Governance Transformation: Juridical Analysis of Account Number Buying and Selling Practices

Musa Darwin Pane[1*]
Law Study Program, Faculty of Law
Universitas Komputer Indonesia, Jalan Dipati Ukur 102-106, Bandung, INDONESIA
musa@email.unikom.ac.id

Diah Pudjiastuti[2]
Criminal Justice Studies Program
International Women University, Jalan Pasirkaliki 179A, Bandung
INDONESIA
diahpudjiastuti@iwu.ac.id

ABSTRACT

The buying and selling of accounts—especially bank accounts—has grown to be a major problem as digital transactions become more commonplace. Nonetheless, the legal structure presents difficulties for law enforcement because it is unclear how account trading is regulated, notably with relation to Indonesia's Information and Electronic Transactions Law (ITE Law). The purpose of this research is to evaluate the efficacy of current legal frameworks, explore the difficulties and consequences of account trading in the context of the digital economy, and make suggestions for reforming governance. This study, which takes a normative juridical approach, uses legal texts and literature reviews as secondary data sources. Research questions are addressed through qualitative analysis, with an emphasis on the creation and application of account trading policies. The study finds that the ITE Law has ambiguities about account trading that could jeopardize the security of personal data and impede law enforcement actions. To properly address these issues, governance change is necessary, necessitating updated legal frameworks, improved institutional capabilities, stakeholder collaboration, and public education. In order to tackle the intricacies of account trading, it is imperative to improve rules, bolster law enforcement capacities, foster public consciousness, and fortify stakeholder participation. Efforts should also be directed toward strengthening law enforcement and monitoring systems and protecting personal data.

Keywords: Account trading, digital economy, governance transformation, legal certainty, law enforcement.

© The Author(s) 2024
L. Warlina and S. Luckyardi (eds.), *Proceedings of the International Conference on Business, Economics, Social Sciences, and Humanities - Humanities and Social Sciences Track (ICOBEST-HSS 2024)*, Advances in Social Science, Education and Humanities Research 854,
https://doi.org/10.2991/978-2-38476-269-9_7

1. INTRODUCTION

As society and technology advance, people are increasingly reliant on digital tools, including for communication. Nearly all global economic activities, particularly in Indonesia, utilize the internet and electronic systems. Among these activities is online transactions, commonly referred to as e-commerce.(Ranto, 2019)

Technological advancements have spurred rapid business expansion, enabling the exchange of information across long distances and facilitating transactions without the need for physical meetings, relying instead on computers and telecommunications equipment. This development in information technology is reshaping global society, transcending territorial limitations. The internet and information technology, innovations of the past decade, have profoundly impacted human life, revolutionizing various activities by offering efficiency, effectiveness, and mobility. However, the misuse or improper use of these technological advances also introduces new challenges and issues.(Hanim, 2011)

Various online scams, employing diverse tactics to trap victims, illustrate this phenomenon. Criminals often employ specific bank accounts as a tool to persuade potential victims, typically avoiding the use of personal accounts. CNBC discovered the sale of such accounts on the Tokopedia e-commerce platform through a search for "bank account".(Yuni Astutik & Rahajeng Kusumo Hastuti, 2020)

The buying and selling of bank accounts is openly conducted on social media platforms such as Facebook, Tokopedia, Shopee, and others.(Tim Kompas, 2023) The transactions within this industry entail a legal association between the involved parties. Such a legal association, stemming from an agreement, entails rights and obligations for the parties involved.(Pridbadi, 2021)

Trading account numbers belonging to others is akin to selling personal data, carrying inherent risks related to banking. In the hands of unscrupulous individuals, such data can be exploited for illicit purposes like online gambling or money laundering. For instance, a perpetrator might use someone else's ID card to create an account number, later utilizing it to facilitate criminal activities. Ironically, the unwitting owner of the account number may find themselves reported to the authorities for fraud. Moreover, even if the data owner is aware of the account number sale and receives money from it, they may be unaware of its criminal use, posing challenges for law enforcement in applying relevant statutes, especially in cases involving technology-mediated transactions.

