in general and in relation to the use of information technology (POJK No. 12/POJK.03/2021 Tentang Bank Umum, 2021).

Even though in practice there are two types of banks in the context of providing digital services, namely conventional commercial banks that provide digital banking services and digital banks themselves, the two types of banking services that use information technology support have the same problems and risks. In relation to the deepfake threat, the two banks in digital services face operational threats and unavoidable potential crimes, both against banks and bank customers as well as third parties as targets. For example, in current practice several digital banks have started implementing an account opening system only through the mobile banking application provided by the bank concerned. In the process, prospective customers only need to upload the required personal identity documents into the application and the entire account opening process will be carried out through interaction between the customer and the bank in the application, without going through the bank's physical office at all.

In one of the processes, it is the same as in conventional commercial banks to request authentication and a customer signature specimen at the time of opening an account, in some digital banks the process is replaced by a facial recognition process which is carried out via a video call connection. This is intended as a way of biometric authentication from the bank to identify customers and store the person's personal data. This mechanism is a development of the provisions in Article 11 POJK 12/POJK.03/2018, which stipulates that in conducting business relations with customers or prospective customers through digital banking services, banks are required to:

a. identification of customers or prospective customers; and
b. verification of customer or prospective customer information and supporting documents.

Verification referred to in letter a, in the provisions of Article 11 Paragraph (2) POJK 12/POJK.03/2018 it is explained that it can be carried out in the following manner:

1. face to face:
    a. directly (face to face); or
    b. use bank-owned software with bank-owned hardware or customer or prospective customer hardware; and/or
2. without going through face-to-face meetings but using bank-owned software with bank-owned hardware or customer or prospective customer hardware.

Furthermore, in the provisions of Paragraph (4) it is stated that the intended verification, whether carried out face-to-face or fully through software, is carried out by taking into account the authentication factor, at least two factors (two - factor authentication/ 2FA) with one of them being a customer characteristic factor (what you are). The ‘what you are ‘factor itself is one of three types of 2FA that verifies personality based on special characteristics that are only owned by the party concerned, for example fingerprint, facial, and/or eye retina biometric data (Kenton, 2022).

With such arrangements, can banking institutions be ensured that they are safe from the threat of crime using information technology, in this case deepfakes? The answer is no. As mentioned in an example case in the earlier section, the case of transferring a number of funds at the behest of a person using a voice altered by deepfake AI and spoofing does not only happen once or twice. In 2020, for example, there was a similar case in the UAE where criminals used an AI deepfake to clone the voice of a target subject, namely a director of a company, to ask the bank to transfer funds in the amount of $35,000,000 under the pretext of acquisition purposes (Julianto, 2021). The bank manager concerned authorizes the transaction because of his belief in the authenticity and legitimacy of the ‘voice’ of the customer in question, which according to him is the voice of the customer who is entitled and authorized for the transaction. Another recent case also occurred in Kerala, India, this year, where a man was tricked by criminals who changed the appearance of his face using deepfake technology and made a video call to the target subject to then borrow some money. The victim, in his confession, said that the face of the perpetrator who made the video call had the exact same face and appearance as one of his colleagues, the perpetrator even mentioned the names of several other friends of the victim to convince him (Bhati, 2023). Similar cases have also occurred in northern China, Mongolia to be precise, and it is even possible that they have

occurred or will occur in other parts of the world that have not been handled. In other words, the crime of using deepfakes against banking institutions can be seen from two perspectives, namely: i) banks as targets of crime, or ii) banks as media to support fraudulent crimes against third parties.

As it develops, the deepfake threat to banking institutions can create potential crimes with a much more developed mode. Reflecting on the cases that have occurred, deepfake threats against banks can occur in various modes, such as:

1. New account fraud, namely falsifying identity from the start when opening an account, using fake identities and documents or stolen information as the basis for opening an account or loan, thus convincing the bank that the identity used is the 'real' identity and then used as a basis for applying for a loan that will not be paid or even for money laundering crimes (Shufti Pro, 2022). This crime can be easily carried out when using deepfakes as a supporting instrument, because the characteristics of crimes that use identity forgery and fraud are in line with the functions that can be implemented by deepfakes;
2. Ghost fraud, which departs from the concept of ghost workers, is a phenomenon where there are employees who are still registered as workers at the company concerned and receive a salary, but in fact the person has actually been working for a long time or has never even worked (Ifeanyi Okagu et al., 2020). In relation to deepfakes, this crime is vulnerable to being abused by banks, if the perpetrator can steal the identity of a customer who has died and manipulated his identity using a deepfake, to continue to manage and withdraw all the facilities available to the customer who has died; and
3. Synthetic identity fraud, namely the crime of falsifying one's identity by using a combination of a number of information on the identity of the target subject, whether combined between original and fake information, completely artificial (fake), or information stolen or obtained illegally.

