JURNAL AKTA
Volume 11 No. 3, September 2024
SINTA 2 by Nationally Accredited Journal,
Decree No. 164/E/KPT/2021

Defining Legal Contours of Digital Identity Theft

Tantimin[1)], Emiliya Febriyani[2)], Agustianto[3)], and Rufinus Hotmaulana Hutauruk[4)]

[1)] Faculty of Law, Universitas Internasional Batam, Indonesia,
Email: tantimin.lec@uib.ac.id
[2)] Faculty of Law, Universitas Internasional Batam, Indonesia,
Email: emiliya@uib.ac.id
[3)] Faculty of Law, Universitas Internasional Batam, Indonesia,
Email: agustianto.lec@uib.ac.id
[4)] Faculty of Law, Universitas Internasional Batam, Indonesia,
Email: rufinus.hotmaulana@uib.ac.id

Abstract. *The proliferation of digital technology has challenged the traditional understanding of identity and subsequently brought forth its own unique legal implications. Identity theft, as a crime that has existed even before this development, has also brought its own unique legal implications, particularly in the realm of criminal law. Using the normative legal research method, this research aims to establish the boundaries around digital identity theft, to distinguish it from traditional identity theft, and to provide a more relevant and robust understanding of its criminality within the digital age. The results of this study highlight the gaps in Indonesia's current legal framework, emphasizing the need for a revised approach that distinctly addresses the complexities of digital identity theft. The research proposes a model of normative development aimed at refining legal definitions and enhancing enforcement mechanisms to combat this modern crime better. This model seeks to provide a more relevant and robust legal framework, ensuring that the legal system is responsive and adaptive to the challenges posed by digital advancements.*

Keywords: *Criminal Law; Cyber Crime; Cyber Law; Digital Identity Theft; Fraud; Identity Theft; Privacy Rights; Legal Development*

1. INTRODUCTION

The rapid advancement of digital technology has fundamentally changed the landscape of personal identity and security.[1] Digital identities encompass a range of personal information and credentials used to verify an individual in the digital realm, which has become an inseparable part of daily life.[2] These identities are used across platforms such as social media, online banking, and e-commerce, to authenticate users and

[1] Alexandra Giannopoulou, "Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity," *Digital Society* 2, no. 2 (2023): 27.
[2] Johannes Sedlmeir et al., "Digital Identities and Verifiable Credentials," *Business & Information Systems Engineering* 63, no. 5 (2021): 603.

facilitate their online activities.[3] However, the rise of digital identities has been followed by a continued increase in their unauthorized creation and theft, which has caused about US$23 billion in financial loss in the United States alone.[4] This has raised concerns over the safety of digital spaces and necessitates technical prevention measures.[5] Digital identity theft, particularly characterized by the illicit acquisition and use of someone's personal data, poses severe risks to individuals and organizations alike.[6] Therefore, it's important to analyze the existing laws to prevent current and possible future risks of digital identity theft.

Digital identity creation involves collecting and managing data points such as usernames, passwords, biometric information, and personal identification numbers (PINs).[7] However, these same data, when misappropriated, can be exploited to commit a wide array of fraudulent activities, including financial fraud, unauthorized transactions, and identity fraud.[8] The unauthorized creation and manipulation of digital identities often bypass traditional security measures, making detection and prevention increasingly complex. Legal boundaries are crucially needed to clearly distinguish between lawful and unlawful actions in the realm of digital identity to set the standard of criminal provisions regarding identity theft, particularly when public concern is taken into account.[9] This involves addressing the theft of digital identities and the unauthorized creation of synthetic identities, where fabricated information is used to create new, fraudulent personas. The complexity and scale of these activities raise the urgency to formulate legal frameworks that are capable of tackling this novel challenge.

One of the central challenges in formulating legal frameworks for digital identity theft is the intrinsic nature of digital data and the damages that are caused by their misappropriation as both intangible and ubiquitous.[10] Unlike physical theft, digital identity theft involves the illicit access and use of information that can be duplicated and disseminated with relative ease within the digital realm. This intangibility can make

---

3 Sachin Parate, Hari Prasad Josyula, and Latha Thamma Reddi, "Digital Identity Verification: Transforming KYC Processes in Banking Through Advanced Technology and Enhanced Security Measures," *International Research Journal of Modernization in Engineering Technology and Science* 5, no. 9 (2023): 129.

4 Suzanne Sando, "2024 Identity Fraud Study: Resolving the Shattered Identity Crisis," *Javelin*, April 10, 2024.

5 Yasser Alhelaly, Gurpreet Dhillon, and Tiago Oliveira, "When Expectation Fails and Motivation Prevails: The Mediating Role of Awareness in Bridging the Expectancy-Capability Gap in Mobile Identity Protection," *Computers & Security* 134 (2023): 2. Gomgom Siregar and Sarman Sinaga, "The law globalization in cybercrime prevention," *International Journal of Law Reconstruction* 5, no. 2 (2021): 212.

6 Gargi Sarkar and Sandeep K Shukla, "Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies," *Journal of Economic Criminology* 2 (2023): 5–7.

7 Fennie Wang and Primavera De Filippi, "Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion," *Frontiers in Blockchain* 2 (2019): 8.

8 Eric S Boos, Chandler Givens, and Nick Larry, "Damages Theories in Data Breach Litigation," *Sedona Conference Journal* 16 (2015): 132.

9 Philip F. Disanto, "Blurred Lines of Identity Crimes: Intersection of the First Amendment and Federal Identity Fraud," *Columbia Law Review* 115, no. 4 (2015): 1034.

10 Alexander Savelyev, "The Inadequacy of Current Remedies for Violation of Data Subjects' Rights and How to Fix It," *Legal Issues in the Digital Age* 2, no. 2 (2020): 52–53.

it difficult to trace the perpetrators,[11] and significantly complicates the consolidation of traditional legal interests in the digital space.[12] Consequently, legal systems must evolve to recognize and address the unique characteristics of digital data, to tackle the growing prevalence of identity theft, which threatens many users of digital platforms.