The prevalent occurrence of account number sales indicates a considerable demand for such services within the market. Several factors contribute to this phenomenon, including the desire for privacy, deception, the demand for disguised identities, and financial motives. However, it's crucial to recognize that selling account numbers without the owner's consent is unlawful and can lead to severe repercussions. In response, governmental and law enforcement bodies must take action to address this phenomenon and safeguard the public from potential fraud and deceit.

In essence, law comprises norms and sanctions designed to govern human conduct. From this perspective, the primary role of law is to oversee human behavior, delineating permissible actions and prohibiting others. In Indonesia, the legal framework governing advancements in information technology is delineated in Law Number 11 of 2008 concerning Information and Electronic Transactions, with its implementation specified in Government Regulation Number 82 of 2012 regarding the Implementation of Electronic Systems and Transactions. These legislative instruments serve as key pillars for addressing

issues within the realm of information technology, including those arising in online transactions for electronic goods. Additionally, as per Article 1 Paragraph 2 of the ITE Law, electronic transactions are defined as legal acts conducted using computers, computer networks, and/or other electronic media.(Maryanto, 2021)

The concept of online buying and selling refers to a transactional process where the interaction between the seller and buyer occurs remotely, without the need for physical meetings. Communication between the parties involved can take place through various channels such as chat, telephone, SMS, WhatsApp, and other similar means. As described by W. Purwo and Anang Arief Wahyudi, this form of commerce is commonly referred to as e-commerce. E-commerce encompasses a dynamic array of technologies, applications, and business procedures that facilitate connections between businesses, consumers, and specific communities via electronic transactions, involving trade in services and information conducted through electronic platforms. Another interpretation characterizes e-commerce as the buying, selling, and exchange of goods and services facilitated by electronic systems. This entails electronic funds transfers, data exchange, and automatic inventory management, among other functionalities.(Pratama, 2020)

From this standpoint, the primary concern revolves around two key issues. Firstly, the connection between the regulatory framework governing the buying and selling of accounts as outlined in Law Number 1 of 2024, which amends Law Number 11 of 2008 concerning Information and Electronic Transactions, and the establishment of legal certainty. Secondly, the linkage between the implementation policies concerning individuals involved in buying and selling accounts, as stipulated in Law Number 1 of 2024, and the assurance of legal certainty.

In light of the challenges and opportunities presented by technological advancements, a governance transformation is essential. Governance transformation involves the evolution of policies, regulations, and institutional frameworks to effectively manage and oversee the digital landscape. This transformation is critical to address the new issues arising from the digital age, such as online scams, privacy concerns, and cybercrime. In Indonesia, this entails not only updating existing laws but also ensuring their implementation aligns with the dynamic nature of technology and e-commerce.

Governance transformation aims to create a regulatory environment that fosters innovation while protecting public interests. This involves enhancing legal frameworks like the Information and Electronic Transactions Law (ITE Law) to cover emerging threats and ensure robust enforcement mechanisms. Additionally, it requires the development of policies that promote digital literacy and cybersecurity awareness among the public to mitigate risks associated with online activities.

Effective governance transformation also relies on collaboration between various stakeholders, including government bodies, law enforcement agencies, private sector entities, and civil society. This collaborative approach ensures that diverse perspectives are considered in policy-making, leading to more comprehensive and effective regulations. Moreover, it facilitates the establishment of mechanisms for monitoring and evaluating the impact of these policies, allowing for continuous improvement and adaptation to new technological trends.

Ultimately, governance transformation is about creating a resilient and adaptive legal and regulatory system that can keep pace with the rapid evolution of technology. It aims to balance the need for innovation with the imperative of protecting individuals and

maintaining social order, thereby ensuring that technological advancements contribute positively to societal development.

