|Jurnal Ilmu Komputer dan Sistem Informasi |JIKSI|Vol. 5| No. 1|Feb|Year 2024|

A Literature Study: Ethical Problems in Information Technology in Identity Theft Cases

M. Yonandio Lazuardi[1*]

Abstract

Identity theft has become a major ethical and security issue in the digital era. The widespread use of information technology has enabled offenders to exploit personal information with increasing sophistication. Identity theft occurs when an individual's personal data such as name, address, date of birth, or bank information is stolen and used without consent, often resulting in financial and reputational damage. This study identifies and analyzes ethical concerns arising from identity theft, emphasizing privacy violations and misuse of customer data. Using a literature study method, this paper reviews prior research on the causes, impacts, and mitigation of identity theft within the context of information ethics. The findings highlight that identity theft stems not only from technical vulnerabilities but also from moral negligence and weak regulatory enforcement. Strengthening data-protection policies, promoting digital ethics, and raising public awareness are essential steps toward reducing such crimes and preserving trust in information systems.

Keywords

Identity Theft; Data Security; Privacy Protection; Information Ethics; Cybercrime

Article History

Received 01 November 2023
Accepted 01 February 2024

How to Cite

Lazuardi, M.Y, (2024). A Literature Study: Ethical Problems in Information Technology in Identity Theft Cases, (JIKSI), 5(1), [8-14].

[1*] Universitas Bina Darma, Indonesia, Corresponding email: myonandio@gmail.com

Introduction

Technological innovation has profoundly transformed human civilization, reshaping how individuals communicate, learn, transact, and govern. The integration of digital systems into daily life has created an interconnected world where information flows rapidly across geographical and institutional boundaries. This transformation has brought tremendous benefits—enhancing efficiency, productivity, and accessibility in communication, education, business, and public administration. In essence, technology has become a catalyst for socio-economic development and global integration. However, the same innovations that empower society also introduce new forms of vulnerability, giving rise to crimes and ethical violations that exploit the digital environment for malicious intent. Among the most pervasive and damaging of these is identity theft, a crime that involves the unlawful acquisition and misuse of personal information for deceptive or fraudulent purposes (Rebovich et al., 2015).

Identity theft represents a fundamental breach of trust in digital interactions. It threatens not only financial security but also psychological well-being and personal dignity. Victims may suffer significant financial losses, emotional distress, and reputational harm as their identities are exploited by perpetrators for personal gain. The perpetrators of such crimes often operate under the protection of anonymity provided by cyberspace, which allows them to conceal their digital footprints and evade accountability. Mahmud (2019) notes that the virtual nature of cyberspace enables offenders to act with minimal fear of detection or punishment, creating a persistent challenge for law enforcement and policymakers. The borderless character of digital crime complicates jurisdictional authority and raises questions about how ethical and legal norms can effectively govern a virtual, transnational domain.

In practice, identity theft frequently occurs through data aggregation—a process in which perpetrators collect fragmented pieces of personal data such as full names, national identification numbers, contact information, and social media details from various online sources. These fragments are then compiled into a comprehensive digital profile that can be used for fraudulent transactions, phishing scams, or impersonation (Sudama et al., 2020). This method reflects how seemingly trivial data disclosures, when combined and analyzed, can yield powerful insights into individuals' digital identities. As digital footprints become increasingly traceable, the risk of identity misuse grows proportionally, particularly when individuals and organizations fail to apply adequate data protection measures.

The threat of identity theft manifests in two primary dimensions. The first is individual identity theft, in which the personal data of specific individuals are stolen and exploited for economic or social manipulation—such as fraudulent financial transactions, unauthorized access to accounts, or damage to personal reputation. The second is organizational identity theft, where institutions or corporations become targets of large-scale cyberattacks, leading to massive data breaches, erosion of public trust, and substantial financial loss. Such incidents not only endanger institutional credibility but also compromise the privacy of thousands, if not millions, of data subjects.

Beyond its legal ramifications, identity theft poses profound ethical challenges. Misusing another person's personal data violates core moral principles of honesty, fairness, and respect for autonomy. It undermines the fundamental human right to privacy, which is integral to personal dignity and freedom in the digital age. From an ethical perspective, identity theft represents both an individual failure—on the part of the offender—and a systemic failure—on the part of organizations that neglect to secure user data adequately. The moral responsibility thus extends beyond perpetrators to include corporations and government

entities tasked with protecting citizens' digital identities. In this context, ethical governance of information systems becomes not merely a technical obligation but a moral imperative.

This study therefore aims to examine the ethical dimensions of identity theft within the field of information technology, exploring how digital misconduct undermines moral responsibility and social trust. It emphasizes the urgent need for preventive measures grounded in ethical awareness, robust governance frameworks, and consistent legal enforcement. By analyzing both the ethical and legal aspects of identity theft, this research seeks to contribute to the broader discourse on digital ethics, data protection, and the moral accountability of individuals and institutions in the information society.