Indonesia has tried to by enacting Law No. 27 of 2022 on Personal Data Protection. However, this particular development still has its own limitations, particularly regarding the scope of protection and responsibility of data processors,[13] among many others. For overall digital governance, Indonesia typically relies on Law No. 8 of 2011 on Electronic Information, which has seen many amendments over the years, as Indonesia is continuously faced with novel challenges that come alongside many forms of digital transformation. However, it's important to note that this framework is generalized in nature, as it aims to govern many aspects of the digital transformation, which continues to affect many facets of life. While the issues regarding privacy and security within the digital environment remain a serious concern within Indonesia's legal politics, possible regulatory lag might open ways for exploitations, particularly when digital identities are utilized fraudulently. Therefore, the analysis regarding key regulatory frameworks in Indonesia for this topic must be assessed in a holistic manner, covering many aspects that might affect the prevalence of digital identity theft.

Furthermore, the intersection of privacy rights and security measures presents a significant legal dilemma.[14] Effective protection against digital identity theft requires robust data security measures, including encryption, multi-factor authentication, and regular monitoring for unauthorized access. However, legal frameworks must ensure that security measures do not become overly intrusive or violate fundamental privacy rights. For instance, the General Data Protection Regulation (GDPR) in the European Union sets a precedent for balancing data protection with individual privacy by establishing stringent requirements for data processing and greater control over personal information.[15] The GDPR addresses this balance through provisions such as the right to be forgotten, outlined in Article 17, the requirement for data breach notification in Article 33, data minimization principles in Article 5, and stringent consent requirements in Article 6, all of which aim to ensure that while data security measures are implemented, individuals retain substantial control over their personal information, reducing the risks of digital identity theft.

As digital technology is getting more integrated into the daily lives of many Indonesians, legal implications regarding its utilization has become a topic of legal. A

---

[11] Vida Vilić, "Users' Considerations About Possibilities of Self-Protection on Social Networks," *Open Journal for Legal Studies* 1, no. 1 (2018): 13.

[12] R. Andrew Grindstaff, "Article III Standing, the Sword and the Shield: Resolving a Circuit Split in Favor of Data Breach Plaintiffs," *William & Mary Bill of Rights Journal* 29, no. 3 (2021): 856.

[13] Patricia Edina Sembiring, Ahmad M. Ramli, and Laina Rafianti, "Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik," *Veritas et Justitia* 10, no. 1 (June 29, 2024): 149.

[14] Yanshu Wang, "Realistic Dilemma and Path Optimization of Online Personal Information Protection," *Lecture Notes in Education Psychology and Public Media* 39, no. 1 (2024): 188.

[15] Ruziev Ruziev Rustam, Abduvaliev Bokhadir, and Rakhmatov Uktam, "An Overcoming the Privacy Paradox: Legal Aspects of Data Protection in the Digital Age," *International Journal of Cyber Law* 1, no. 4 (June 2023): 4.

study embarked on the analysis regarding 'the privacy paradox,' which is the phenomenon where people claim to value privacy but give away personal data easily or neglect privacy protections, highlighting that the term is logically flawed and doesn't constitute a paradox.[16] Unlike the popular trend among privacy-conscious users of electronic systems, the study highlighted the gap between people's attitudes and behaviors regarding privacy, showing that these do not always reflect true preferences. The study concluded that efforts to align the two different aspects of preferences fell short of understanding that whenever both aspects fail to align, there is no inconsistency that justifies calling it a paradox. An aspect of this dynamic between the utilization of digital technology and privacy that reflects people's preferences is consent, as highlighted by another study.[17] The study highlighted consent as a critical component of the right to privacy under Law No. 27 of 2022, but the law's focus on data collection and processing overlooks specific safeguards for digital identity theft, leaving individuals vulnerable to unauthorized exploitation of their data as digital identities. While the studies emphasized the importance of privacy and consent, they did not fully address the legal consequences of issues such as unauthorized data usage and identity theft, which may occur when privacy protections are insufficient or poorly enforced.

Identity theft as a crime is a problem that has emerged as one of the most concerning out of all crimes committed using the current relevant technologies. A study highlighted exactly this by underscoring different methods used in the crime of identity theft.[18] The study also highlighted that, due to the complex nature of identity theft, which can combine different methods, be it physical or digital, the effort to tackle and seek justice from it remains a significant challenge. Even more concerning, the study also underscored the difficulty in assessing the safety of victims, as most of them can only assume that they're safe when there's no longer notification regarding the misuse of their identity. Concerns are also raised by a study analyzing different types of cybercrimes, with identity theft as one of the popular methods used by criminals in the virtual realms.[19] It critically highlighted the fact that identity theft as a crime could also be used to commit even more crimes, as it helped protect the identity of the perpetrators.

Based on the literature review, a gap can be identified regarding the crime of identity theft, which has always been analyzed in the traditional or broader sense. There needs to be a narrower focus of analysis on the criminality of identity theft in the digital realm, as it presents unique legal implications and challenges that subsequently need to be tackled. This research aims to fill this gap by bridging the understanding between traditional identity theft and digital technology to eventually create a separate understanding of what is called 'digital identity theft.' This research ultimately explores

---

[16] Daniel J. Solove, "The Myth of the Privacy Paradox," *George Washington Law Review* 89, no. 1 (2021): 2–4.

[17] Vera W. S. Soemarwi and W. Susanto, "Digital Technology Information in Indonesia: Data Privacy Protection Is a Fundamental Right," in *Proceedings of the International Conference on Economics, Business, Social, and Humanities (ICEBSH 2021)*, vol. 570, 2021, 564.

