IJSSR
International Journal of Social Service and Research

Vol. 4, No. 9, September 2024
e-ISSN: 2807-8691 | *p*-ISSN: 2807-839X

LEGAL CONSIDERATIONS FOR THE USE OF TECHNOLOGY IN THE DIGITAL BANKING SECTOR

Fatika Redita Suryadarma
Universitas Sebelas Maret, Indonesia
*e-mail: fatikareditasuryadarma@gmail.com

Keywords

Digital banking, digital economy, Financial Services Authority (OJK), technology regulation, bank supervision

ABSTRACT

With the rapid development of the digital economy in Indonesia, the development of digital banking has a great opportunity to grow. The potential to meet customer needs and expectations for faster and more efficient banking services based on digital technology has made the image of digital banks more popular among the public, especially for young people. This study explores the effectiveness and completeness of regulations governing the use of technology in Indonesia's rapidly transforming digital banking sector, which is currently undergoing a transformation process. By evaluating the current regulatory framework, the study provides insights into potential gaps and areas where the regulations may need to be strengthened or updated to ensure the secure and efficient operation of digital bank services. The use of artificial intelligence (AI) in the banking sector contributes to the transformation to digital banking, especially in identifying fraudulent attempts, assisting in the process of surveillance, analysis, and evaluation of transactions, as well as improving the standards of credit scoring, customer service, and automation. This article provides an overview of considerations if Indonesia implements international standard regulations for the security of cyber systems for the smooth running of digitalbank services. This paper emphasizes the need to implement a collaboration-based approach by involving government, industry, academia, and civil society to strengthen global digital resilience and security. The application of DORA principles in Indonesia can help strengthen the digital infrastructure of banks in the country.

INTRODUCTION

The birth of the industrial revolution era has changed human cognitive behavior, lifestyle, and interpersonal dynamics. The industrial revolution, especially in the fourth period, certainly has a big impact on all human activities today. These impacts not only include technological changes, but also spread to the economy, social dynamics, and politics (Prasetyo & Sutopo, 2018). The terminology of industry 4.0 was born from the idea of the fourth industrial revolution, which was also conveyed by the European Parliamentary Research Service that the industrial revolution basically occurred four times (Davies, 2015). The industrial revolution is known to have first occurred in the United Kingdom in 1784, when steam engines and mechanization began to replace work done by humans. The second revolution occurred at the end of the 19th century. At that time, production machines driven by electrical energy began to be used for mass production activities. Then the third revolution began in 1970, where manufacturing automation began using computer technology. In today's era, the rapid development of sensor, interconnection, and data analysis technologies has given rise to the idea of combining these technologies in various industrial fields. This idea became the basis of the next revolution. The number four in the sentence Industrial Revolution 4.0 refers to the fourth revolution. Industry 4.0 was

announced theoretically, because the actual event has not yet happened and is still an idea (Drath & Horch, 2014).

The industrial revolution 4.0 is often referred to as a cyber physical system. This revolution focuses on automation and combines it with cyber technology. The characteristic that signifies this revolution is the incorporation of information and communication technology in the industrial field. The development of the industrial revolution has caused changes in various sectors. For example, if initially a factory needs enough workers to make a product, then by utilizing technology the workers can be replaced with machines (Purba et al., 2021). The term Industry 4.0 was officially born in Germany, precisely at the time of the Hannover Fair in 2011 (Kagermann et al., 2011). This is motivated by Germany's development plan policy entitled High-Tech Strategy 2020, where industry 4.0 is part of the policy. The purpose of the policy is to keep Germany at the forefront of manufacturing (Heng, 2015). Several other countries participate in realizing the concept of industry 4.0 with different terms, for example Industrial Internet of Things, Smart Factory, Smart Industry, and Advanced Manufacturing. Although they have different names, they all have the same goal, which is to increase the competitiveness of each country's industry in the face of a dynamic global market. This condition is influenced by the rapid development and use of digital technology around the world.

The potential and benefits born by the industrial revolution 4.0 include production flexibility, improved service to customers and increased revenue. The realization of these potential benefits is expected to have a positive impact on a country's economic sector (Prasetyo & Sutopo, 2018). The emergence of the fourth industrial revolution is marked by the integration of digital technology as an important asset for industry stakeholders to expand their business operations.

The digital economy in Indonesia is a rapidly growing sector and has great development potential. Collaboration between the government and the community can be a key component in encouraging digital transformation. The growth potential of the digital economy is supported by a large population, with 171.17 million internet users (64.8% of the total population) and 355 million mobile users (133% of the total population). According to estimates from Google, Temasek, and Bain & Company, the internet economy in Indonesia is projected to grow at a double-digit rate, and is estimated to reach a value of $124 billion by 2025 (Davis & Neves, 2021). The digital economy affects the lifestyle and behavior of people who are dominated by millennials and generation Z. Fulfilling needs that can be done through e-commerce platforms is increasing in line with the birth of digital payment innovations both through banks and through financial technology companies (Tobing et al., 2021). This is strengthened by the Covid-19 pandemic which has also accelerated the development of digital financial services. Most consumers are expected to maintain and increase the use of mobile banking and online banking post-pandemic.

Research conducted by Barquin et al. (2021) shows that digital banking transformation is happening rapidly. This is because people are interested in existing trends, such as the increasing use of digital wallets for various transactions, including banking, and the increased use of teleconferencing during the pandemic. It shows that around 80% of customers continue to maintain or increase their mobile banking and online banking activities after the Covid-19 pandemic.

The transformation of conventional services into digital services is considered the most beneficial for the younger generation. An open attitude towards the presence of technology and adaptive belonging to most of the young generation makes banking services such as ATMs, mobile banking, internet banking, and SMS banking considered commonplace. Nowadays, of course, people are starting to think about what if opening an account, saving, applying for credit or loans, and other banking services are carried out online without having to physically present themselves at the bank concerned. This potential is seen by the bank as an opportunity to increase the interest of prospective customers to become active customers, as well as provide the services that customers want so that they remain loyal to the bank (Kholis, 2020).

The term "digital bank" is increasingly known along with the emergence of new bank operators who claim to be digital banks by offering business and operational models based on digital technology. As if not wanting to lose customers, conventional banks, both public and private, are also competing to develop and introduce their digital banks to the wider community. This technological development is then considered a digital revolution in banking sector activities, because this sector has significantly changed the way banks operate and serve customers. The relatively fast transformation is evidenced by the emergence of banking transaction services that can be accessed through each customer's device, such as mobile banking and internet banking (Billiam et al., 2022). This view then has an impact on the

emergence of a public stigma that conventional banking procedures become quick to use and less attractive (Amudhan et al., 2020).