In the event that one mode or another of the above occurs, do Indonesian laws and regulations not have the proper mechanism to deal with it? As far as the author's understanding of the laws and regulations governing the banking sector, there are no legal provisions to prevent the potential threat in question. However, in the event that the actions mentioned above can be agreed as a crime, which has not been determined grammatically correctly and explicitly based on laws and regulations in Indonesia and is returned to the interpretation of judges as law enforcers and justice, then the handling of crimes against the use of deepfakes

against banks can refer to the provisions of Article 35 of the ITE Law, which stipulates ‘every person intentionally and without rights or against the law manipulates, creates, changes, deletes, destroys Electronic Information and/or Electronic Documents with the aim that Electronic Information and/or Electronic Documents are considered as if they were authentic data. This is because there is an unlawful nature in the act of abusing deepfakes, namely ‘without the authority attached to him or without him having the right to do so’ (Puslitbang Hukum dan Peradilan Badan Litbang Diklat Kumdil Mahkamah Agung RI, 2013), which means that as long as the use of deepfakes is not based on a legitimate basis (for example, the consent from the subject used as the model or something similar) and causes harm to certain parties, it should be categorized as a crime using Article 35 of the ITE Law.

Therefore, prevention and anticipatory measures against the threat of deepfake use against banking institutions return to banking readiness, especially digital banks and banks that provide digital banking services, both in terms of security infrastructure, risk management and mitigation measures, as well as minimizing the involvement of the human element in verifying and authenticating procedures that require information technology, to be able to guarantee the implementation of the principles of protection and security of customer personal data. Society as users also have an important role to be able to increase understanding and awareness of the potential dangers that can arise as the use of information technology increases in banking products and services. Finally, authorities as supervisors and regulators in the banking sector need to regulate security measures for information technology systems that can be used in the banking sector, such as using ‘secure by design’ framework approach, establishing a testing mechanism for digital systems carried out by banks, collaborating with private parties to improve digital security services, and/or develop the right cybersecurity knowledge and culture, in order to ensure the reliability of the expected digital models, processes and governance.

CONCLUSION

The conclusion to this legal writing are:

1. Whereas the deepfake threat to banking institutions is real and can endanger the reliability of banks, including the banking system in Indonesia, namely in the form of operational risks arising from the use of information technology in line with developments in the direction of transformation towards digitalization of Indonesian banking. Therefore, it is necessary to understand, juridically, that the misuse of

deepfakes in any form to obtain economic benefits and is carried out without rights is a criminal act, because of its illegal nature and the fulfillment of elements of criminalization against it.

2. Whereas the potential for cybercrime against the banking world can occur, both banks as the subject of crime targets and banks as a part involved in crime, with deepfakes as the main supporting media for carrying out these crimes, which mainly use elements of manipulation, forgery, and/or fraud, for example modes of crime such as new account fraud, ghost fraud, and synthetic identity fraud.
3. Whereas Indonesian regulations on banking operations in dealing with the threat of crime with a new mode of using deepfakes have not been optimally anticipated because risk management arrangements in the field of information technology implementation in banking have not yet been regulated in detail and comprehensively, and there has been no interference from the authorities as supervisors for prosecution of crimes using deepfakes. Steps to prevent and take action against fraud that have occurred are still being returned to each banking institution, and there is no mechanism for testing digital systems by the authorities against banks.

Therefore, the government needs to create guidelines through technical regulations and be able to monitor the use of technology in industrial sectors that involve the benefit of society and may have impact on the country on a large scale, including guidelines regarding privacy, security and accountability in the use of technology, especially IT game changer as mentioned above, as has been done by other countries in efforts to digitize the banking industry.