[18] Megan Wyre, David Lacey, and Kathy Allan, "The Identity Theft Response System," *Trends and Issues in Crime and Criminal Justice*, no. 592 (2020): 6.

[19] Muh. Fadli Faisal Rasyid et al., "Cybercrime Threats and Responsibilities: The Utilization of Artificial Intelligence in Online Crime," *Jurnal Ilmiah Mizani: Wacana Hukum, Ekonomi Dan Keagamaan* 11, no. 1 (April 2024): 52.

the criminality of digital identity theft, the normative challenges in tackling it, and how distinct it is from other types of crimes that share similar elements.

2. RESEARCH METHODS

This research utilizes the normative legal research method to analyze the relevant positive laws that are being enforced.[20] A normative analysis typically dives into the implications of a certain issue and how the existing legal norms see them, which, in its purest form, involve the utilization of secondary data in the form of positive laws.[21] This fits the purpose of the research, which is to analyze the criminal aspects of identity theft, the challenges of its enforcement, and how it can be improved. Secondary data used in this research include Law No. 11 of 2008 on Electronic Information Transactions, Law No. 19 of 2016 on Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 1 of 2024 on Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions, Law No. 27 of 2022 on Personal Data Protection, Title 18 of the United States Code. Secondary data are analyzed descriptively, data analysis, to provide a comprehensive normative analysis of the existing norms and structures around digital identity theft.

3. RESULTS AND DISCUSSION

3.1. Traditional v. Digital Identity Theft

Identity as a concept is important for every person, as it constitutes the very fabric of their being. Therefore, its misappropriation ultimately compromises the integrity of systems that represent integral components of the fabric of society.[22] Identity is used in many interactions, and in the digital context, people can bring their own unique social dimensions to society, particularly by sharing values and identities.[23] As digital technology is continuously changing the landscape of identity, further advances in digital technology eventually integrate the aspects that make up an identity into the digital environment, creating what is essentially known as digital identity. Digital identity itself is, to put it simply, a digital version of traditional identity. In other words, it's the digitized aspects of traditional identity condensed into a single set of data that can be used to identify a person.[24] At a glance, this might be particularly simple. However, the difference between the two can have a wide array of implications for the person behind that identity.

Due to the significance of identity in many facets of life, the protection of identity remains a topic of paramount importance and will become even more relevant as novel

---

[20] Hari Sutra Disemadi, "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies," *Journal of Judicial Review* 24, no. 2 (2022): 295.

[21] David Tan, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum," *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 2467.

[22] Susan Helser, "FIT: Identity Theft Education: Study of Text-Based versus Game-Based Learning," in *International Symposium on Technology and Society, Proceedings*, vol. 2016-March, 2016, 4.

[23] Deborah Lupton, "The Internet of Things: Social Dimensions," *Sociology Compass* 14, no. 4 (2020): 3.

[24] AR Friedman and LD Wagoner, "The Need for Digital Identity in Cyberspace Operations," *Journal of Information Warfare (JIW)* 13, no. 2 (2014): 42.

technologies continue to be invented and developed.[25] Identity, when stolen, can cause significant damage to the person that it belongs to.[26] Beyond financial repercussions, stolen identities can be used to disrupt an individual's social and professional lives.[27] Stolen identities can also be used to commit crimes, unfairly linking the victim to illegal activities and potentially leading to legal repercussions.[28] The legal system must be able to prevent such things from happening and give severe repercussions to those who are behind such criminal acts. The legal system must also be able to consolidate the changes that have happened in society into the relevant legal framework to ensure that they are not being exploited to make ways for identity theft.

Identity theft as a crime has evolved throughout history, as criminals have been continuing to find ways to adapt to the sociotechnical changes that are happening to society to be able to continue to abuse other people's identities.[29] In general, identity theft can be defined as the unlawful utilization of another person's identification.[30] Identity theft is often utilized by criminals to take advantage of a person's position in society, which can eventually be used to commit other criminal offenses, such as property theft and many forms of fraud. In the traditional sense, identity theft can happen using many physical acts, such as house break-ins, mail theft, dumpster diving, and wallet theft.[31] This criminal offense has caused considerable concern, particularly because it keeps evolving and causing much damage and disturbances within society.

In the digital sense, identity theft as a criminal offense brings different unique factors. While it can also happen in conjunction with other acts that can be considered traditional, digital identity theft overall can happen in a much simpler manner while also having about the same potential of abuse for further criminal offenses. This is because the developments of digital technology can render identity theft easier and even damage the perspective of the crime itself, leading some to think that it's less severe.[32] Due to the nature of the digital environment, where it's often difficult to verify the identity of people we are interacting with, many often let their guard down as they continue to interact with individuals who might be posing as someone else on

---

[25] Hong Wu and Wenxiang Zhang, "Digital Identity, Privacy Security, and Their Legal Safeguards in the Metaverse," *Security and Safety* 2 (2023): 2–3.

[26] Yuan Li et al., "Responding to Identity Theft: A Victimization Perspective," *Decision Support Systems* 121 (2019): 15.

[27] Samuel H. Goh et al., "Graduate Student Perceptions of Personal Social Media Risk: A Comparison Study," *Issues In Information Systems* 17, no. IV (2016): 109.

[28] Fawzia Cassim, "Protecting Personal Information in the Era of Identity Theft: Just How Safe Is Our Personal Information from Identity Thieves?," *Potchefstroom Electronic Law Journal* 18, no. 2 (2015): 76.

[29] Abdul Bashiru Jibril et al., "Online Identity Theft on Consumer Purchase Intention: A Mediating Role of Online Security and Privacy Concern," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12067 LNCS, 2020, 2.

[30] Wyre, Lacey, and Allan, "The Identity Theft Response System," 2.