The potential to meet customer needs and expectations for faster and more efficient banking services based on digital technology has made the image of digital banks more popular among the public, especially for young people. This opportunity is even greater due to the influence of the Covid-19 pandemic which has played a role in changing the lifestyle of people who initially still used conventional banking services to users of digital bank services. Positive developments can be seen from the increase in public preference, adaptation, and acceptance of the use of digital financial platforms and instruments, such as e-commerce, to meet daily needs (Mawarni et al., 2021).

This study explores the effectiveness and completeness of regulations governing the use of technology in Indonesia's digital banking sector, which is undergoing rapid transformation. The research contribution of this study lies in its exploration of the effectiveness and completeness of regulations governing the use of technology in Indonesia's rapidly transforming digital banking sector. By evaluating the current regulatory framework, the study provides insights into potential gaps and areas where the regulations may need to be strengthened or updated to ensure the secure and efficient operation of digital banking services. This contributes to the ongoing discussion on how regulatory policies can keep pace with technological advancements and enhance the security and trustworthiness of digital banking.

METHODS

The type of research applied is normative legal research. In the context of normative research. This study provides an overview of considerations if Indonesia implements international standard regulations for the security of cyber systems for the smooth running of digital bank services which are currently undergoing a transformation process. In this study, primary and secondary legal materials were used. In this study, an approach was made to the Financial Services Authority Regulation Number 12/POJK.03/2021 concerning Commercial Banks, especially in Article 24 Paragraph (1) letter A.

RESULTS

The transformation from conventional banking to digital banking is basically the process of combining online banking and mobile banking services in one application platform that can be accessed via mobile phones. In line with this transition process, banks need human resources who have special expertise in data analysis, a broad understanding of bank risk mitigation and the use of technology, and are able to solve problems with a high degree of complexity (Winasis, S., Riyanto, S., & Ariyanto, 2020).

The first digital bank to operate in Indonesia is known to be Jenius, which is under the auspices of PT. Bank Tabungan Pensiunan Nasional Tbk (BTPN) in 2016. Jenius offers a variety of fully digital-based banking services, which allow customers to open accounts, save, apply for credit, and make various financial transactions through the mobile application without the need to visit a branch office. Offering features such as multifunctional debit cards, easy financial management, and integration with various other digital services, Jenius has managed to gain popularity among the younger generation who are relatively open to technology, as well as driving the transformation of digital banking in Indonesia. This innovation has provided convenience and comfort for customers in accessing banking services anytime and anywhere.

Since its launch, Jenius has continued to innovate to meet the needs of its customers. Through features such as Save It, Flexi Saver, Dream Saver, and Maxi Saver, customers can manage their savings more flexibly and according to their respective financial goals. Jenius also provides a Split Bill feature that makes it easier for customers to automatically split costs with their friends. In addition, Jenius Connect allows customers to connect their Jenius accounts with various digital services such as e-wallets and other online payment platforms, thus providing convenience in transactions in the digital era.

The terminology of digital banks is then described by the Financial Services Authority in POJK Number.12/POJK.03/2021 concerning Commercial Banks where a legal entity bank (Bank BHI) that operates as a digital bank is defined as a bank that provides and carries out its business activities through electronic channels without a physical office (branch) other than the head office. The services offered by digital banks include customers being able to open accounts, save, apply for credit, and use other banking services without the need to physically come to the bank. The operational aspects and requirements that must be met by conventional BHI Banks and those operating as Digital Banks have been initiated by the OJK in the Financial Services Authority Regulation (POJK) No. 12/POJK.03/2021

concerning Commercial Banks. This regulation aims to increase banking competitiveness, adaptability to technological innovation, and contribution to the national economy.

The electronic channel in Article 23 Paragraph (3) refers to the media used by BHI bank which operates as a digital bank to carry out its business activities, especially through digital technology which is mentioned that it does not require a physical office other than the head office. The meaning of electronic channels in this article refers to the use of various platforms for digital bank operations, such as internet banking, mobile banking, and other digital banking applications that allow customers to make transactions and access banking services electronically.

The development of the digital economy in the banking sector, which is currently improving, makes the Financial Services Authority must focus on playing an important role in the implementation of digital banks. The restrictions on people's mobility that occurred in 2020 made the digitalization of the banking sector must receive more attention from those who play the role of supervisors and regulators of the banking sector. A society that is now more adaptive to technology must also be shaded by harmonized legal protection.

Based on the perspective of banking law, the existence of digital banks requires strengthening regulations and policies. The rapid development of technology is difficult to regulate, of course, with a rule-based approach that tends to be rigid. In contrast, principle-based regulation makes it easier for banks to adapt to changes and the banking ecosystem. This principle-based approach allows banks to innovate while still paying attention to the prudential principle. Some of the aspects that require regulatory strengthening in digital banking transformation include: data, technology, risk management, collaboration, and institutional structure. The success of banks in transforming into Digital Banks is highly dependent on the ability to manage these aspects well.

The key elements that must be complied with for BHI banks operating as digital banks are contained in Article 24 Paragraphs (1) and (2) of POJK No. 12/POJK.03/2021. The key elements in the form of requirements that must be possessed by BHI banks operating as digital banks, one of which is stated in Article 24 Paragraph (1) letter (a) which states that digital banks must "have a business model with the use of innovative and safe technology in serving customer needs".

The use of the word "business model" in the article refers to the operational design and strategy used by banks to provide digital-based banking services as a whole. This includes various aspects such as market segmentation, organizational structure, products and services offered, and technologies used to support bank operations. A digital bank's business model can also include how the bank interacts with its customers, including through digital platforms such as mobile banking applications, as well as how the bank manages risk and complies with applicable regulations. At the core of this business model is the use of digital technology to improve operational efficiency, expand access to banking services, and provide a better customer experience. Digital banks are expected to have a clear and structured business model and be able to operate effectively, innovatively, and maintain compliance with regulatory standards set by the Financial Services Authority (OJK).

Looking at the circular of the Digital Blueprint for Banking Transformation published in 2021 by the OJK, the business model that was originally conventional-based can shift to a platform-based business model that is connected to the digital economy ecosystem by utilizing Application Programming Interface or API technology (OJK, 2021).

Business models that involve the use of digital technology can provide opportunities that have great positive value. The utilization of business model opportunities for a sector can help develop operational activities in it. In the banking and finance sector, digitalization as a tool for business model development can affect work culture and work environment so that it can create an effective and efficient work method (Samsuri, 2022). Business models that collaborate on the use of technology such as Artificial Intelligence (AI) or familiarly called artificial intelligence, big data analysis, blockchain, and API (Application Programming Interface) show that digital banking services prioritize efficiency and accessibility (Arner et al., 2015). Through digital platforms, customers can easily access remote banking products and increase financial inclusivity.

