Journal of Multidisciplinary Academic and Practice Studies (JoMAPS)
ISSN 2656-2359, Vol 2, No 3, 2024, 261-265 *https://doi.org/10.35912/jomaps.v2i3.2219*

Cyber law analysis of E-KTP data leakage: A case approach of 102 million KTP data allegedly leaked from the Ministry of Social Affairs to a hacker forum

Richart Sahatatua[1], Yenrizka Gusmaria[2], I Ketut Astawa[3], Ade Maman Suherman[4], Try Setiady[5], Wahyu Donri Tinambunan[6]
Universitas Singaperbangsa Karawang, Indonesia[1-6]
manurungrichart@gmail.com[1], ygusmaria@gmail.com[2], ketut.astawa@fh.unsika.ac.id[3], Ade.maman@fh.unsika.ac.id[4], tri.setiady@fh.unsika.ac.id[5], wahyu.donri@fh.unsika.ac.id[6]

Article History
Received on 30 May 2024
1st revision on 9 June 2024
Accepted on 17 June 2024

Abstract:
Purpose: The Identity Card (KTP) is a personal identification document mandatory for all Indonesian citizens. The Indonesian government, through Law No. 24 of 2013 on Population Administration and its implementing regulation, Permendagri No. 73 of 2022, regulates the detailed recording of identity in population documents to ensure official registration and protection of every citizen's identity. However, the issue of data leakage has become increasingly urgent in today's digital era. The case of the leak of 102 million KTP data from the Ministry of Social Affairs (Kemensos) raises significant concerns regarding the privacy and security of individual data. This data leak, allegedly spread on a hacker forum, highlights the vulnerabilities of the government's information technology infrastructure.
Method: This research employs a document analysis method, collecting information from primary and secondary sources, including news reports, laws, and regulations related to data security, as well as case studies on cybercrime. An interdisciplinary approach is used, combining literature from law, information technology, and cybersecurity to gain a comprehensive understanding of the legal challenges in the E-KTP data leak case.
Results: The findings emphasize the importance of strengthening regulations, raising public awareness, and enforcing strict legal measures to protect personal data. This research aims to provide insights into improving personal data protection and information security in Indonesia, offering recommendations for enhancing the protection of citizens' data in the future.
Keywords: *Data Protection, Cybersecurity, E-KTP, Legal Analysis, Information Security*
How to Cite: Sahatatua, R., Gusmaria, Y., Astawa, I. K., Suherman, A. M., Setiady, T., & Tinambunan, W. D. (2024). Cyber law analysis of E-KTP data leakage: A case approach of 102 million KTP data allegedly leaked from the Ministry of Social Affairs to a hacker forum. *Journal of Multidisciplinary Academic and Practice Studies*, 2(3), 261-265.

1. Introduction

The identity card (KTP) is a personal identity data that must be owned by every Indonesian citizen. The Indonesian government through Law No. 24 of 2013 on Population Administration and its implementing regulation, Permendagri No. 73 of 2022, regulates in detail the recording of identity in population documents. This regulation aims to ensure that every citizen is officially registered and their identity is well protected (Ukwuoma, Cirman, & Oye, 2022).

However, in today's digital era, the issue of data leakage is becoming increasingly urgent. Personal data security is a major concern as this data can be misused for various crimes such as identity theft, fraud, and other illegal activities. The case of ID card data leaks, especially those involving large scales such as the leak of 102 million ID card data from the Ministry of Social Affairs (Kemensos) of the Republic of Indonesia, raises serious concerns about the privacy and security of individual data (Oranefo & Egbunike, 2021).

The leak was allegedly spread on a hacker forum, which shows that the information technology infrastructure used by government agencies is still vulnerable to cyber-attacks. This case not only harms individuals whose personal data was leaked, but also tarnishes the government's credibility in managing sensitive data.

In this context, it is important to understand the legal implications of the E-KTP data leak as well as the government's responsibility in protecting citizens' data. A cyber law analysis of this data leak case is highly relevant to explore how existing regulations are applied and what can be done to improve the data security system. Through this research, it is hoped to provide better insight into personal data protection and information security in Indonesia, as well as provide recommendations to improve the protection of citizens' data in the future.