2. LITERATURE REVIEW

Indonesia is a legal state as referred to in Article 1 paragraph 3 of the 1945 Constitution, which means that everything must be based on and regulated by law. (Siallagan, 2016). Based on that, all forms of Bank products must be regulated by law, such as bank account numbers which serve as a means to hold funds and also represent personal identity within them. Banks are institutions that gather funds from the public in the form of deposits and channel them to the public in the form of credit or other forms in order to improve the standard of living of the community.(Shandy Utama et al., 2021). Therefore, law enforcement is essentially a process to realize legal objectives into reality. Based on this, Sudikno Mertokusumo emphasizes that law enforcement should always be inseparable from certainty, justice, and utility. In line with these three values, Satjipto Raharjo states that law enforcement is an effort to realize ideas about justice, legal certainty, and social utility into reality. The process of embodying these ideas is the essence of law enforcement. (Muhamad Erwin, 2012)

The digital age, marked by rapid technological advancements, necessitates a transformation in governance to address the new challenges and opportunities that arise. Governance transformation involves updating and evolving policies, regulations, and institutional frameworks to effectively manage and oversee the digital landscape. In Indonesia, this transformation is crucial to address issues such as online scams, privacy concerns, and cybercrime, which have become prevalent with the increased use of digital tools and e-commerce.

Governance transformation aims to create a regulatory environment that balances innovation with the protection of public interests. This involves enhancing legal frameworks, such as the Information and Electronic Transactions Law (ITE Law), to cover emerging threats and ensure robust enforcement mechanisms. It also requires the development of policies that promote digital literacy and cybersecurity awareness among the public, thereby mitigating risks associated with online activities.

A key aspect of governance transformation is ensuring that law enforcement is equipped to handle the complexities of the digital era. This includes training law enforcement officers in cybercrime investigation techniques, establishing specialized cybercrime units, and fostering international cooperation to tackle cross-border cyber threats. Effective governance also requires collaboration between various stakeholders, including government bodies, law enforcement agencies, private sector entities, and civil society. This collaborative approach ensures that diverse perspectives are considered in policy-making, leading to more comprehensive and effective regulations.

Moreover, governance transformation involves the continuous monitoring and evaluation of policies to ensure they remain relevant and effective in the face of rapid technological changes. This dynamic approach allows for the adaptation of legal and regulatory frameworks to new technological trends, thereby maintaining a balance between innovation and regulation.

In the context of banking, governance transformation is essential to address the sale and misuse of bank account numbers, which represent a significant threat to personal data security and financial integrity. By implementing robust legal frameworks and enforcement mechanisms, Indonesia can safeguard the public from potential fraud and ensure that banking practices remain secure and trustworthy.

Ultimately, governance transformation is about creating a resilient and adaptive legal and regulatory system that can keep pace with the rapid evolution of technology. It aims to ensure that technological advancements contribute positively to societal development, fostering an environment where innovation thrives while public interests are protected. This transformation is vital for maintaining legal certainty, justice, and utility in the digital age, aligning with the principles emphasized by legal scholars such as Sudikno Mertokusumo and Satjipto Raharjo.

3. METHODOLOGY

This study adopts a normative juridical approach, relying on secondary data sources for analysis. Primary data consists of legal texts, including laws and regulations, while secondary sources encompass books, articles from journals (both in print and online), and other library materials. Additionally, tertiary sources such as dictionaries are consulted. These materials are thoroughly examined and presented descriptively. Subsequently, qualitative analysis is conducted to address the research questions, leading to conclusions and recommendations.

4. DISCUSSION

4.1. The Policy Formulation Regarding The Sale and Purchase Of Accounts In The Amandement To Law Number 11 0f 2008 on Information and Electronic Transactions, as Outlined in Law Number 1 of 2024, Aims To Ensure Legal Certainty

Each law upheld by society encompasses the principle of certainty, including the inherent laws within society (living law). This certainty principle is a fundamental aspect of every law's creation, ensuring a sense of justice and fostering order. These principles suggest that a law is deemed to possess certainty when it predates or is established before the actions it regulates occur (principle of legality). This pursuit of certainty stands as a primary objective of law, alongside justice and societal benefit.(Remaja, 2014)

A contract is a product of mutual consent between two or more parties, detailing the matters they wish to execute, the method and timeline of execution, and the parties responsible for carrying out the agreement. In the context of online sales and purchases,a contract is deemed legitimate if it satisfies subjective and objective criteria. Compliance with these criteria confirms the validity of the contract. Contracts also establish the rights and responsibilities of the parties involved, underscoring the significance of meeting all prerequisites for validity. In the event of future issues or disagreements, resolution can be sought by referring to the terms outlined in the agreed-upon contract.