The business model in digital banking must be designed to collaborate with technology to provide effective and efficient services to customers. The innovation in question can include the use of digital platforms that allow various transactions to be carried out online without the need for physical interaction, which can increase the speed and convenience of services. In addition, digital banks are required to implement strict security systems to protect customer data and privacy, ensuring that sensitive information is not misused or stolen. Good risk management is also an important aspect,

including a strong risk mitigation strategy to deal with various cybersecurity threats. Thus, an innovative and secure business model not only improves operational efficiency but also builds customer trust in digital banking services.

The digital bank business model in accordance with Article 24 Paragraph 1 of the POJK must also reflect adaptation to technological developments and dynamic market needs. Digital banks need to use a flexible and responsive approach to change, such as the integration of artificial intelligence (AI) for customer data analysis, the use of blockchain for transaction security, and the application of big data analytics to understand and meet customer needs. In addition, digital banks must be able to offer inclusive banking services, reaching customers in remote areas that were previously not served by conventional banks. Sustainability aspects are also an important part of this business model, where digital banks are expected to not only focus on financial gains, but also contribute to sustainable and inclusive economic development. The digital bank's business model not only serves as an operational roadmap, but also as a commitment to provide sustainable added value for all stakeholders, including the banking sector, customers, and the wider community.

In the digital era, the sustainability aspect of the banking sector is becoming increasingly important to pay attention to. Rapid digital transformation has changed the way banks operate and interact with their customers. Sustainability in the banking sector includes several key elements, such as reducing carbon footprint, improving operational efficiency, and social responsibility. Banks are now turning to greener digital solutions, reducing the use of paper by using e-banking systems and digital documentation. Sustainability aspects in the banking sector include several things, including environmental aspects, social aspects, and governance aspects.

The importance of sustainability is also reflected in the bank's efforts to support green and sustainable projects. Through green financing and investments in renewable energy, banks play an important role in fostering a more sustainable economy. In addition, banks also play a role in educating customers on the importance of sustainable and responsible financial practices. As conveyed by the Vice President of Environmental, Social, and Government Division of PT. BRI Tbk., Yosephine Ajeng who explained that the sustainable economic aspect can be carried out through the following things. The first is the environmental aspect, the bank implements green banking policies, environmental risk management, carbon emission management, and eco-efficiency operations. Second, the social aspect, banks can carry out human capital management, human rights, financial inclusion, and social responsibility. Finally, in the aspect of governance, banks can apply product governance, corporate governance, business ethics, and cybersecurity and information security systems (Putih, 2022).

The economic aspect of sustainability, especially the banking sector in the era of digitalization, is not only about the use of new technology, but also about the commitment to create a positive impact on the environment and society. Banks must continue to innovate and adapt to technological changes while maintaining strong sustainability principles to ensure balanced and sustainable long-term growth.

There are several strategic steps that financial institutions can take to ensure the sustainability of the banking sector in the era of digitalization. First, banks must integrate ESG (Environmental, Social, and Governance) practices into their business strategies. Referring to a circular published by the State Savings Bank entitled Sustainable Growth of Green Indonesia, the purpose of implementing ESG practices for the banking sector is to set clear sustainability goals, report progress transparently, and create harmony between economic, social, and environmental aspects (Kemenkeu, 2023). Second, digital banks must routinely supervise and inspect the cybersecurity system. This is done with the consideration that with the increasing use of digital services by customers, the risk of cybercrime that may occur also increases. In addition to routine supervision and inspection, digital banks are also expected to continue to innovate in realizing the creation of an ideal scope related to guarantees for data privacy and security. Next is the development of skills regarding technology and things that support digital services for employees. Digital banks must accommodate human resource training and development to ensure that employees have the necessary skills to support evolving operational activities. This includes training on the use of new technologies, as well as providing an understanding of how they can be used to improve services and operational efficiency.

Fourth, products and services must continue to innovate. Digital banks must continue to study the potential of fintech to collaborate or invest in start-ups that offer innovative solutions. Digital banks must also continue to look for ways to improve the customer experience through technological innovations such as the use of AI to customize services, develop mobile applications that are easier to use, and apply blockchain technology for transparency and transaction efficiency. Finally, banks must

be active in the community and support social initiatives. This includes providing support to small and medium-sized enterprises (SMEs), participating in community-building projects, and promoting financial inclusion. Thus, banks can play a greater role in promoting inclusive and sustainable economic growth. It is hoped that by implementing these strategies, banks can ensure that they not only survive, but also thrive in the era of digitalization, while remaining committed to sustainability principles. Through a holistic and integrated approach, the banking sector can contribute significantly to sustainable development and the well-being of the wider community.

The use of AI in the banking sector contributes to the transformation to digital banking, especially in identifying fraudulent attempts, assisting in the process of surveillance, analysis, and evaluation of transactions, as well as improving the standards of credit scoring, customer service, and automation. The service that is expected to be more effective and efficient if utilizing AI is considered suitable for the banking sector (Mikalef et al., 2022). Currently, the use of AI carried out by the banking and finance sectors is widely used to improve the efficiency of back office processes. For example, the use of facial scanning to make transactions, the application of voice, face, and fingerprint biometric technology for authentication and authorization, and the use of machine learning technology to identify patterns of fraud and cyberattacks.

Production effectiveness through the use of AI is becoming a popular topic around the world. It is estimated that companies using AI will experience a 40% increase in production in 2023. Some countries have even implemented AI up to 56% in their industrial sectors (Ririh et al., 2020). In Indonesia, to implement AI effectively, the Agency for the Assessment and Application of Technology (BPPT) has issued the National Strategy for Artificial Intelligence Indonesia 2020-2045. However, this strategy is still in the form of a general policy guide and has not been regulated in detail. In fact, it is known that many companies in Indonesia have developed and applied AI technology in their production processes. Strategic sectors such as banking, e-commerce, and healthcare are some examples of sectors that have used AI.

The occurrence of massive changes due to the development of increasingly widespread technology, creating an era of inevitable disruption. Nowadays, the use of the role of technology in the form of the use of artificial intelligence bases that spread to various sectors, machine learning, the use of blockchain, biometrics, cloud computing, the internet of things (IoT), the use of augmented reality or virtual reality, and quantum computers have become normal in various fields sector.