[31] Vincent Alagna, "A Comparative Analysis of Identity Theft within America and Australia," *Criminal Justice* Spring 5 (2020): 2.

[32] Majid Sarfi, Morteza Darvishii, and Mostafa Zohouri, "Why People May View Online Crimes as Less Criminal: Exploring the Perception of Cybercrime," *International E-Journal of Criminal Sciences*, no. 18 (2023): 9.

platforms like social media.[33] Even more concerning, these names and photos can easily be extracted from the internet using many methods, which oftentimes only involve a basic level of understanding of the technicalities behind websites or the use of third-party apps and websites.[34]

Furthermore, perpetrators of digital identity theft can also remain anonymous, which further complicates the prosecution of the crime. Digital technologies can allow individuals to remain anonymous to ensure privacy and protect themselves from many types of unlawful surveillance. However, this noble development to help protect privacy rights can also be utilized to provide cover and layers of safety for criminals who steal other people's identities, allowing them to conceal their identities.[35] Electronic system providers have tried to provide proactive measures in preventing digital identity theft, mainly by introducing a system of verification that comes with a badge that indicates that a user has been verified to be the real person with the correct identity as indicated in that electronic system. However, this doesn't necessarily denote the chances of abuse, as cases of fraud supported by identity theft continue to occur, as criminals can still find some workarounds to commit identity theft, such as creating a fake verification badge behind their accounts' background image.[36]

From the criminal law standpoint, establishing clear lines between traditional identity theft and digital identity theft is both imperative and urgent. As digital technologies continue to develop, the values behind digital identities will also rise significantly.[37] Consequently, the urgency to protect them will become even more important, as digital technologies can also provide ways that can essentially help criminals steal digital identities. It's also imperative for a legal framework to provide preventive measures, mainly from providing an adequate level of compliance for data protection and privacy, to ensure that data controllers are processing data securely. Lastly, the lines that are going to be established must be able to consolidate the differences between the two forms of identity theft to provide a mechanism of remedy to prevent further damage to the person behind a digital identity. These are essential in ensuring that digital identity theft doesn't become a common problem in a society that will be ever-so-reliant on digital interactions.

---

[33] Kunwar Surendra Bahadur, "A Brief Study On Negative Effects of Social Media On Youth," *Bayan College International Journal of Multidisciplinary Research* 1, no. 2 (2021): 5.

[34] Cassandra Cross and Rebecca Layt, "'I Suspect That the Pictures Are Stolen': Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities," *Social Science Computer Review* 40, no. 4 (2022): 963.

[35] Christie Franks and Russell Smith, *Identity Crime and Misuse in Australia 2019*, *Australian Institute of Criminology* (Canberra: Australian Institute of Criminology, 2020), 31.

[36] Kuwihoi New and ZianXiang Kong, "Exploring Teenage Awareness of Social Media Fraud in Malaysia," *International Journal of Academic Research in Business and Social Sciences* 13, no. 12 (2023): 467.

[37] Loso Judijanto et al., "Analysis of the Influence of Social Media Use, Educational Technology, and Digital Identity on Educational Culture Change in West Java," *West Science Social and Humanities Studies* 2, no. 3 (March 2024): 380–381. Milla Mudzalifah and Pujiyono, "The Politics of Criminal Law in Cybercrime: An Efforts to Combat Information Technology Crimes in Indonesia," *Jurnal Pembaharuan Hukum* 10, no. 1 (2023): 78.

3.2. Digital identity theft v. data theft in Indonesian legal framework

It's imperative to analyze the relevant legal framework in dealing with identity theft, particularly in a civil law country like Indonesia, where the legal system prioritizes codified law over other aspects of the legal system.[38] In the traditional sense, identity theft as a distinct crime is not covered by Indonesia's Criminal Law Code. This leaves a considerable gap within the Indonesian legal system, as there are no basic legal norms that can be utilized to help prevent identity theft and punish those who commit it. It's even more problematic when the fact that stolen identity can be used to facilitate other crimes is taken into account. Despite the position of identity crime as a facilitator crime, or the crime used to facilitate other crimes,[39] it is in itself a serious crime, and its aspects must be consolidated into the legal framework properly. Furthermore, this problem can also complicate the establishment of clear legal norms to define digital identity theft and how it differs from traditional identity theft.

Indonesia has tried to consolidate the changes brought by digital technology into its legal system by establishing clear lines regarding the responsibilities of electronic system providers, along with the norms that electronic system users must adhere to. This was done through the enactment of Law No. 11 of 2008 on Electronic Information Transactions (EIT Law). However, the EIT Law doesn't provide any provision regarding identity or the protection of it. Some provisions can be used to provide a generalized connection to what constitutes identity, such as Article 1 number 1 and Article 1 number 4, which both provide the basic definition of electronic information and electronic documents. Interestingly, these provisions do not mention identity as one of the forms of information that might be included within an electronic document, although the information referred to can actually be used to identify. Furthermore, Article 9 governs that business actors offering products through Electronic Systems must provide complete and correct information relating to the terms of the contract, the producer, and the products offered. The information referred to in Article 9 specifically mentioned the identity of all the parties relevant to the contract, as elaborated in the explanation of the article. However, these provisions are as far as the EIT Law goes in providing clear lines for digital identity.

EIT Law itself has been amended many times, first through Law No. 19 of 2016 on Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (First Amendment to EIT Law) and Law No. 1 of 2024 on Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions (Second Amendment to EIT Law). The changes brought by both the First and Second Amendments to EIT Law don't bring about the much-needed provisions to provide clear lines for digital identity and digital identity theft. However, the First Amendment to EIT Law provides a clearer direction of legal development for data protection, as it brought many changes in how Indonesia regulates data protection and privacy, which would later be followed by Law No. 27 of 2022 on Personal Data Protection (PDP Law). PDP Law was the first

[38] Nyoman Nidia Sari Hayati, Sri Warjiyati, and Muwahid, "Analisis Yuridis Konsep Omnibus Law Dalam Harmonisasi Peraturan Perundang-Undangan Di Indonesia," *Jurnal Hukum Samudra Keadilan* 16, no. 1 (June 2021): 4.