2. Literature review

The literature used in this research covers a wide range of sources relevant to understanding the context of cyber law, personal data protection and public policy related to information security. This research combines national laws, international regulations, case studies, and a review of the development of cyber law and public policy in the government sector. The following are some of the key literatures that form the basis of this research:

2.1 Law No. 11/2008 on Electronic Information and Transactions (UU ITE)

The ITE Law provides a strong legal basis for protecting electronic data in Indonesia. It regulates various aspects of the use of information technology and electronic transactions, including provisions on the protection of personal data. Personal data in this context includes information contained in the E-KTP. Government Regulation No. 71/2019 on the Implementation of the EIT Law further stipulates the obligation for data owners and electronic system providers to protect the confidentiality, integrity, and availability of personal data (Djafar, 2019).

2.2 International Regulations

This study also covers relevant international regulations, such as the General Data Protection Regulation (GDPR) in the European Union. The GDPR is one of the most comprehensive personal data protection regulations in the world, providing strict guidelines on how personal data should be collected, stored and processed. GDPR emphasises on data protection principles such as lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. It also provides significant rights to individuals, such as the right to access their data, the right to be forgotten, and the right to restrict data processing. The implementation of GDPR in various countries shows the importance of strict regulations and effective law enforcement in protecting personal data (Adelika & Nurbaiti, 2023).

2.3 Case Studies and Overview of Cyber Law Developments

This research reviews various data leakage case studies in different countries to understand how cyber law is applied and the challenges faced in law enforcement against cybercrime. The data breach case studies in the United States, the European Union, and Asia provide valuable perspectives on the different approaches used to address data breaches and protect personal data. For example, the Target Corporation data breach case study in the United States demonstrated the importance of proactive security measures and rapid response in dealing with data breach incidents (Yudistira & Ramadani, 2023). In the European Union, the British Airways data leak case underlined the severe legal consequences and significant fines for companies that fail to protect personal data.

2.4 Public Policy on Cyber Security in the Public Sector

Literature on public policies related to cyber security in the public sector is also reviewed in this research. The main focus is on how government agencies manage and protect the sensitive data they hold. The study reviewed various policies and best practices in the management of sensitive data within the government. For example, the policies and procedures implemented by the Singapore government in protecting the personal data of its citizens show the importance of a holistic approach that includes strict regulations, training and awareness among government employees, and investment in information security technology (Riyadi & Suriaatmadja, 2023). This study also highlights the importance of co-operation between the public and private sectors in creating a strong cyber security environment.

2.5 Additional Regulations and Related Literature

In addition to the primary sources mentioned above, this study also reviewed additional relevant regulations and literature, such as:

1. Law No. 27 of 2022 on Personal Data Protection. This law provides more specific protection for personal data in Indonesia, establishing rights and obligations for data owners and electronic system providers, as well as sanctions for data protection violations (Djafar, 2019). Cyber Law Books and Journals: Works such as "Criminal Offences of Information & Electronic Transactions" by Chazawi and Ferdian provide in-depth insights into the legal aspects of cyber in Indonesia (Ferdian & Chazawi, 2015).
2. Journal Articles and Case Study Reports Articles such as "Twitter Sentiment Analysis of Personal Data Protection with Machine Learning Approach" by Nursiyono and Huda, and "Legal Protection of PT PLN's Consumer Personal Data Leak" by Riyadi and Suriaatmadja add depth to analyses on personal data protection and information security (Nursiyono & Huda, 2023).

By combining various literature sources from various disciplines, this research aims to provide a holistic understanding of the cyber legal challenges faced in handling the E-KTP data leak. In addition, this research also seeks to provide useful insights for the development of policies and law enforcement strategies that are more effective in protecting people's personal data from cyber threats.

3. Methodology

This research uses document analysis method by collecting information from primary and secondary sources such as news reports, laws and regulations related to data security, as well as case studies related to cybercrime. An interdisciplinary approach is also used by combining literature from the fields of law, information technology, and cyber security to gain a comprehensive understanding of the legal challenges faced in this E-KTP data leak case.

4. Results and discussions

4.1 Legal Protection of Personal Data in the Context of E-KTP Data Leakage

Legal protection of personal data is crucial in this digital era, especially in the case of the leak of 102 million ID card data from the Ministry of Social Affairs. Law No. 11/2008 on Electronic Information and Transactions (ITE Law) provides a strong legal basis to protect electronic data in Indonesia. However, its implementation still faces challenges such as a lack of awareness and understanding among the public and government institutions. Leakage of E-KTP data can result in various negative consequences, including identity abuse, fraud, and other crimes that can harm individuals and society at large (Djafar, 2019).