Hence, the exponential expansion of electronic transactions necessitates legislative measures. These regulations should offer precise definitions of account buying and selling within a legal framework, encompassing crucial elements like the account owner's consent, permissible account types for trading, and relevant legal constraints. Moreover, the

legislation must criminalize the sale of account numbers without the owner's authorization, imposing stringent legal penalties. This entails explicit prohibitions, sanctions, and enforcement protocols. Additionally, the law should encompass provisions governing the safeguarding of account holders' personal information in the context of account transactions. This encompasses policies on data utilization, disclosure, and response protocols in the event of a data breach. Furthermore, it is imperative to outline the responsibilities of online platforms facilitating account transactions, including identity verification, transaction oversight, and reporting suspicious activities to authorities. Moreover, the policy should delineate clear procedures for resolving disputes arising from account transactions, which may involve mediation, arbitration, or legal proceedings.

Given this, it is essential for the law to grant adequate power and resources to the regulatory body responsible for overseeing and enforcing regulations regarding the sale and purchase of accounts. Moreover, there is a need to implement public education initiatives concerning the hazards and repercussions associated with engaging in illicit account transactions. This can enhance public consciousness and diminish the demand for such services. Additionally, the formulation of policies must engage diverse stakeholders, including governmental bodies, financial institutions, online platforms, civil society organizations, and the broader public.

Considering these factors, the policy regarding the formulation of account sales and purchases in Law Number 1 of 2024, amending Law Number 11 of 2008 on Electronic Information and Transactions, will establish a robust framework for ensuring legal certainty in the rapidly expanding digital economy.

The formulation of prohibited acts in the ITE Law does not specifically address the sale of account numbers as an illicit activity. Law Number 1 of 2024, also known as the ITE Law, was crafted in response to advancements in information technology within the legal sphere. Its purpose is to govern all virtual activities undertaken by individuals, reflecting the evolving landscape of virtual interactions and transactions.

It is essential to develop policies that prioritize stringent protection of personal data for account holders to prevent data misuse and safeguard individual privacy. Therefore, legislation must explicitly stipulate that selling account numbers without owner consent is unlawful and may incur severe legal penalties. This measure will aid in mitigating instances of fraud and deception linked to account number trading. Additionally, policies should outline the obligations of online platforms or marketplaces that facilitate such transactions. They should implement rigorous verification processes and assume responsibility for ensuring the legality and compliance of facilitated transactions with relevant laws.

Hence, legislation should foster collaboration among online platforms, financial institutions, and law enforcement agencies to enhance the efficacy of addressing instances of fraud and illicit account number sales. Given that the effectiveness of the law extends beyond its content to encompass the legal structure and culture, it becomes evident that educating the public about the risks linked to illegal trading of account numbers is crucial. Such efforts can diminish the market demand for such services. Additionally, policies should bolster enhanced monitoring and law enforcement measures to address infractions associated with the sale and purchase of account numbers more effectively. Taking these factors into account, the formulation and execution of policies within Law Number 1 of 2024, amending Law Number 11 of 2008 regarding Electronic Information and Transactions, can establish a holistic framework to address the issue of illicit account number sales, safeguarding public welfare and individual privacy.

In the context of digital transactions and the evolving landscape of online interactions, governance transformation is critical to ensure that regulatory frameworks keep pace with technological advancements. Governance transformation involves modernizing and adapting the legal and regulatory infrastructure to address new challenges posed by the digital economy.

One key aspect of governance transformation is the development of comprehensive laws and regulations that address the specificities of digital transactions. This includes updating existing laws to cover new forms of cybercrime, such as the illicit sale of bank account numbers, and ensuring that these laws provide clear definitions, penalties, and enforcement mechanisms. Effective governance requires that laws are not only reactive but also proactive, anticipating future trends and threats in the digital space.