[39] Russell Smith and Penny Jorna, *Identity Crime and Misuse in Australia: Results of the 2016 Online Survey*, *Australian Institute of Criminology* (Canberra: Australian Institute of Criminology, 2018), 12.

comprehensive legal framework for data protection and, to date, remains the only comprehensive legal framework for data protection.[40]

Fortunately, the PDP Law does provide provisions that can actually be used as the legal basis for the protection of digital identity. To start, Article 1 number 1 states that Personal Data is data about an identified or identifiable individual individually or in combination with other information either directly or indirectly through electronic or non-electronic systems. The consolidation of the term 'identified or identifiable individual' here is crucial as it implicitly acknowledges digital identity as a part of personal data, which is a crucial development from the provision provided in the EIT Law. The PDP Law also provides a more comprehensive version of EIT Law's Article 9, through Article 5, which governs that the Personal Data Subject has the right to obtain information about the clarity of identity, the basis of legal interests, the purpose of the request and use of Personal Data, and the accountability of the party requesting Personal Data.

Most importantly, digital identity theft as a crime on its own and digital identity theft as an inchoate crime must also be separated. Digital identity theft, due to its connection to personal data, as highlighted previously, can simply be prevented and punished according to the PDP Law. However, the theft of data is a much more generalized conceptualization of a crime despite its wide array of implications. This goes back to the purpose of the crime itself, where digital identity theft can be punished the same way as data theft, which is often done by illegally selling or trading stolen data on the black market. On the other hand, digital identity theft, in its purest form, is often done to facilitate other crimes, such as fraud, by impersonating a person in the digital space to gain illicit access to private services such as online banking or many kinds of online business ventures.

Therefore, it's clear that the legal framework in Indonesia doesn't support what constitutes digital identity theft, which mainly involves impersonation. Impersonation itself is covered by Article 378 of the Criminal Law Code, which governs that any person who, with intent to unlawfully benefit himself or another, by means of a false name or false dignity, deceit, or a series of falsehoods, induces another person to deliver any property to him, or to give a debt or to cancel a debt, shall, being guilty of fraud, be punished by a maximum imprisonment of 4 years. However, it's important to note that this crime doesn't put stolen identity as one of its necessary elements, although normatively, there's no provision that has the capacity to separate identity theft from impersonation. Due to the complexity of its nature and its wide array of legal implications, the criminalization of digital identity theft must include both the misuse of someone's identity or impersonation and the theft of digital data that, when accumulated, can be used to identify someone.

The fact that these two aspects remain separated within the Indonesian legal framework highlights the inadequacy of dealing with digital identity theft. Moreover, it is also problematic for the Indonesian legal framework to rely mainly on criminal provisions regarding data theft, as it can have completely different implications. The separation of these aspects could've been reconciled if there was at least a provision within the Criminal Law Code specifically governing the issue of identity theft, even in the traditional sense. Therefore, establishing the legal basis for identity theft at general

[40] Admiral and Mega Ardina Pauck, "Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Service," *Lex Scientia Law Review* 7, no. 2 (2023): 1002.

is crucial to help prevent and prosecute identity theft, both in the traditional and the digital sense.

3.3. Proposed Model of Normative Development

In navigating the complex interplay between technological advancements and the law, a recurring challenge is balancing the rapid pace of digital innovation with the robustness and adaptability of legal frameworks. This challenge is particularly pronounced in the context of identity theft, an issue that has morphed into the digital age with its own unique legal implications. As our societal interactions and personal transactions are increasingly relying on digital platforms,[41] the legal system must evolve not only to address current inadequacies but also to prevent future abuses by consolidating important provisions that can provide a normative baseline. Though complex, the distinction between digital and traditional identity theft ultimately highlights a broader necessity for a responsive and anticipatory legal system. This is essential in safeguarding individuals' rights and identities in an ever-evolving digital landscape. Legal adaptation is also important in keeping up with cybercriminals, who also continually evolve to adapt to digital technology advancements.[42]

As highlighted previously, the Indonesian legal framework, as it currently stands, reveals certain gaps that need serious legislative attention, particularly in terms of clearly defining and distinctly handling digital identity theft as a crime. Despite existing legislation, such as the EIT Law and the PDP Law, there remains a significant need for specificity and enforceability. These laws provide a foundational structure upon which more nuanced regulations regarding data protection and data theft could be built, but they fail to properly address digital identity theft as a distinct crime due to the lack of support from the Criminal Law Code. By bringing key amendments to these frameworks, Indonesia can deter digital identity theft and significantly mitigate the risks associated with future technological developments.

Therefore, the distinct differences between digital identity theft and data theft must also be taken into account. This is because digital identity theft often involves more targeted manipulations of individual personas, whereas data theft can be broader, affecting massive datasets indiscriminately. Thus, by creating legal provisions that recognize and differentiate these offenses, the legal system can provide clearer, more effective guidelines and enforcement strategies tailored to protect individuals' digital lives, ensuring a more secure and trustworthy digital environment for all users. This research proposes a model of normative development that Indonesia can consider as a way to enhance its legal framework for the digital environment that specifically governs the act of digital identity theft.

Table 1 outlines a targeted approach to amending the Indonesian legal framework to address the intricacies of digital identity theft effectively. Due to its close relation to data protection, it might be best suited for these normative developments to be introduced within the data protection network, which is currently governed by the PDP Law and is about to be supported by an implementing decree that is currently in

---

[41] Zelina Pose, "Identity Verification: Ensuring Trust and Security in a Digital World," *Journal of Biometrics & Biostatistics* 14, no. 3 (2023): 1.