Based on an article titled Digital Banking and The Future Legal Considerations written by Hammad & Al-Mehdar Law Firm (2022), the trend regarding banking digitalization has been intensively used by millennials and Generation Z since 2018. These two young age groups indirectly affect the development of digital banking by placing high expectations on more efficient digital banking services. The article mentions that currently there are several focuses that are challenges for digital banking in carrying out its operations. These challenges include a deeper focus on online security related to online banking operations, the move from conventional banking to digital banking, the emergence of digital banks without physical bank offices, the use of Application Programming Interface (API) to create open banking, the use of blockchain technology to help create security on digital transactions, The use of Artificial Intelligence (AI) and the Internet of Things (IoT) that offers new experiences to customers, and the emergence of the introduction of metaverse technology and the concept of digital banking using virtual reality. Challenges related to technology make it necessary for a country to face banking transformation in the digital era. On the other hand, innovations related to the use of technology in the banking sector present opportunities for the business sector, therefore, it is important to analyze these technological innovations in more detail to see what legal challenges a country may face in the next few years.

The characteristics of AI in information processing automation allow AI to be equated with "Electronic Agents" in Indonesia's laws and regulations. Article 1 of the ITE Law defines "Electronic Agent" as "a device of an electronic system that is made to perform an action on a certain Electronic Information automatically organized by a person." The word "automatic" in the definition of "Electronic Agent" was used as a basis by Pratidina (2017) to construct AI as an "Electronic Agent." If we follow this construction, the regulations regarding "Electronic Agents" also apply to AI.

The application of AI in various industrial sectors in Indonesia must not only consider technical and operational aspects, but also ensure compliance with applicable regulations. Understanding AI as an "Electronic Agent" provides a clear legal framework for the management and use of this technology, including in terms of responsibilities and liabilities that may arise. Additionally, companies that utilize

AI need to prepare adequate infrastructure and human resources to manage these technologies effectively and safely. Training and upskilling for employees is essential so that they are able to adapt to technological changes and ensure that the implementation of AI can provide maximum benefits.

Overall, recognizing AI as an "Electronic Agent" under Indonesia's legal framework is an important first step in ensuring that these technologies can be safely and efficiently integrated into various sectors, helping to drive innovation and sustainable economic growth (Asfahaliza & Anggraeni, 2022).

The position of artificial intelligence in Indonesia law is currently still in the stage of development and adjustment. In general, regulations regarding AI in Indonesia have not been specified in detail in the national legal framework. However, some existing regulations are beginning to accommodate the development of this technology, especially in the financial and banking sectors. For example, the Financial Services Authority (OJK) through POJK No. 12/POJK.03/2021 regulates the use of innovative technologies including AI in digital banking services.

Simply put, artificial intelligence can be categorized as something "innovative" as described in Article 24 Paragraph 1 of POJK Number 12/POJK.03/2021. The word "innovative" in the context of digital banking technology has a close relationship with the use of artificial intelligence (AI). In digital banking, AI is used to improve operational efficiency and provide a more personalized service experience to customers. AI technology allows banks to analyze customer data in depth and in real-time, which is then used to predict customer needs and provide recommendations for relevant products or services automatically.

The possibilities for technological innovation in the field of digital banking in Indonesia are vast and promising, driven by the rapid development of technology and the high use of digital media among the public. With the increasing number of tech-savvy young people and the increasing use of the internet, digital banking has a great opportunity to grow. Technological innovations such as artificial intelligence (AI), blockchain, Big Data Analytics, and the Internet of Things (IoT) can be integrated to create more efficient and secure banking services.

Regulations regarding financial sector innovation tests are published in POJK Number 3 of 2024 concerning the Implementation of Financial Sector Innovation. Where, in Article 1 Paragraph (3) it is stated that technological innovation in the financial sector, hereinafter abbreviated as ITSK, is a technology-based innovation that has an impact on products, activities, digital services, and business models in the digital financial ecosystem. The implementation of ITSK is intended to comply with the licensing provisions regulated by the Financial Services Authority. Supervision and testing of digital products related to banking is carried out with sanbox. According to Article 1 Paragraph (7) of the POJK, a sandbox is a means of testing or developing innovations and mechanisms provided by the OJK.

The trial through sanbox is a good step initiated by the OJK in its role as a financial sector supervisor. The regulatory sanbox initiated by the OJK aims to support innovation in the financial services sector by testing products, services, business models, and mechanisms in financial and banking services.

Behind all the convenience and efficiency offered by the use of AI, there is a domino effect that needs to be considered. The use of AI has negative impacts, such as increased cyber-crime risks, data leaks, and data manipulation. The lack of proper oversight and policies can lead to uncertainty in responsibility and accountability for decisions made by AI systems in the banking industry. This can reduce the level of customer trust in the security and privacy of their data, and potentially cause financial and reputational losses to the financial institutions involved. Therefore, careful and comprehensive regulation of the use of AI in the banking sector is essential to protect the interests of all parties involved.

Regulations on the use of AI in Indonesia are still in the development stage, with several initial steps already taken to regulate and guide the use of this technology. One of the important efforts is the publication of Indonesia's National Strategy for Artificial Intelligence 2020-2045 by the Agency for the Assessment and Application of Technology (BPPT), which serves as a general policy guide. However, specific regulations governing the use of AI in detail are still lacking. In the legal framework, AI can be categorized as "Electronic Agents" according to the ITE Law, which regulates electronic devices that perform actions automatically. However, more detailed rules are needed to address issues such as responsibility, accountability, data security, and privacy related to the use of AI. Governments and relevant institutions need to work together to develop comprehensive regulations, which include ethical standards, transparency, and strict supervision, so that the use of AI can be carried out safely, fairly, and provide maximum benefits to society and industry in Indonesia.

The use of innovative technologies in digital banking, such as APIs, blockchain, and artificial intelligence (AI), offers many opportunities to improve operational efficiency, expand access to services, and provide a more personalized experience for customers. However, this innovation also brings with it various legal challenges that must be faced. Legal considerations are very important to ensure that the application of the technology is not only safe but also in accordance with applicable regulations. For example, API technology allows for broader integration between banks and third-party service providers, but also opens up potential risks related to data leaks and customer privacy breaches. Regulations such as the Financial Services Authority (OJK) Regulation on Customer Data Protection and cybersecurity must be adapted to overcome this new challenge.

Additionally, blockchain implementations in banking transactions offer greater transparency and security, but they also require a clear legal framework to address issues such as the validity of smart contracts and law enforcement in a decentralized ecosystem. The application of artificial intelligence (AI) for data analysis and service personalization also raises questions about legal liability in the event of algorithmic errors or data biases that harm customers. Exploring the various legal aspects of the application of innovative technologies in digital banking, assessing the effectiveness of existing regulations, and identifying areas that require further attention to ensure that technological innovations can go hand in hand with consumer protection and legal compliance (Asfahaliza & Anggraeni, 2022).