Another important element is the enhancement of institutional capacities. Regulatory bodies must be equipped with the necessary resources, technology, and expertise to monitor, regulate, and enforce digital transaction laws effectively. This might involve setting up specialized units within law enforcement agencies dedicated to tackling cybercrime and fraud related to digital transactions. Training programs for law enforcement officers on the latest cyber threats and investigative techniques are essential to ensure that they can effectively address and mitigate risks.

Governance transformation also calls for increased collaboration between various stakeholders. This includes not only governmental and regulatory bodies but also private sector entities such as financial institutions, online platforms, and cybersecurity firms. A collaborative approach ensures that policies and regulations are well-informed, practical, and have the support needed for effective implementation. For instance, online platforms should work closely with regulatory bodies to implement robust verification processes and promptly report suspicious activities.

Public education and awareness are crucial components of governance transformation. By educating the public about the risks and legal consequences of engaging in illicit activities like the sale of account numbers, it is possible to reduce demand for such services and promote safer online behavior. Public awareness campaigns can also inform individuals about how to protect their personal information and recognize potential scams.

Moreover, governance transformation should include mechanisms for regular review and adaptation of laws and policies. The digital landscape evolves rapidly, and legal frameworks must be flexible enough to adapt to new developments. This might involve establishing advisory committees or task forces that continuously assess emerging threats and recommend updates to laws and regulations.

Finally, governance transformation must prioritize the protection of personal data and privacy. Strong data protection laws are essential to safeguard individuals' personal information from misuse and abuse. Legislation should mandate stringent data protection measures for all entities involved in digital transactions, including requirements for secure data storage, limited data sharing, and protocols for responding to data breaches.

In conclusion, the transformation of governance structures is essential to address the complexities of the digital economy and ensure that legal frameworks are equipped to handle the challenges posed by technological advancements. By developing comprehensive, forward-looking laws, enhancing institutional capacities, fostering collaboration, educating the public, and prioritizing data protection, governance transformation can create a secure and trustworthy environment for digital transactions.

This, in turn, will support the broader goals of legal certainty, justice, and societal benefit in the digital age.

4.2. The Implementation Policy For Individuals Engaging In The Buying And Selling Of Accounts Under Law Number 1 of 2024, Amending Law Number 11 of 2008 Regarding Information and Electronic, Is Closely Tied To Legal Certainty

An electronic contract, as defined by the ITE Law, pertains to agreements formed between parties using electronic systems. Such contracts are established when a legal entity conducts transactions or legal activities through computers, computer networks, or other electronic means. These transactions may take place through electronic contracts or alternative forms of agreements, serving as mutual agreements between involved parties.

The validity of an agreement is fundamentally independent of its physical form. Whether in print or electronic format, verbal or written, an agreement is legally recognized if it fulfills the criteria outlined in Article 1320 of the Civil Code. These conditions entail mutual consent between the parties involved, legal capacity to act, a defined subject matter of the agreement, and the presence of a lawful consideration.(Triantika et al., 2020)

Furthermore, Government Regulation Number 71 of 2019 delineates the specific legal prerequisites for an electronic agreement or contract, stipulating that it must entail mutual agreement between the parties involved. It must also be executed by a legally competent entity or a representative with the requisite authority as per statutory regulations. Additionally, the agreement must pertain to specified matters, and the transaction's subject matter must not contravene statutory regulations, ethical standards, or public order.

Electronic contracts, as sanctioned by the ITE Law, hold validity as legal evidence, as electronic information and/or documents serve as an extension of legal evidence within the framework of procedural law applicable in Indonesia.