Methodology

This study employed a qualitative literature-based research approach, which relies on the systematic collection, evaluation, and interpretation of secondary data from credible academic sources. Such an approach is appropriate for exploring conceptual and normative issues—such as the ethical and legal implications of identity theft—that require in-depth theoretical understanding rather than empirical measurement. According to Arikunto (2013), a literature study is a structured process of analyzing existing written works to construct conceptual frameworks, identify research gaps, and synthesize prior findings to generate new insights. This methodological orientation enables researchers to develop a holistic understanding of complex phenomena by integrating multiple scholarly perspectives.

The data sources in this study consisted primarily of books, peer-reviewed journal articles, conference papers, and previous research discussing themes of information ethics, data privacy, cybercrime, and identity theft. Official documents, such as government regulations and international guidelines on cybersecurity, were also reviewed to provide contextual depth regarding the legal and policy dimensions of the topic. The inclusion of diverse secondary sources ensured that the analysis was grounded in both theoretical discourse and real-world regulatory practice.

The analytical process in this study followed three systematic stages designed to ensure rigor, coherence, and comprehensiveness:

1. Data Collection.
   The first stage involved identifying and gathering scholarly publications relevant to key concepts such as identity theft, information ethics, digital privacy, and cybercrime governance. Databases such as Google Scholar, Scopus, and national repositories were used to locate academic literature published within the last decade, complemented by foundational works that established the conceptual basis for ethical analysis in information systems. Selection criteria emphasized source credibility, recency, and thematic relevance to ensure analytical validity.
2. Critical Review and Theoretical Framing.
   In the second stage, the selected materials were systematically reviewed to extract theories and models explaining ethical violations and digital misconduct. This included frameworks of ethical responsibility, information morality, and socio-technical perspectives on privacy. The theoretical review provided a foundation for interpreting how technological advancement interacts with human values and institutional governance. It also allowed for identifying recurring ethical

dilemmas—such as negligence in data protection and misuse of personal information—that underlie cases of identity theft.

3. Synthesis and Conceptual Integration
   The final stage involved synthesizing insights from the reviewed literature to identify critical factors contributing to the emergence of identity theft in digital environments. These factors were then categorized into ethical, technical, and regulatory dimensions to facilitate a comprehensive understanding of the issue. Based on this synthesis, the study formulated preventive measures emphasizing the integration of ethical awareness, digital literacy, and institutional responsibility. The results were presented in a narrative-descriptive form, consistent with the qualitative nature of the research.

By adopting this literature-based qualitative design, the study not only consolidates existing academic knowledge but also provides a normative framework for addressing ethical and legal challenges in digital identity management. This methodological approach ensures that the discussion remains conceptually grounded, contextually relevant, and theoretically robust, allowing the findings to contribute meaningfully to the broader discourse on information ethics and cybersecurity governance.

Results and Discussion

Ethical Issues in Information Technology

Ethical violations in information technology emerge when digital practices conflict with established moral or professional standards. Kumalasari (2021) categorizes common ethical breaches in IT as follows:

1. Unauthorized Access: Illegally entering computer systems to obtain confidential information.
2. Illegal Content: Disseminating false, immoral, or prohibited material online.
3. Data Forgery: Manipulating or falsifying electronic data.
4. Cyber Espionage: Conducting digital surveillance for illicit gain.
5. Cyber Sabotage and Extortion: Damaging systems and demanding ransom for restoration.
6. Intellectual-Property Infringement: Copying or distributing creative works without consent.
7. Privacy Violation: Collecting or exposing personal data without authorization.
8. Carding: Engaging in credit-card fraud through stolen data.
9. Denial-of-Service (DoS) Attacks: Overloading servers to disrupt access.
10. Hate Sites: Publishing content promoting hostility or discrimination.
11. Cyberstalking: Harassing individuals through persistent online contact.
12. Hacking and Cracking: Unauthorized exploration or exploitation of systems.
13. Fraud: Misrepresentation for unlawful financial benefit.
14. Online Gambling and Pornography: Engaging in prohibited digital activities.

Although privacy infringement and identity theft may appear similar, the former often arises from internal misuse of data, while the latter typically involves external actors stealing personal information for criminal purposes.

Ethical Issues in E-Commerce

Ethical problems also emerge in e-commerce, where customers routinely share personal and financial information. Rahmawati (2020) notes that inadequate data-protection policies

and weak system security often result in privacy breaches. Such conditions facilitate identity theft through unauthorized access to user credentials.

To mitigate these risks, governments and organizations must implement comprehensive cybersecurity regulations, enforce data-protection compliance, and educate employees on secure data-handling practices.

Types of Identity Theft

Mahmud (2019) classifies identity theft into five main categories: Criminal Identity Theft: Using another person's identity while committing crimes, causing wrongful accusations against the victim.Financial Identity Theft: Exploiting someone's personal data to access bank accounts or obtain credit illegally.Identity Cloning: Assuming another person's identity for personal gain, leading to reputational harm.Medical Identity Theft: Using another individual's medical insurance for unauthorized healthcare services.Child Identity Theft: Stealing minors' identities for fraudulent activities, often undetected until adulthood.