[42] Olukunle Oladipupo Amoo et al., "The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System," *World Journal of Advanced Research and Reviews* 21, no. 2 (2024): 206.

legislative development.[43] By defining digital identity and its theft with greater precision, the law can provide clear guidelines for enforcement and compliance, crucial for the legal system to be seen as a legitimate and effective protector of digital rights. An example of the basic norm regarding this can be taken from the United States, which, through 18 U.S.C. § 1028, makes it a crime to misuse someone's identifying information, whether personal or financial. Personal identifying information can include social security numbers, driver's license numbers, credit card or bank account information, and PIN numbers obtained through the internet. Building on this, the definition of digital identity theft to be covered by Indonesia must be able to consolidate the more complex nature of digital identity theft in current digital landscapes, which might involve further efforts of identification from a much more complex dataset while also maintaining the element of impersonation to ensure distinction from data theft. This is mainly because the provisions in the PDP Law currently focus on broad data protection and do not explicitly tackle the specifics of digital identity theft, such as the impersonation and fraudulent misuse of digital identities.

Table 1: Model of normative development

Aspect	Current Status	Proposed Enhancements
Legal Definitions	Ambiguous definitions of digital identity and its theft	Introduce precise legal definitions that differentiate between digital identity theft and other forms of data theft, directly addressing the nuances of digital interactions.
Penalties and Remedies	General penalties not specific to digital realms	Establish specific penalties and remedies for digital identity theft, enhancing deterrent effects and providing clear legal recourse for victims.
Verification Compliance	No verification methods or mechanisms are installed as a part of the broader data protection or electronic systems' legal compliance.	Update the current state of the legal compliance to include verification as a feature that has to be readily available on all digital platforms, along with mandatory verification for fintech platforms.
Overseeing Body	There is not a single body established by any law regarding data protection and electronic systems that can oversee the issues relevant to the digital environment.	Establish a body that can oversee digital issues to better identify new exploits that might be used by cybercriminals for many crimes, including identity theft.

As there's no existing provision regarding digital identity theft, the model also proposes a criminal provision that can put a distinction between data theft and digital identity theft by essentially outlining the element of impersonation and utilization of personal identification data for fraudulent purposes, and introducing heavier fines and jail time

[43] Bella Christine and Christine S.T. Kansil, "Hambatan Penerapan Perlindungan Data Pribadi Di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Syntax Literate; Jurnal Ilmiah Indonesia* 7, no. 9 (2023): 16334–16335.

as possible punishment than the provision of Article 65 jo. Article 67 of the PDP Law.[44] It's also imperative to add a verification mechanism as a part of the legal compliance for data protection. This preventive mechanism must be made available across all platforms and mandatory for some, particularly those within the fintech landscape. To support this, the PDP Law must also provide better provisions regarding data identification mechanisms to ensure the legal boundaries between lawful and unlawful identification methods of any datasets.

Lastly, the model also proposes the establishment of a government body to oversee the issues relevant to data protection, including digital identity theft. This body is important in providing a clear line of connection between the government and data subjects, particularly those with identifiable data, who are at risk of digital identity theft. It can also watch over many data protection practices to ensure a better level of compliance and subsequently lower the risk of identity theft that can stem from possible exploits within the digital environment. With this model, this research hopes that digital identity theft can be better prevented and punished more severely while raising awareness of the dangers of digital identity theft, which will become even more increasingly relevant as digital technology continues to develop.

4. CONCLUSION

This research ultimately argues that digital identity theft is a unique crime that must be normatively distinguished from impersonation, traditional identity theft, and data theft, as it has all elements of the three. Due to the fact that Indonesia's legal framework has been identified to be lacking in many aspects relevant to the effort to tackle digital identity theft, this research proposes a model of normative development. This model aims to introduce specific legal definitions that clearly differentiate between digital identity theft and other types of data theft while also establishing robust penalties and remedies tailored to the unique challenges of the digital realm. Additionally, the model proposes the inclusion of mandatory verification mechanisms across all digital platforms and the establishment of a dedicated oversight body to proactively monitor and address emerging threats in the digital landscape, ensuring a responsive and adaptive legal system. Ultimately, this study expands the Indonesian legal understanding of identity theft by proposing a distinct theoretical framework for digital identity theft, which necessitates the development of specific legal norms and definitions to address the unique aspects of identity misuse in the digital age. Further research is needed to address this study's limitation, which arises from its reliance solely on normative analysis. Incorporating qualitative methods such as interviews or surveys of victims of digital identity theft could provide practical insights and validate the effectiveness of the proposed model.

[44] Article 65 of the PDP Law governs that it is unlawful for any person to obtain or collect personal data that does not belong to them with the intention of benefiting themselves or others, which may result in harm to the data subject. It is also illegal for any person to unlawfully disclose or use personal data that does not belong to them. Article 67 governs the criminal punishments, respectively, assigning up to five years in prison and/or a fine of up to IDR 5 billion for unlawfully obtaining or collecting personal data not one's own, up to four years in prison and/or a fine of up to IDR 4 billion for unlawfully disclosing such data, and again up to five years in prison and/or a fine of up to IDR 5 billion for using personal data unlawfully. Law No. 27 of 2022 on Personal Data Protection.

5. REFERENCES

Journal Article:

Admiral, Admiral, and Mega Ardina Pauck. "Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Service." *Lex Scientia Law Review* 7, no. 2 (2023): 995–1048. https://doi.org/10.15294/lesrev.v7i2.77881.

Alagna, Vincent. "A Comparative Analysis of Identity Theft within America and Australia." *Criminal Justice* Spring 5 (2020): 1–21, https://scholarsarchive.library.albany.edu/honorscollege_cj/24/.