REFERENCES

Alattas, K., & Bayoumi, M. (2020). Artificial Intelligence in Deepfake Technologies Based on Supply Chain Strategy. *International Journal of Supply Chain Management*, *9*(5), 411–414. https://doi.org/https://doi.org/10.59160/ijscm.v9i5.5671

Amalia Afnan, H. (2022). Perlindungan Hukum Penyalahgunaan Artificial Intellegence Deepfake pada Layanan Pinjaman Online. In *Repository UMS*. Universitas Muhammadiyah Surakarta.

Aprilia, Z. (2023). *Makin Canggih, Perry Bilang BI Mulai Pakai Teknologi AI*. CNBC Indonesia. https://www.cnbcindonesia.com/tech/20231129195008-37-493136/makin-canggih-perry-bilang-bi-mulai-pakai-teknologi-ai

Arif, M. (2022). Profil Internet Indonesia 2022. In *APJII* (Issue June). https://online.fliphtml5.com/rmpye/ztxb/#p=99

Awah Buo, S. (2020). *The Emerging Threats of Deepfake Attacks and Countermeasures*. https://doi.org/https://doi.org/10.13140/RG.2.2.23089.81762

Bhati, D. (2023). *Kerala Man Loses Rs 40,000 to AI-based Deepfake WhatsApp Fraud, All About the New Scam*. Indiatoday.In. https://www.indiatoday.in/technology/news/story/kerala-man-loses-rs-40000-in-ai-based-deepfake-whatsapp-fraud-all-about-the-new-scam-2407555-2023-07-17

C. Helmus, T. (2022, July). Artificial Intelligence, Deepfakes, and Disinformation: A Primer. *RAND National Security Research Division, PE-A1043-1*.

Europol Innovation Lab. (2022). *Facing Reality? Law Enforcement and the Challenge of Deepfakes*. https://doi.org/10.2813/08370

Fransisca Lahur, M. (2023). *Konten Jokowi Pidato "Bahasa Mandarin", Kominfo: Deepfake, Acara 2015 & Bahasa Indonesia*. Tekno.Tempo.Co. https://tekno.tempo.co/read/1789272/konten-jokowi-pidato-bahasa-mandarin-kominfo-deepfake-acara-2015-bahasa-indonesia

Goldin, M. (2022). *Video of Biden singing 'Baby Shark' is a deepfake*. APNews.Com. https://apnews.com/article/fact-check-biden-baby-shark-deepfake-412016518873

Hadya Jayani, D. (2021). *Ekonomi Digital Indonesia Tertinggi di Asia Tenggara*. https://databoks.katadata.co.id/datapublish/2021/11/11/ekonomi-digital-indonesia-tertinggi-di-asia-tenggara

Ibrahim, M. (2023). *Bank Harus Waspada! Tiap Pekan Ada 1.924 Serangan Siber*. Infobanknews.Com. https://infobanknews.com/bank-harus-waspada-tiap-pekan-ada-1-924-serangan-siber/

Ifeanyi Okagu, F., Uzoamaka Obeta, Roseline & Thomas, & Chuko, F. (2020). The Plague of Payroll Fraud in Local Government Administration in Nigeria. *International Journal of Innovative Legal & Political Studies*, *8*(2), 22–30. http://seahipaj.org/journals-ci/june-2020/IJILPS/full/IJILPS-J-3-2020.pdf

Julianto, A. (2021). *Use Deepfake Theft Action In The UAE Won 35 Million Dollars*. Voi.Id. https://voi.id/en/technology/94752

Kenton, W. (2022). *What Is Two-Factor Authentication (2FA)? How It Works and Example*. Investopedia.Com. https://www.investopedia.com/terms/t/twofactor-authentication-2fa.asp

Luthan, S. (2009). Asas Dan Kriteria Kriminalisasi. *Jurnal Hukum Ius Quia Iustum*, *16*(1), 1–17. https://doi.org/https://doi.org/10.20885/iustum.vol16.iss1.art1

Meskys, E., Liaudanskas, A., Kalpokiene, J., & Jurcys, P. (2020). Regulating Deep Fakes: Legal and Ethical Considerations. *Journal of Intellectual Property Law and Practice*, *15*(1), 24–31. https://doi.org/10.1093/jiplp/jpz167

Muhammad Rifki Noval, S. (2019). Perlindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi: Penggunaan Teknik Deepfake. *Seminar Nasional Hasil Penelitian & Pengabdian Kepada Masyarakat (SNP2M)*, *November*, 13–18.