Bank Indonesia (BI) and the Financial Services Authority (OJK) have a responsibility to limit and regulate the use of innovative technology in the banking sector to ensure the stability and security of the financial system. BI is responsible for maintaining monetary stability and the payment system, while the OJK supervises and regulates all financial services activities, including banking. The two agencies are working together to develop comprehensive regulations, which govern the use of innovative technologies to stay within a strict legal corridor. BI and OJK set security and data protection standards that must be complied with by banks that use innovative technology, to prevent the risk of data leaks and cyberattacks. In addition, they also ensure that the AI algorithms used in decision-making do not contain biases that can lead to discrimination against customers. Through rigorous audits and supervision, BI and OJK identify and address potential misuse of AI technology, including practices that can disrupt financial stability or harm customers. It is hoped that by establishing clear guidelines and regulations, BI and OJK will strive to facilitate innovation in the banking sector, while protecting the interests of customers and maintaining the integrity of Indonesia's financial system.

The Financial Services Authority or OJK is an institution that carries out the task of regulating and supervising financial services activities in the banking sector, capital market, and non-bank financial institutions including insurance, pension funds, financing institutions, and other financial services institutions (Heriyadi, 2023). The role and function of the OJK can be seen based on the authority of the OJK which consists of the regulation and supervision of financial institutions, both banks and non-banks (Arno & Assad, 2017). As for its function as a banking supervisor and regulator, the OJK is authorized to grant permits for the establishment of a bank, permits for opening bank branches, supervision of the articles of association, work plans, human resource management, and revocation of business licenses. In addition, OJK is also authorized to regulate and supervise all types of activities contained in banking which include sources of financing, provision of funds, and bank activities in the service sector. The OJK is also authorized to regulate and supervise aspects related to the health and prudence aspects of banks.

The use of innovative technologies in banking, such as APIs, blockchain, and artificial intelligence (AI), brings with it significant responsibilities and risks for financial institutions. The main responsibility of banks in this context is to ensure that the technology used is in accordance with applicable regulations, especially those related to data protection and customer privacy. Banks must implement strict security measures to prevent data leaks and cyberattacks, which can harm customers and damage the bank's reputation. For example, the implementation of API technology requires strict access controls and data encryption to protect sensitive information.

Other risks involve potential errors or biases in AI algorithms used for data analysis and credit decisions, which could result in discrimination or unfair decisions for certain customers. In addition, the use of blockchain technology, while offering high security, also faces legal challenges regarding the validity of smart contracts and enforcement mechanisms in a decentralized environment (Asfahaliza & Anggraeni, 2022). Banks must be prepared to address these legal and operational issues by developing comprehensive internal policies, staff training, and close collaboration with regulators to ensure that technological innovations can be implemented safely and efficiently.

The protection of customer personal data has a major impact on the development of digital banking services. This security is key in building online trust, which is essential for digital transactions. Customer personal data is vital because customers will not want to transact digitally if they feel that their personal data is not secure. One aspect of this data protection is how customer data is processed, including sensitive data that, if it falls into the hands of irresponsible parties, can cause financial losses for customers. The threat arising from the weak protection of customer personal data is directly correlated with the development of digital banking services. An example of a regulation that is critical of personal data protection is the European Union General Data Protection Regulation (EU GDPR). The purpose of these regulations is to protect data privacy in today's digital economy, by giving individuals greater control over their data and establishing stricter rules for entities that manage or store such data. This regulation applies not only to companies in the European Union, but also to all global companies that store personal data of EU citizens. This rule later became a model for data protection laws outside the European Union.

The General Data Protection Regulation (GDPR) is a personal data protection regulation implemented in the European Union and has a global impact, including on the digital banking sector. The implementation of GDPR in Indonesia in the context of digital banking can be adapted by paying attention to several important points.

1. User Consent, which means that any data collection must be based on the explicit consent of the user. In its implementation in Indonesia, this means that digital banks must ensure that the consent given by customers for the use of their data is explicit and well-documented. A concrete example is through a clear and informative consent form on a banking application or website.
2. Transparency and Access Rights, which means users have the right to know how their data is used and have access to it. In Indonesia, digital banks must provide transparent information about the purpose of data collection and provide customers with access to view, update, or delete their personal data if necessary. This can be implemented through an easily accessible and fully functional user dashboard.
3. Data Protection by Design and by Default. This concept requires that systems and processes involving personal data are designed with data protection in mind from the outset. Digital banks in Indonesia can apply this principle by ensuring that security and privacy features are integrated from the early stages of developing their products and services.
4. Notification in the event of data misuse. In the event of a data breach, banks must notify the authorities and affected customers within a certain time. Deployment in Indonesia requires clear and expedited procedures for reporting security incidents, including the appointment of an incident response team that is ready to handle data breaches immediately.
5. Appointment of a Data Protection Officer (DPO): Digital banks that handle personal data on a large scale are required to appoint a Data Protection Officer. In Indonesia, this position must be filled by individuals who have expertise in data protection and information security, tasked with ensuring compliance with data protection regulations.
6. The Right to Be Forgotten. Users have the right to request the deletion of their personal data if it is no longer necessary for the original purpose for which it was collected. Digital banks in Indonesia must set up mechanisms to meet these data deletion requests, as well as ensure that data is completely deleted from all systems.

It is hoped that by implementing GDPR principles, digital banking in Indonesia can improve customer data protection and strengthen public trust in their services. Strong personal data protection not only protects customers, but also provides a competitive advantage for digital banks that prioritize security and privacy in their operations.

European companies operating in Indonesia comply with the EU GDPR rules because the regulation also covers the activities of European companies outside the EU territory. However, many local companies in Indonesia have not adopted personal data protection policies in their internal policies (Reynaldi & Tifana, 2020). The absence of a legal umbrella regulating personal data protection is the main reason why local companies have not followed data protection rules. In the context of the banking industry going forward, with the increasing push for the integration of digital banking services in the digital economy system, the implementation of international regulations on the protection of personal data for banking consumers is important. The existence of rules that can protect bank

consumers and regulate how banks collect, process, and exchange consumer data is expected to increase consumer confidence in using digital banking services.

On the other hand, the absence of regulations governing data protection will pose a threat to privacy and personal data management, such as data leaks. The threat of data leaks is increasing in line with the rapid development of the digital economy in Indonesia. On the other hand, the personal data protection law (Law No. 27 of 2022 concerning Personal Data Protection) is also relevant to the use of AI, considering that this technology often involves extensive processing of personal data. These regulations aim to protect individual privacy and ensure that data managed by AI systems is used ethically and responsibly. In addition, the Indonesia government has also shown its commitment to developing the AI ecosystem through initiatives such as the national AI roadmap, which is expected to provide guidance for the development and implementation of AI in various sectors.