Privacy Risks on Social Media

Leona et al. (2021) identified social-media platforms as a primary source of privacy exposure. Users often reveal personal information publicly, which cybercriminals can easily exploit. To enhance privacy, users should: Configure and review privacy settings regularly. Limit disclosure of personal identifiers. Restrict connections to trusted contacts. Avoid suspicious links and advertisements. Employ strong, unique passwords for each platform.

Identity Theft in Educational Institutions

Briones et al. (2013) documented a case of identity theft involving a university's wireless network. Attackers created a fake login portal mimicking the university's official page to harvest students' credentials. Many victims reused the same passwords on other accounts, resulting in extensive data compromise.This case underscores the importance of institutional responsibility in maintaining network security and providing cybersecurity education to all users.

Contributing Factors

Rahayu and Nasution (2023) and Luthiya et al. (2021) identify several root causes of identity theft in Indonesia: Low public awareness of data-protection rights. Weak security infrastructure and inadequate encryption. Limited law-enforcement capacity. Absence of comprehensive personal-data-protection legislation. Collectively, these factors reveal that identity theft is a multifaceted issue involving ethical lapses, regulatory gaps, and technological vulnerabilities.

Discussion

The ethical dimensions of identity theft extend beyond the act of stealing data. They involve broader questions of moral responsibility, institutional accountability, and respect for digital privacy. From an ethical standpoint, individuals and organizations are obliged to safeguard data entrusted to them. Negligence in doing so constitutes not merely a technical failure but a breach of public trust.

Furthermore, cultural attitudes toward data sharing in online environments contribute to the persistence of this problem. Many users underestimate the risks associated with revealing personal details on social media or unverified platforms. Consequently, preventive education and ethical awareness campaigns are crucial to fostering responsible digital behavior.

From a policy perspective, Indonesia's evolving legal framework for cybersecurity must prioritize personal-data protection. Effective governance requires collaboration between

government agencies, educational institutions, and private-sector entities to enforce ethical and legal standards consistently.

Conclusion and Recommendations

Identity theft represents both a technological and ethical crisis in the digital era. It violates individual privacy, erodes public trust, and threatens the moral foundation of information systems. The literature reveals that inadequate cybersecurity, low ethical awareness, and insufficient legal protection are primary enablers of this crime. To mitigate these risks, institutions must implement robust data-security mechanisms, governments must strengthen data-protection laws, and individuals must cultivate ethical awareness regarding information sharing. Sustainable solutions require integrating technical safeguards with ethical education to create a responsible and secure digital society.

Disclosure Statement

The author declares no conflict of interest regarding the research, authorship, or publication of this article.

Acknowledgments

The author expresses sincere gratitude to Universitas Bina Darma, Palembang, for academic supervision and to all scholars whose prior research contributed to this study.

References

Arikunto, S. (2013). Research Procedure: A Practical Approach. Jakarta: Rineka Cipta.

Artiningsih, A., & Sasmita, A. S. (2016). Data breaches and identity theft: A case study of U.S. retailers and banking. Jurnal Paramadina, 13, 1476–1496.

Briones, M., Coronel, A. M., & Chavez-Burbano, P. (2013). Case study: Identity theft in a university WLAN. WCCIT. IEEE.

Irshad, S., & Soomoro, T. R. (2018). Identity theft and social media. International Journal of Computer Science and Network Security, 18(1), 43–55.

Kumalasari, V. (2021). Professional Ethics in Information Technology. Semarang: Yayasan Prima Agus Teknik.

Leona, N. E., Anisa, N. C., Ni Putu, J. M., & Aisha, R. I. S. (2021). Awareness of privacy threats and privacy protection behavior in social-media use. Proceedings of the National Seminar on Technology and Information Systems, 101–109.

Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Criminal-law policy on regulating personal-data theft as misuse of information technology. Jurnal Hukum Pidana & Kriminologi, 2(2), 14–29.

Mahmud, R. (2019). Identity-theft categories and cases. CyberSecurity and Digital Forensics, 2(1), 38–42.

Maskun. (2013). Cybercrime. Jakarta: Kencana Pieter.

Rahayu, D. R., & Nasution, M. I. P. (2023). Policy to prevent personal-data theft in electronic media. JSIT, 3(2), 263–266.

Rahmawati, N. (2020). Data breaches and identity theft in e-commerce. CyberSecurity and Digital Forensics, 3(1), 7–13.

Rebovich, D. J., Allen, K., & Platt, J. (2015). The New Face of Identity Theft. Center for Identity Management and Information Protection (CIMIP).

Reynolds, G. W. (2014). Ethics in Information Technology (5th ed.). Boston, MA: Cengage Learning.

Ryano, A. (2008). Bridging theory and application: Learning from social-networking-site issues. Institut Teknologi Bandung.

Sudama, W. I., Imanto, A. I., Wijayanti, S. W., Agustini, T. Y., & Fatoni, Z. (2020). The influence of identity-theft risk and risk perception on online-shopping intention. IBR, 3(2), 180–196.

Biographical Notes

M. YONANDIO LAZUARDI is a postgraduate student in the Master of Information Technology Program at Universitas Bina Darma, Palembang. His research focuses on information ethics, cybersecurity, and data-privacy issues, particularly the moral and legal aspects of identity theft in the digital era.