Regarding the significance of opening bank accounts in driving economic activities, any infractions related to this process can pose risks to customers and tarnish the image of financial institutions. Hence, it's imperative to conduct a review of regulations to discern any discrepancies stemming from either misinterpretations or deliberate violations. Pinpointing issues like customer misconceptions and ambiguous regulations is crucial, demanding a thorough examination of banking ethics.(Lubis & Machmud, 2024)

In instances where bought or sold accounts, whether acknowledged or not, are utilized for illicit activities such as fraud or money laundering, this poses a legal conundrum with significant ramifications. Law enforcement entities, such as the police, tasked with uncovering the truth through investigations and inquiries, encounter challenges in applying regulations pertaining to account transactions. Instead, they resort to regulations addressing subsequent offenses like fraud, as outlined in Article 378 of the Criminal Code. This article stipulates that individuals who, with the intent of gaining unlawful benefit for themselves or others, employ false identities or deceitful practices to induce another person into relinquishing property or forgiving a debt, are subject to a maximum imprisonment of four years for fraud.

Furthermore, those engaged in online buying and selling may also fall under the purview of Article 28, paragraph 1 of the ITE Law. This provision addresses individuals who deliberately disseminate false and misleading information leading to financial losses for consumers in electronic transactions.

Moreover, concerning the trade of account numbers containing personal data, the ITE Law lacks a specific definition of personal data. Nevertheless, it stipulates that users accessing information via electronic means pertaining to an individual's personal data must obtain consent from the concerned individual, unless statutory regulations state otherwise.

Additionally, if fraud is confirmed, in accordance with the initial provisions outlined in paragraph (1) of Bank Indonesia Regulation Number 2/19/PBI/2000 regarding the criteria and procedures for authorizing or granting written consent to disclose bank secrets, it is stipulated that freezing and/or seizing deposits held under the name of depositors who have been identified as suspects or defendants by law enforcement authorities, such as the police, prosecutor, or judge, can be carried out in accordance with prevailing laws and regulations without necessitating approval from the Bank Indonesia Management.

Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions defines personal data as information pertaining to an individual, whether identified or identifiable alone or when combined with other data, directly or indirectly, through electronic or non-electronic means. Additionally, Minister of Communication and Information Technology Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems stipulates that personal data of certain individuals must be accurately stored, maintained, and safeguarded for confidentiality. Furthermore, specific individual data refers to authentic information associated with and capable of identifying an individual, directly or indirectly, in accordance with legal provisions.

Although there are various regulations protecting personal data, there is still ambiguity in determining and regulating the buying and selling of account numbers in the ITE Law. This lack of clarity hampers law enforcement, where law enforcement agencies, such as the police, face limitations in handling cases related to account number transactions due to the absence of specific provisions or the need for expanded authority. Additionally, identifying perpetrators of these activities is difficult, often done anonymously or using fake identities. The issue becomes more complex with the challenge of gathering sufficient digital evidence, given the easily changeable and difficult-to-trace digital nature. Furthermore, law enforcement also faces difficulties in coordinating with online platforms facilitating account number transactions. Lack of cooperation from relevant parties hinders law enforcement efforts and prevention. Moreover, there is still a lack of public awareness and legal education regarding the risks and consequences of buying and selling account numbers. Without a clear understanding of the legal implications, individuals may engage in these activities without considering the repercussions. The complexity of protecting personal data in account transactions adds to law enforcement challenges. Effective protection requires cooperation among governments, financial institutions, and online platforms to identify, prevent, and address these illegal practices.

Therefore, it is crucial to refine more precise regulations, enhance the capabilities of law enforcement officers in managing digital cases, raise legal awareness and public education, and bolster cooperation among all pertinent stakeholders. Additionally, concerted efforts are needed to enhance the safeguarding of personal data and fortify a more efficient monitoring and law enforcement mechanism for addressing instances of buying and selling illegal account numbers.

Governance transformation is essential to align legal frameworks with the rapid advancements in technology and the evolving nature of digital transactions. This transformation involves updating laws, enhancing institutional capacities, fostering collaboration among stakeholders, and promoting public awareness.

To effectively govern electronic contracts and transactions, it is imperative to update existing laws and introduce new regulations that address the specificities of the digital environment. This includes providing clear definitions of what constitutes the illicit sale of account numbers, establishing stringent penalties for such activities, and creating robust enforcement mechanisms. Laws must be proactive, anticipating future challenges and technological developments, ensuring that they remain relevant and effective.