Novyanti, H., & Astuti, P. (2021). Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau dari Hukum Pidana. *Novum: Jurnal Hukum*.

Nurhayati-Wolff, H. (2021). *Internet penetration rate in Indonesia from 2017 to 2020 with forecasts until 2026*. Statista.Com. https://www.statista.com/statistics/254460/internet-penetration-rate-in-indonesia/#statisticContainer

POJK No. 38/POJK.03/2016 Tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, (2016). https://peraturan.bpk.go.id/Details/128349/peraturan-ojk-no-38pojk032016-tahun-2016

POJK No. 12/POJK.03/2018 Tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum, (2018). https://peraturan.bpk.go.id/Details/128612/peraturan-ojk-no-12-pojk032018-tahun-2018

Otoritas Jasa Keuangan. (2021a). Cetak Biru Transformasi Digital Perbankan. In Departemen Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan (Ed.), *Otoritas Jasa Keuangan*.

POJK No. 12/POJK.03/2021 Tentang Bank Umum, (2021). https://peraturan.bpk.go.id/Details/227209/peraturan-ojk-no-12pojk032021-tahun-2021

Otoritas Jasa Keuangan. (2021b). Roadmap Pengembangan Perbankan Indonesia 2020-2025. In Departemen Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan (Ed.), *Otoritas Jasa Keuangan*.

Perdana Kurniaputra, D. (2023). *Rangkaian Aksi Tukang Becak Tipu Teller BCA, Kuras Rekening Rp 320 Juta*. Finance.Detik.Com. https://finance.detik.com/moneter/d-6538799/rangkaian-aksi-tukang-becak-tipu-teller-bca-kuras-rekening-rp-320-juta

Plato-Shinar, R. (2019). Law and Ethics: The Bank's Fiduciary Duty towards Retail Customers. *Research Handbook on Law and Ethics in Banking and Finance*, 214–236.

Puslitbang Hukum dan Peradilan Badan Litbang Diklat Kumdil Mahkamah Agung RI. (2013). *Makna "Sifat Melawan Hukum" dalam Perkara Pidana Korupsi (Kajian tentang Putusan Mahkamah Agung RI Tahun 2005-2011)*.

Setyo Wardani, A. (2023). *Pakar Sebut BSI Jadi Korban Ransomware, 1,5 TB Data Milik 15 Juta Nasabah Dicuri dan Hacker Minta Tebusan*. Liputan6.Com. https://www.liputan6.com/tekno/read/5285443/pakar-sebut-bsi-jadi-korban-ransomware-15-tb-data-milik-15-juta-nasabah-dicuri-dan-hacker-minta-tebusan

Shufti Pro. (2022). *New Account Fraud- A New Breed of Scams*. https://shuftipro.com/reports-whitepapers/new-account-fraud.pdf

Sjofjan, L. (2015). Prinsip Kehati-hatian (Prudential Banking Principle) Dalam Pembiayaan Syariah sebagai Upaya Menjaga Tingkat Kesehatan Bank Syariah. *Pakuan Law Review*, *1*(2), 1–44.

Stupp, C. (2019). *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*. Wsj.Com. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Thi Nguyen, T., Viet Hung Nguyen, Q., Tien Nguyen, D., Thanh Nguyen, D., Huynh-The,

T., Nahavandi, S., Tam Nguyen, T., Pham, Q.-V., & M. Nguyen, C. (2022). Deep Learning for Deepfakes Creation and Detection: A Survey. *Computer Vision and Image Understanding*, *223*(C). https://doi.org/10.1016/j.cviu.2022.103525

Thies, J., Zollhöfer, M., Stamminger, M., Theobalt, C., & Nießner, M. (2020). Face2Face: Real-time Face Capture and Reenactment of RGB Videos. *CVPR2016*, 96–104. https://doi.org/https://doi.org/10.48550/arXiv.2007.14808

Uddin Mahmud, B., & Sharmin, A. (2020). Deep Insights of Deepfake Technology: A Review. *DUJASE*, *5*(1 & 2), 13–23. https://doi.org/https://doi.org/10.48550/arXiv.2105.00192

Wijaya, K. (2021, April). Digital Banking VS Digital Bank. *Majalah Infobank Lppi*, *1*, 1–5. https://lppi.or.id/site/assets/files/1890/kw-serial_berbagi-digital_banking_vs_digital_bank.pdf