The threat of data leakage is certainly the biggest challenge in the banking sector. This is because banks manage millions of customer data needed for various banking transactions. Customers have no other choice but to entrust their personal data to the bank. Therefore, banks must maintain this trust by preventing data leaks. Leakage of customer data can cause financial losses for customers and harm the bank, both financially and reputationally. This leak can occur due to a hack of the bank system or deliberate actions such as the sale of data by bank employees. The large volume of data managed by banks must be balanced with efforts to strengthen data security so that it is not easily hacked. The management of customer data must also be accompanied by good data management and governance to avoid misuse by bank employees.

To ensure compliance and security in the use of innovative technology in banking, the Financial Services Authority (OJK) in Indonesia must adopt several comprehensive strategies. First, OJK needs to continuously update regulations to address new challenges, focusing on data protection, cybersecurity, and financial system integrity. Second, it should enhance supervision through regular audits and inspections of digital bank operations to ensure compliance, utilizing technology to detect cyber threats in real-time. Third, OJK can provide guidelines and training for financial institutions, offering a framework for security and compliance, alongside workshops to raise awareness about risks and mitigation strategies. Additionally, OJK should ensure banks implement technology that supports interoperability, using APIs like the Open Bank Project and frameworks such as Spring for secure and integrated digital services.

Uniform use of APIs and open source frameworks across Indonesia's banks can help improve the interoperability, efficiency, and security of the digital banking system. With this standardization, banks can ensure that all their systems and applications can communicate smoothly, reduce development costs, and improve the speed and security of services provided to customers.

The formulation of the concept of regulation regarding protection against cyber-attacks must consider several things to ensure the security, privacy, and integrity of cyber-related systems. These things to consider include:

1) Government Cooperation: The formulation of regulations on protection against cyberattacks to harmonize the use of technology in various sectors must cover all aspects, including data protection, network security, and responsive response in the event of an attack. To address these challenges, collaborative efforts involving various stakeholders, including governments, the private sector, and civil society, are needed. Knowledge exchange, training, and capacity building must be enhanced to ensure that all countries have adequate capabilities to deal with cybercrime (Ariyaningsih et al., 2023). Collaboration between the government and cyber security protection service providers can be the main foundation in forming an integrated data protection system. This collaboration concept can be the initial focus in designing advanced regulations regarding data protection and network security.
2) Regular Updates on Cyber Security Regulations: Regulations must be flexible in order to adapt quickly to technological advances and changes in cyber threats. It is important to have a mechanism for evaluating and updating regulations regularly to keep them relevant and effective. The application of international standards and best practices also needs to be considered in Indonesia, to ensure that domestic regulations are in line with global norms. This opens up opportunities for international cooperation in dealing with cross-border cyber threats. Regulations must establish a clear and unambiguous legal framework regarding definitions, responsibilities, and sanctions related to cybersecurity breaches. This includes

cybercrimes such as hacking, malware, data theft, and DDoS (distributed denial-of-service) attacks.

3) Strengthening Cyber Security in the Financial, Trade, and Industrial Sectors: Regulations must safeguard core infrastructure, including the industrial, trade, and financial sectors, from cyberattacks by enforcing strict safety standards and sector-specific cybersecurity protocols. Regular risk assessments and security trials are essential to maintain effective protection against evolving threats. Governments should foster collaboration between public and private sectors by sharing cyber threat information and requiring transparent reporting of incidents for timely response. Adopting international standards like ISO/IEC 27001 and the NIST Cybersecurity Framework can enhance Indonesia's protection of key infrastructure and promote global cooperation. Additionally, regulations should support cybersecurity education and training for workers and the public to increase awareness and preparedness. A comprehensive, collaborative regulatory approach can ensure critical sectors like finance, health, and energy remain secure in the digital age.
4) International Cooperation: The concept of effective regulation must certainly encourage the formation of international cooperation in information sharing, investigation, and law enforcement because cyberattacks often occur around the world. International cooperation is the key to overcoming these challenges. Countries need to collaborate more closely through bilateral and multilateral agreements, as well as actively participate in international organizations focused on cybersecurity (Najwa, 2024). Capacity building should also be a priority, with international initiatives aimed at improving technological and human resource capabilities in developing countries. In addition, harmonization of laws and regulations in different countries can help create more uniform standards, facilitating coordination and enforcement across borders (Pangestika et al., 2024).

The Budapest Convention on Cybercrime is one example of an international initiative related to the issue of cybercrime. Ratified in 2001 by the Council of Europe, the Budapest Convention establishes a comprehensive strategic framework for dealing with various types of cybercrime, such as device misuse, data breach attempts, and illegal access to computer systems. States participating in the convention are required to ratify national legislation in accordance with these provisions and cooperate closely with other countries in terms of the investigation and prosecution of cybercrime. In this regard, cooperation between countries includes legal assistance and the establishment of joint investigative teams to handle complex cases that span multiple jurisdictions. The Budapest Convention also helps countries build capacity and expertise to prevent, prevent, and respond to cyber threats. This can be achieved through international trainings, workshops, and conferences facilitated by cybersecurity agencies such as INTERPOL and Europol.

Cyberattacks can occur anywhere in the world and often involve criminal networks operating in different countries. Therefore, international cooperation is very important. Countries that have not yet ratified the Budapest Convention, including Indonesia, can consider this concept to form regulations that accommodate international cooperation to address cyber threats and protect their vital infrastructure from cyberattacks.

An article published by Chernenko et al. (2022) highlights several key points about how important international cooperation is in tackling and dealing with cyberattacks. In this article, recommendations for dealing with cybercrime such as the application of existing cyber norms, and the development of new international agreements to deal with cybercrime are also written. In addition, this article emphasizes the need to implement a collaboration-based approach by involving government, industry, academia, and civil society to strengthen global digital resilience and security. The Budapest Convention is cited as an effective model of cooperation in harmonizing national laws and facilitating international law enforcement against cybercrime.

The form of international cooperation efforts has been realized by the holding of the Budapest Convention. The Budapest Convention, also known as the convention on cybercrime, is the first international treaty that aims to harmonize national laws related to cybercrime, increase cooperation among countries in law enforcement, and establish effective investigative procedures. The convention was ratified by the European Council in 2001.

The Budapest Convention on Cybercrime is the most comprehensive and widely recognized international legal framework in the fight against cybercrime. The Convention provides guidelines for countries in shaping appropriate domestic legislation, as well as establishes mechanisms for

international cooperation in terms of law enforcement (Muchamad, 2023). The convention deals with various forms of cybercrime such as illegal access to computer systems, attempted data theft, and software misuse. States that have ratified the convention are required to update their laws in accordance with the provisions of the convention, as well as collaborate in cross-border investigations, share information, and provide mutual legal assistance. The Budapest Convention also encourages the rapid reporting of cyber incidents and security vulnerabilities to prevent further spread of threats. The convention has been ratified by more than 65 countries. This makes the Budapest Convention a global standard for handling and enforcing cybercrime laws.