Regulatory bodies must be equipped with the necessary resources, technology, and expertise to monitor, regulate, and enforce digital transaction laws effectively. This might involve creating specialized units within law enforcement agencies dedicated to combating cybercrime, including fraud and the illegal sale of account numbers. Training programs for law enforcement officers on the latest cyber threats and investigative techniques are essential to enhance their capability to address these issues.

Effective governance in the digital age requires collaboration between various stakeholders, including government agencies, financial institutions, online platforms, and cybersecurity firms. This collaborative approach ensures that policies and regulations are well-informed, practical, and supported by all relevant parties. Online platforms should work closely with regulatory bodies to implement robust verification processes and promptly report suspicious activities. Financial institutions and cybersecurity firms can provide insights and technological solutions to enhance the security and monitoring of digital transactions.

Public education and awareness are critical components of governance transformation. Educating the public about the risks and legal consequences of engaging in illicit activities, such as the sale of account numbers, can reduce the demand for such services and promote safer online behavior. Public awareness campaigns should inform individuals about how to protect their personal information and recognize potential scams. This effort can significantly contribute to preventing illegal activities and protecting personal data.

The digital landscape evolves rapidly, necessitating regular review and adaptation of laws and policies. Governance transformation should include mechanisms for continuous assessment of emerging threats and trends, allowing for timely updates to legal frameworks. Establishing advisory committees or task forces that monitor technological developments and recommend necessary legal adjustments can ensure that laws remain effective and relevant.

Protecting personal data is a cornerstone of governance transformation. Strong data protection laws are essential to safeguard individuals' personal information from misuse and abuse. Legislation should mandate stringent data protection measures for all entities involved in digital transactions, including requirements for secure data storage, limited data sharing, and protocols for responding to data breaches. These measures help build trust in digital transactions and protect individuals' privacy.

Governance transformation is crucial for effectively managing the challenges posed by the digital economy, particularly in the realm of electronic contracts and transactions. By updating laws, enhancing institutional capacities, fostering stakeholder collaboration, promoting public awareness, regularly reviewing legal frameworks, and prioritizing data protection, governance transformation can create a secure and trustworthy environment for digital transactions. This holistic approach not only addresses the issue of illicit account number sales but also ensures legal certainty, justice, and societal benefit in the rapidly evolving digital age.

5. CONCLUSION AND RECOMMENDATION

In the ever-evolving digital landscape, the phenomenon of buying and selling accounts has emerged, with bank accounts being traded as commodities. While Electronic Agreements or Contracts are governed by the ITE Law as valid agreements, the practice of trading accounts poses complex challenges in the legal and financial realms. One crucial aspect is the safeguarding of personal data. Despite legal frameworks in the ITE Law addressing data protection, the absence of clear definitions and regulations regarding account trading impedes law enforcement efforts. This presents new hurdles for authorities in identifying culprits, gathering digital evidence, and liaising with online platforms facilitating this illicit activity. Furthermore, handling account trading cases is compounded by elements like fraud and money laundering, necessitating robust law enforcement to mitigate customer losses and uphold financial institution integrity.

Governance transformation is essential in addressing these challenges effectively. This transformation involves updating and refining laws to provide precise definitions and stringent penalties for illicit activities related to account trading. Enhancing institutional capacities is crucial, equipping regulatory bodies and law enforcement agencies with the necessary resources, technology, and expertise to monitor and enforce digital transaction laws. Collaboration among stakeholders—government agencies, financial institutions, online platforms, and cybersecurity firms—is vital to ensure comprehensive and practical policy implementation. Public education and awareness campaigns play a critical role in mitigating participation in unlawful practices by informing individuals about the risks and legal repercussions of account trading. In conclusion, governance transformation through updated laws, enhanced institutional capacities, stakeholder collaboration, and public education is imperative to effectively manage the complexities of account trading. This holistic approach ensures legal certainty, protects personal data, and upholds the integrity of financial institutions, thereby fostering a secure and trustworthy digital environment.