To overcome this challenge, concrete steps are needed such as raising awareness about the importance of data privacy, strengthening regulations, and strict law enforcement. Raising public awareness about the importance of personal data protection can be done through educational campaigns and training for the public and government employees. Strengthening regulations is also important to ensure that existing laws are comprehensive enough to address various forms of cybercrime. Strict law enforcement against personal data protection violations will provide a deterrent effect for criminals and strengthen public confidence in the existing legal system (Putri, Syamsu, & Triono, 2024).

4.2 Cyber Law Implications for Government Agencies

The Ministry of Social Affairs and other government agencies have a legal obligation to protect sensitive data such as E-KTP. Data leaks can lead to serious legal consequences, including civil and criminal liability and public prosecution that can undermine public trust in the credibility and integrity of government agencies. In this context, it is important for government agencies to update their information security policies and systems to deal with increasingly complex cyber security threats (Riyadi & Suriaatmadja, 2023).

Measures that government agencies can take include the use of data encryption to protect sensitive information, restricting access to personal data to authorised parties, and implementing up-to-date security systems to prevent unauthorised access. In addition, government agencies need to adopt a comprehensive information security policy and ensure that all employees understand and comply with the policy. Training and awareness-raising among government employees is also important to ensure that they are able to identify and effectively deal with cyber security threats (Fakir & Miah, 2021).

4.3 Law Enforcement Mechanism against Cyber Criminals

Law enforcement against cyber criminals involved in the E-KTP data leak involves thorough investigation, evidence collection, and fair trial. Challenges in law enforcement include the limitations of existing laws, the complexity of digital footprints, and cross-border co-operation. Cybercriminals often use techniques and tools to hide their digital footprints, thus complicating the investigation and prosecution process (Yudistira & Ramadani, 2023).

To improve the effectiveness of law enforcement against cybercrime, a stronger legal framework and better capacity of law enforcement agencies are required. Updating regulations to accommodate technological developments and emerging cybercrime tactics is essential. In addition, increased international co-operation between law enforcement agencies from different countries is also needed to tackle cross-border cybercrimes. Investments in digital forensic technology and training for law enforcement officers can help improve their ability to identify, track and prosecute cyber criminals.

5. Conclusion

The leak of 102 million ID card data from the Ministry of Social Affairs demonstrates the complexity and challenges of dealing with data security threats in the digital era. Legal protection of personal data requires better implementation and higher awareness among the public and government agencies. The implications of cyber law for government agencies emphasise the importance of strong policies and up-to-date information security systems in managing sensitive data. Law enforcement mechanisms also need to be strengthened to provide a deterrent effect and prevent similar crimes in the future. Joint efforts from various parties are needed to ensure that personal data protection and information security remain a priority in facing data security challenges in the evolving digital era.

References

Adelika, A., & Nurbaiti, N. (2023). Upaya Pencegahan Terjadinya Pencurian Data Pada E-Ktp Bagi Penduduk Pada Dinas Kependudukan Dan Pencatatan Sipil Kota Medan. *Jurnal Pengabdian Masyarakat Khatulistiwa*, 6(2), 124-133.

Djafar, W. (2019). *Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan.* Paper presented at the Seminar Hukum dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM.

Fakir, M. K. J., & Miah, M. R. (2021). Factors Influencing E-WOMs in Restaurant Business: Evidence from Bangladesh. *Journal of Sustainable Tourism and Entrepreneurship*, 3(1), 17-36.

Ferdian, A., & Chazawi, A. (2015). Tindak Pidana Informasi & Transaksi Elektronik. *Malang: Media Nusa Creative*.

Nursiyono, J. A., & Huda, Q. (2023). Analisis Sentimen Twitter Terhadap Perlindungan Data Pribadi Dengan Pendekatan Machine Learning. *Jurnal Pertahanan dan Bela Negara*, 13(1), 1-16.

Oranefo, P. C., & Egbunike, C. F. (2021). An exploration of the viability of forensic accounting techniques in combating financial statement fraud in Nigerian organizations. *Annals of Management and Organization Research*, 3(1), 69-81.

Putri, A. M., Syamsu, S., & Triono, A. (2024). Policy to replace electronic card into population digital in South Lampung Regency. *Journal of Governance and Accountability Studies*, 4(1), 19-29.

Riyadi, G. A., & Suriaatmadja, T. T. (2023). *Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*. Paper presented at the Bandung Conference Series: Law Studies.

Ukwuoma, H. C., Cirman, N. E., & Oye, P. O. (2022). The role of e-Government in overcoming the consequences of the COVID-19 pandemic in Nigeria. *Journal of Governance and Accountability Studies*, 2(1), 79-92.

Yudistira, M., & Ramadani, R. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO. *UNES Law Review*, 5(4), 3917-3929.