There are several international agreements that can be used for the development of digital banks in Indonesia that have not been ratified by the country. One of them is the Digital Economy Partnership Agreement (DEPA). DEPA is an agreement between Singapore, Chile, and New Zealand, which covers various important aspects of the digital economy, including artificial intelligence, digital inclusion, and data protection. DEPA is designed to regulate and encourage technological innovation in the financial sector and can serve as a reference for the development of legislation in Indonesia (Natalegawa & Poling, 2022).

According to an excerpt from the official website of EIOPA (European Insurance and Occupation Pensions Authority), the Digital Operational Resilience Act (DORA) from the European Union is also an important regulation that can be used as a reference. DORA focuses on strengthening IT security for financial entities such as banks, and ensuring high digital operational resilience. DORA includes IT risk management, third-party service provider oversight, and comprehensive digital resilience testing. The application of DORA principles in Indonesia can help strengthen the digital infrastructure of banks in the country.

The aspects regulated in this international agreement that have not been regulated in depth in Indonesia include:

1) IT Risk Management and Third-Party Monitoring Assistance: The Digital Operational Resilience Act (DORA) from the European Union requires a comprehensive framework for risk management, especially in the IT sector. Banks must identify, manage, and mitigate risks associated with information technology, including risks from third-party service providers they use. This includes procedures for continuous risk evaluation and monitoring of IT systems and third-party services, ensuring that third-party service providers adhere to strict security standards. In practice, banks in Europe implement IT risk management systems by using a software to help perform the function of monitoring bank operations, evaluating performance and controlling IT systems and third-party services. The bank also regularly audits third-party service providers to ensure they comply with established security standards.
2) Use of Artificial Intelligence: The Digital Economy Partnership Agreement or DEPA includes a module on artificial intelligence and digital inclusion that aims to ensure that technological innovation is accessible to all levels of society. This includes the development and application of AI technologies that can help provide better and more inclusive financial services, as well as initiatives to ensure that digital technologies are available to all levels of society, including those in remote areas. Digital banks can use AI to offer financial products that are accommodated based on customer data analysis, thereby increasing the accessibility and relevance of financial services. DEPA also launched a digital literacy program to help people understand and use digital banking technology. Without digital inclusion and the implementation of AI, many communities may fall behind technological developments, resulting in a gap in access to financial services. This can hinder inclusive economic growth and widen social inequality.

Nevertheless, the implementation of international legal principles is inseparable from various challenges. One of the biggest challenges is the capacity gap between developed and developing countries (Hastri, 2021). Developing countries often do not have adequate technological infrastructure and human resources to deal with cybercrime effectively. Developing countries tend to need more assistance in the form of technology and training to build strong cyber law enforcement capacity. In addition, differences in legal and regulatory systems between countries add complexity to international law enforcement coordination (Jubhari, 2022). Actions that are considered a crime in one country may not be recognized as an offense in another, thus hindering cooperation efforts.

The application of international legal principles in law enforcement against cybercrime and cyberattacks is crucial but complex. Principles such as sovereignty, non-intervention, and international cooperation must be applied effectively to address the challenges arising from the transnational nature of cybercrime. The Budapest Convention on Cybercrime serves as an important framework, although capacity gaps and regulatory differences between countries remain major obstacles. Closer international collaboration, technological capacity building, and active participation of the private sector are urgently needed to improve the effectiveness of cyber law enforcement (Pangestika et al., 2024).

As a consideration, Indonesia can accede to international agreements that accommodate the handling of cross-border cybercrime. Indonesia has the ability to accede to international treaties aimed at handling cross-border cybercrime, although it was not involved in the initial signing of the agreement. Through accession, Indonesia can formally join and bind itself to the terms of the treaty, which opens up opportunities for closer cooperation with other countries in the fight against cybercrime. Participation in this agreement will not only strengthen national capacity in dealing with cyber threats, but also clarify Indonesia's commitment to international collaborative efforts. Thus, Indonesia can significantly contribute to global efforts in tackling cybercrime, while improving national cybersecurity to face evolving challenges.

In the future, it is hoped that by implementing these measures, Indonesia can create a strong, secure, and inclusive digital banking ecosystem. This will certainly help make Indonesia a barometer of digital banking, create sustainable innovation, and provide broad economic benefits for the entire community. Mature and collaborative implementation will ensure that digital banking in Indonesia not only develops but also has a significant positive impact on the national economy.

CONCLUSION

The transition to digital banking has brought new challenges, including the need for legal considerations to ensure customer data security and maintain trust. The Indonesian government's rules for digital service trials, initiated by the OJK in POJK Number 3 of 2024, do not fully accommodate technological innovation limits for digital bank business models, raising questions about the credibility and professionalism of the OJK. Additionally, Indonesia's regulations do not accommodate international agreements that allow cooperation between countries, potentially exposing it to cybercrime if perpetrators are outside the country's territory. Future research could explore the integration of international agreements and cross-border collaboration in regulating digital banking systems to address cybercrime. This could involve examining how Indonesia can participate in or accede to international agreements that facilitate cooperation in managing cross-border cyber threats. The effectiveness of current Indonesian regulations in accommodating international cybersecurity standards could also be assessed. Proposing regulatory frameworks that align with global best practices for digital banking, particularly in mitigating cybercrime from outside national borders is also suggested.

REFERENCES

Amudhan, S., Banerjee, S., & Poornima, J. (2020). IMPACT OF DIGITAL TRANSFORMATION OF BANKING SECTOR IN RURAL AREAS. In *Journal of Positive School Psychology* (Vol. 2022, Issue 2).

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. surya, & Rezi. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi Di Indonesia. *Jurnal Ilmu Hukum Universitas Pasundan*, *1*(1).

Arner, D. W., Barberis, J. N., & Buckley, R. P. (2015). The Evolution of Fintech: A New Post-Crisis Paradigm? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2676553

Arno, A. K., & Assad, A. Z. (2017). PERAN OTORITAS JASA KEUANGAN DALAM MENGAWASI RESIKO PEMBIAYAAN DALAM INVESTASI "BODONG." *Al-Amwal : Journal of Islamic Economic Law*, *2*(1). https://doi.org/10.24256/alw.v2i1.602

Asfahaliza, A. N. P., & Anggraeni, P. W. (2022). Pengaruh Penerapan Green Banking Terhadap Profitabilitas Perbankan Di Indonesia Periode 2016-2021. *Contemporary Studies in Economic*, *1*(2).