ACKNOWLEDGEMENT

The author would like to express his deepest gratitude to the Chancellor of the Indonesian Computer University and all his staff who have supported the author in submitting this article to the journal Atlantis Press

REFERENCES

Hanim, L. (2011). Pengaruh Perkembangan Teknologi Informasi Terhadap Keabsahan Perjanjian Dalam Perdagangan Secara Elektronik (E-Commerce) Di Era Globalisasi. *Jurnal Dinamika Hukum*, *11*(Edsus). https://doi.org/10.20884/1.jdh.2011.11.edsus.262

Lubis, R. L., & Machmud, A. (2024). *Implementasi Aturan Terkait Pembukaan Rekening Nasabah (Studi Kasus PT Bank Central Asia Tbk)*. *6*(2), 7714–7724.

Maryanto, Y. T. (2021). *PERJANJIAN JUAL BELI ONLINE MELALUI TOKOPEDIA Mahasiswa Fakultas Hukum Universitas Sebelas Maret Abstrak Pembeli . Pada zaman*

yang serba digital ini , baik Penjual maupun Penjual tidaklah dibeli olehnya . Dengan internet sebagai perantara , saat ini dalam. *9*, 281–290.

Muhamad Erwin, F. F. B. (2012). *Pengantar Ilmu Hukum*. PT. Reflika Aditama.

Pratama, G. (2020). 130-64-555-1-10-20200901. *Jurnal Ekonomi Dan Bisnis Islam Jurnal Ecopreneur*, *1*(1), 21–34.

Pridbadi, R. Y. (2021). *Volume 10 , Nomor 1 , Tahun 2021 Website : https://ejournal3.undip.ac.id/index.php/dlr/ KAJIAN YURIDIS PENGGUNAAN REKENING BERSAMA DALAM JUAL BELI ONLINE PADA FACEBOOK MARKETPLACE Ramzy Yanuar Pribadi *, Suradi , Dewi Hendrawati Program Studi S1 Ilmu Huku*. *10*, 235–245.

Ranto, R. (2019). Tinjauan Yuridis Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Jual Beli Melalui Media Elektronik. *Jurnal Ilmu Hukum: ALETHEA*, *2*(2), 145–164. https://doi.org/10.24246/alethea.vol2.no2.p145-164

Remaja, N. G. (2014). Makna Hukum dan Kepastian Hukum. *Kertha Widya: Jurnal Hukum*, *2*(1), 1–26. https://ejournal.unipas.ac.id/index.php/KW/article/view/426/351

Shandy Utama, A., Iqsandri, R., Rizana, Susanty, A. P., Permana, F. A., & Zainuddin. (2021). Perlindungan Negara Terhadap Dana Simpanan Nasabah Pada Perbankan. *Jurnal Sociohumaniora Kodepena (JSK)*, *2*(1), 48–60. https://doi.org/10.54423/jsk.v2i1.60

Siallagan, H. (2016). Penerapan Prinsip Negara Hukum Di Indonesia. *Sosiohumaniora*, *18*(2), 131–137. https://doi.org/10.24198/sosiohumaniora.v18i2.9947

Tim Kompas. (2023). *Rekening Bank Dijual di Media Sosial*. https://www.kompas.id/baca/investigasi/2023/12/05/rekening-bank-dijual-di-media-sosial

Triantika, N. A., Marwenny, E., & Hasbi, M. (2020). Tinjauan Hukum Tentang Pelaksanaan Perjanjian Jual Beli Online Melalui E-Commerce Menueur Pasal 1320 Kuhperdata. *Ensiklopedia Sosial Review*, *2*(2), 119–131. https://doi.org/10.33559/esr.v2i2.488

Yuni Astutik & Rahajeng Kusumo Hastuti. (2020). *Ilegal Nih! Jual Beli Rekening Bank Ada di Tokopedia*. CNBC Indonesia. https://www.cnbcindonesia.com/tech/20200702145618-37-169731/ilegal-nih-jual-beli-rekening-bank-ada-di-tokopedia

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.