Alhelaly, Yasser, Gurpreet Dhillon, and Tiago Oliveira. "When Expectation Fails and Motivation Prevails: The Mediating Role of Awareness in Bridging the Expectancy-Capability Gap in Mobile Identity Protection." *Computers & Security* 134 (2023): 1–20. https://doi.org/https://doi.org/10.1016/j.cose.2023.103470.

Amoo, Olukunle Oladipupo, Akoh Atadoga, Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Femi Osasona, and Benjamin Samson Ayinla. "The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System." *World Journal of Advanced Research and Reviews* 21, no. 2 (2024): 205–17. https://doi.org/10.30574/wjarr.2024.21.2.0438.

Bahadur, Kunwar Surendra. "A Brief Study On Negative Effects of Social Media On Youth." *Bayan College International Journal of Multidisciplinary Research* 1, no. 2 (2021): 1–17, https://bayancollegeijmr.com/index.php/ijmr/article/view/42.

Boos, Eric S, Chandler Givens, and Nick Larry. "Damages Theories in Data Breach Litigation." *Sedona Conference Journal* 16 (2015): 125–50. https://doi.org/10.2139/ssrn.2516941.

Cassim, Fawzia. "Protecting Personal Information in the Era of Identity Theft: Just How Safe Is Our Personal Information from Identity Thieves?" *Potchefstroom Electronic Law Journal* 18, no. 2 (2015): 69–110. https://doi.org/10.4314/pelj.v18i2.02.

Christine, Bella, and Christine S.T. Kansil. "Hambatan Penerapan Perlindungan Data Pribadi Di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Syntax Literate ; Jurnal Ilmiah Indonesia* 7, no. 9 (2023): 16331–39. https://doi.org/10.36418/syntax-literate.v7i9.13936.

Cross, Cassandra, and Rebecca Layt. "'I Suspect That the Pictures Are Stolen': Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities." *Social Science Computer Review* 40, no. 4 (2022): 955–73. https://doi.org/10.1177/0894439321999311.

Disanto, Philip F. "Blurred Lines of Identity Crimes: Intersection of the First Amendment and Federal Identity Fraud." *Columbia Law Review* 115, no. 4 (2015): 941–82, https://columbialawreview.org/content/blurred-lines-of-identity-crimes-intersection-of-the-first-amendment-and-federal-identity-fraud-2/.

Disemadi, Hari Sutra. "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies." *Journal of Judicial Review* 24, no. 2 (2022): 289–304. https://doi.org/10.37253/jjr.v24i2.7280.

Friedman, AR, and LD Wagoner. "The Need for Digital Identity in Cyberspace Operations." *Journal of Information Warfare (JIW)* 13, no. 2 (2014): 42–52, https://www.jstor.org/stable/26487493.

Giannopoulou, Alexandra. "Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity." *Digital Society* 2, no. 2 (2023): 18–37. https://doi.org/10.1007/s44206-023-00049-z.

Goh, Samuel H., Paul M. Di Gangi, Julio C. Rivera, and James L. Worrell. "Graduate Student Perceptions of Personal Social Media Risk: A Comparison Study." *Issues In Information Systems* 17, no. IV (2016): 109–19. https://doi.org/10.48009/4_iis_2016_109-119.

Grindstaff, R. Andrew. "Article III Standing, the Sword and the Shield: Resolving a Circuit Split in Favor of Data Breach Plaintiffs." *William & Mary Bill of Rights Journal* 29, no. 3 (2021): 851–82, https://scholarship.law.wm.edu/wmborj/vol29/iss3/9/.

Hayati, Nyoman Nidia Sari, Sri Warjiyati, and Muwahid. "Analisis Yuridis Konsep Omnibus Law Dalam Harmonisasi Peraturan Perundang-Undangan Di Indonesia." *Jurnal Hukum Samudra Keadilan* 16, no. 1 (June 2021): 1–18. https://doi.org/10.33059/jhsk.v16i1.2631.

Judijanto, Loso, Bhaswarendra Guntur Hendratri, Sabil Mokodenseho, Tania Prinita Aulia Mamonto, and Annisa Mokoginta. "Analysis of the Influence of Social Media Use, Educational Technology, and Digital Identity on Educational Culture Change in West Java." *West Science Social and Humanities Studies* 2, no. 3 (March 2024): 373–82. https://doi.org/10.58812/wsshs.v2i03.703.

Li, Yuan, Adel Yazdanmehr, Jingguo Wang, and H Raghav Rao. "Responding to Identity Theft: A Victimization Perspective." *Decision Support Systems* 121 (2019): 13–24. https://doi.org/https://doi.org/10.1016/j.dss.2019.04.002.

Lupton, Deborah. "The Internet of Things: Social Dimensions." *Sociology Compass* 14, no. 4 (2020): 1–13. https://doi.org/10.1111/soc4.12770.

Mudzalifah, Milla, and Pujiyono Pujiyono. "The Politics of Criminal Law in Cybercrime: An Efforts to Combat Information Technology Crimes in Indonesia." *Jurnal Pembaharuan Hukum* 10, no. 1 (2023): 77-89. http://dx.doi.org/10.26532/jph.v10i1.26707.

New, Kuwihoi, and ZianXiang Kong. "Exploring Teenage Awareness of Social Media Fraud in Malaysia." *International Journal of Academic Research in Business and Social Sciences* 13, no. 12 (2023): 463–500. https://doi.org/10.6007/ijarbss/v13-i12/19859.

Parate, Sachin, Hari Prasad Josyula, and Latha Thamma Reddi. "Digital Identity Verification: Transforming KYC Processes in Banking Through Advanced Technology and Enhanced Security Measures." *International Research Journal of Modernization in Engineering Technology and Science* 5, no. 9 (2023): 128–37. https://doi.org/10.56726/irjmets44476.