Barquin, S., Buntoro, E., Vinayak, H. V., & Pricillia, I. (2021). *Emerging Markets Leap Forward in Digital Banking Innovation and Adoption*. McKinsey.

Billiam, B., Abubakar, L., & Handayani, T. (2022). The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for

the Advancement of Indonesian Banking. *Padjadjaran Jurnal Ilmu Hukum*, *9*(1). https://doi.org/10.22304/pjih.v9n1.a4

Chernenko, E., Demidov, O., & Lukyanov, F. (2022). *Increasing Iinternational Cooperation in Cybersecurity and Adapting Cyber Norms*. Council on Foreign Relations.

Davies, R. (2015). Industry 4.0. Digitalisation for productivity and growth. *European Parliamentary Research Service*, *September*.

Davis, S., & Neves, N. C. (2021). Roaring 20s: The SEA Digital Decade. In *e-Conomy SEA 2021* (Issue November).

Drath, R., & Horch, A. (2014). Industrie 4.0: Hit or hype? [Industry Forum]. *IEEE Industrial Electronics Magazine*, *8*(2). https://doi.org/10.1109/MIE.2014.2312079

Hammad & Al-Mehdar Law Firm. (2022). *Digital Banking & The Future Legal Considerations*. Hammad & Al-Mehdar Law Firm.

Hastri, E. D. (2021). Cyber Espionage Sebagai Ancaman Terhadap Pertahanan Dan Keamanan Negara Indonesia. *Law & Justice Review Journal*, *1*(1). https://doi.org/10.11594/lrjj.01.01.03

Heng, S. (2015). Industry 4.0: Upgrading of Germany's industrial capabilities on the horizon. Deutsche Bank Research. *Baden-Wuerttemberg Cooperative State University*.

Heriyadi, H. (2023). TINJAUAN YURIDIS PERAN DAN FUNGSI OTORITAS JASA KEUANGAN (OJK) DALAM SISTEM KEUANGAN DI INDONESIA. *Jurnal Hukum Progresif*, *11*(1). https://doi.org/10.14710/jhp.11.1.36-44

Jubhari, A. R. (2022). *Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus Ransomware WannaCry di Indonesia* [Doctoral Dissertation]. Universitas Hasanuddin.

Kagermann, H., Lukas, W.-D., & Wahlster, W. (2011). Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution. *VDI Nachrichten*, *13*.

Kemenkeu. (2023). *Laporan Berkelanjutan Bank Tabungan Negara: Tumbuh Berkelanjutan Indonesia Hijau*.

Kholis, N. (2020). PERBANKAN DALAM ERA BARU DIGITAL. *Economicus*, *12*(1). https://doi.org/10.47860/economicus.v12i1.149

Mawarni, R., Fasa, M. I., & Suharto. (2021). Optimalisasi Kinerja Digital Banking Bank Syariah di Masa Pandemi Covid-19. *Jurnal Manajemen Dan Bisnis (JMB)*, *34*(1).

Mikalef, P., Lemmer, K., Schaefer, C., Ylinen, M., Fjørtoft, S. O., Torvatn, H. Y., Gupta, M., & Niehaves, B. (2022). Enabling AI capabilities in government agencies: A study of determinants for European municipalities. *Government Information Quarterly*, *39*(4). https://doi.org/10.1016/j.giq.2021.101596

Muchamad, M. K. (2023). *Kejahatan Siber Ancaman dan Permasalahannya: Tinjauan Yuridis pada Upaya Pencegahan dan Pemberantasannya di Indonesia*. Syiah Kuala University Press.

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum*, *2*(1).

Natalegawa, A., & Poling, G. B. (2022). The Indo-Pacific Economic Framework and Digital Trade in Southeast Asia. In *Center for Strategic and International Studies (CSIS)* (Issue 2022). Center for Strategic and International Studies (CSIS).

OJK. (2021). *Cetak Biru Transformasi Digital Perbankan*. OJK.

Pangestika, E. Q., Suningrat, N., Herwantono, H., Andriyani, W., & Rahardian, R. L. (2024). Penerapan Prinsip Hukum Internasional dalam Penegakan Hukum Terhadap Kejahatan Siber dan Serangan Siber. *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, *7*(2).

Prasetyo, H., & Sutopo, W. (2018). INDUSTRI 4.0: TELAAH KLASIFIKASI ASPEK DAN ARAH PERKEMBANGAN RISET. *J@ti Undip : Jurnal Teknik Industri*, *13*(1). https://doi.org/10.14710/jati.13.1.17-26

Pratidina, I. G. (2017). *Keabsahan Perjanjian Melalui Agen Elektronik dalam Sistem Hukum Kontrak di Indonesia* [Master Thesis]. Universitas Airlangga.

Purba, N., Yahya, M., & Nurbaiti. (2021). Revolusi Industri 4.0 : Peran Teknologi Dalam Eksistensi Penguasaan Bisnis Dan Implementasinya. *Jurnal Perilaku Dan Strategi Bisnis*, *9*(2).

Putih, Y. A. S. (2022). Talkshow Profesi Keuangan Expo. In *PPPK Kemenkeu*. PPPK Kemenkeu.

Reynaldi, F., & Tifana, N. (2020). *Urgensi Perlindungan Data Pribadi dalam Menjamin Hak Privasi: Sebuah Telaah RUU Perlindungan Data Pribadi*. Universitas Padjajaran Press.

Ririh, K. R., Laili, N., Wicaksono, A., & Tsurayya, S. (2020). STUDI KOMPARASI DAN ANALISIS SWOT PADA IMPLEMENTASI KECERDASAN BUATAN (ARTIFICIAL INTELLIGENCE) DI INDONESIA. *Jurnal Teknik Industri*, *15*(2).

Samsuri. (2022). Strategi Keunggulan Bersaing Melalui Digitalisasi Layanan Produk Pada Bank Syariah Indonesia KCP Rogojampi. *Ribhuna: Jurnal Keuangan Dan Perbankan Syariah*, *1*(1).

Tobing, G. J., Abubakar, L., & Handayani, T. (2021). Analisis Peraturan Penggunaan QRIS Sebagai Kanal Pembayaran Pada Praktik UMKM Dalam Rangka Mendorong Perkembangan Ekonomi Digital. *Acta Comitas*, *6*(03). https://doi.org/10.24843/ac.2021.v06.i03.p3

Winasis, S., Riyanto, S., & Ariyanto, E. (2020). Digital Transformation in Indonesian Banking Industry: Impact on Employee Engagement. International Journal of Innovation, Creativity and Change. *International Journal of Innovation, Creativity and Change*, *12*(4).