Pose, Zelina. "Identity Verification: Ensuring Trust and Security in a Digital World." *Journal of Biometrics & Biostatistics* 14, no. 3 (2023): 1–2, https://www.hilarispublisher.com/open-access/identity-verification-ensuring-trust-and-security-in-a-digital-world-100129.html.

Rasyid, Muh. Fadli Faisal, Muh. Akhdharisa SJ, Karlin Z. Mamu, Saptaning Ruju Paminto, Wahab Aznul Hidaya, and Abdennour Hamadi. "Cybercrime Threats and Responsibilities: The Utilization of Artificial Intelligence in Online Crime." *Jurnal Ilmiah Mizani: Wacana Hukum, Ekonomi Dan Keagamaan* 11, no. 1 (April 2024): 49–63, http://dx.doi.org/10.29300/mzn.v11i1.3318.

Ruziev Rustam, Ruziev, Abduvaliev Bokhadir, and Rakhmatov Uktam. "An Overcoming the Privacy Paradox: Legal Aspects of Data Protection in the Digital Age." *International Journal of Cyber Law* 1, no. 4 (June 2023): 1–22. https://doi.org/10.59022/ijcl.47.

Sarfi, Majid, Morteza Darvishii, and Mostafa Zohouri. "Why People May View Online Crimes as Less Criminal: Exploring the Perception of Cybercrime." *International*

E-Journal of Criminal Sciences, no. 18 (2023): 1–17. https://doi.org/10.1387/inecs.25097.
Sarkar, Gargi, and Sandeep K Shukla. "Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies." *Journal of Economic Criminology* 2 (2023): 1–26. https://doi.org/https://doi.org/10.1016/j.jeconc.2023.100034.
Savelyev, Alexander. "The Inadequacy of Current Remedies for Violation of Data Subjects' Rights and How to Fix It." *Legal Issues in the Digital Age* 2, no. 2 (2020): 24–62. https://doi.org/10.17323/2713-2749.2020.2.24.62.
Sedlmeir, Johannes, Reilly Smethurst, Alexander Rieger, and Gilbert Fridgen. "Digital Identities and Verifiable Credentials." *Business & Information Systems Engineering* 63, no. 5 (2021): 603–13. https://doi.org/10.1007/s12599-021-00722-y.
Sembiring, Patricia Edina, Ahmad M. Ramli, and Laina Rafianti. "Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik." *Veritas et Justitia* 10, no. 1 (June 29, 2024): 127–52. https://doi.org/10.25123/vej.v10i1.7622.
Siregar, Gomgom, and Sarman Sinaga. "The law globalization in cybercrime prevention." *International Journal of Law Reconstruction* 5, no. 2 (2021): 211-227. http://dx.doi.org/10.26532/ijlr.v5i2.17514.
Solove, Daniel J. "The Myth of the Privacy Paradox." *George Washington Law Review* 89, no. 1 (2021): 1–51. https://doi.org/10.2139/ssrn.3536265.
Tan, David. "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum." *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 1332–36. http://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/5601.
Vilić, Vida. "Users' Considerations About Possibilities of Self-Protection on Social Networks." *Open Journal for Legal Studies* 1, no. 1 (2018): 9–24. https://doi.org/10.32591/coas.ojls.0101.02009v.
Wang, Fennie, and Primavera De Filippi. "Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion." *Frontiers in Blockchain* 2 (2019): 1–22. https://doi.org/10.3389/fbloc.2019.00028.
Wang, Yanshu. "Realistic Dilemma and Path Optimization of Online Personal Information Protection." *Lecture Notes in Education Psychology and Public Media* 39, no. 1 (2024): 187–92. https://doi.org/10.54254/2753-7048/39/20240728.
Wu, Hong, and Wenxiang Zhang. "Digital Identity, Privacy Security, and Their Legal Safeguards in the Metaverse." *Security and Safety* 2 (2023): 1–14. https://doi.org/10.1051/sands/2023011.
Wyre, Megan, David Lacey, and Kathy Allan. "The Identity Theft Response System." *Trends and Issues in Crime and Criminal Justice*, no. 592 (2020): 1–18. https://doi.org/10.52922/ti04299.

Book:

Franks, Christie, and Russell Smith. *Identity Crime and Misuse in Australia 2019*. *Australian Institute of Criminology*. Canberra: Australian Institute of Criminology, 2020. https://doi.org/10.52922/sr04749.
Smith, Russell, and Penny Jorna. *Identity Crime and Misuse in Australia: Results of the 2016 Online Survey*. *Australian Institute of Criminology*. Canberra: Australian Institute of Criminology, 2018. https://doi.org/10.52922/sr228798.

Conference Proceeding:

Helser, Susan. "FIT: Identity Theft Education: Study of Text-Based versus Game-Based

Learning." In *International Symposium on Technology and Society, Proceedings*, 2016-March:1–4, 2016. https://doi.org/10.1109/ISTAS.2015.7439437.

Jibril, Abdul Bashiru, Michael Adu Kwarteng, Fortune Nwaiwu, Christina Appiah-Nimo, Michal Pilik, and Miloslava Chovancova. "Online Identity Theft on Consumer Purchase Intention: A Mediating Role of Online Security and Privacy Concern." In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Vol. 12067 LNCS, 2020. https://doi.org/10.1007/978-3-030-45002-1_13.

Soemarwi, Vera W. S., and W. Susanto. "Digital Technology Information in Indonesia: Data Privacy Protection Is a Fundamental Right." In *Proceedings of the International Conference on Economics, Business, Social, and Humanities (ICEBSH 2021)*, 570:561–66, 2021. https://doi.org/10.2991/assehr.k.210805.088.

Web Page:

Sando, Suzanne. "2024 Identity Fraud Study: Resolving the Shattered Identity Crisis." *Javelin*, April 10, 2024. https://www.javelinstrategy.com/research/2024-identity-fraud-study-resolving-shattered-identity-crisis.