JOURNAL LA SOCIALE

VOL. 05, ISSUE 02 (471-478), 2024
DOI:10.37899/journal-la-sociale.v5i2.1132

Protection of Personal Data in the Use of Digital ID Cards against Misuse of Data from Cyber Hack

Mia Rizki[1], Augustin Rina Herawati[1], Endang Larasati[1]

[1]*Diponegoro University*

**Corresponding Author: Mia Rizki*
E-mail: miarizkiwaluyo@gmail.com

Article Info

Article history:
Received 16 February 2024
Received in revised form 6 March 2024
Accepted 14 March 2024

Keywords:
Digital ID Card
Personal Data
Data Protection
E-Government

Abstract

Data misuse from cyber hack in Indonesia is still high, judging from data leakage cases in Indonesia, from January to June 2023 there were 35 cases. Data leaks related to personal data on identity cards totaling 377 million data leaked until 2023, the data is contained on the dark web in the form of NIK, full name, date of birth, birth certificate e number, blood type, religion, marital status and so on. Writing using a qualitative descriptive approach, this study uses literature studies, namely data collection techniques by conducting a review study of books, literature, records, and reports related to Digital ID cards and data security. This research also uses a fact approach, a case approach to data misuse by cyber hackers, and a statutory approach. The type of data used is secondary data. There are still many personal data leaks in various factors including human error, malware, system security weaknesses, insider threats, lack of security awareness. The impact of data leaks are fraud and identity theft, threatened privacy, financial fraud, national security threats. There are various alternative recommendations to minimize data leakage, this anticipation can be done by the community, students, and the government. This anticipation is in the form of changing passwords regularly, being careful in using applications or social media that have viruses, avoiding uploading photos of ID cards, conducting cyber security training, community empowerment, bureaucracy forming a special IT department responsible for building virtual protection systems, cooperation with third parties.

Introduction

Globalization is a phenomenon that cannot be avoided by the world community, where globalization offers many updates in all fields, ranging from social, economic, political, and cultural (Syafriyani, 2019). In the era of globalization that is currently occurring and developing influenced by the rapid and broad pace of globalization, where according to Thompson & Laaser (2021) globalization is influenced by 4 main factors including rationalism, capitalism, technological innovation, and regulation. Technological innovation factors encourage infrastructure progress, one of which is in terms of communication, namely the emergence of the internet. The emergence of the internet then encouraged the birth of the era of revolution 4.0. The era of Revolution 4.0 is an era where all life from the civil level, government to the state is able to optimize profits by utilizing digital platforms. Public services are one of the fields of government that are included in the development of digitalization (Syafriyani, 2019).

E-Government is an effort to develop digital-based governance. A structuring of management systems and work processes within the government by optimizing the use of information and communication technology (Ali et al., 2021). E-Government allows people to be able to

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

interact and receive services from local, regional, and central governments more quickly and efficiently without having to take a lot of money and time to perform services.

Changes in government services in Indonesia based on E-Government are driven by an increase in the number of internet usage in Indonesia which is growing very rapidly reaching 215.63 million people in the 2022-2023 period from a total population of 275.78 million people, the data is based on the results of a survey by the Indonesian Internet Service Providers Association (APJII). This number increased by 2.67% when compared to internet usage in the previous period which was 210.03 million users. The increase in this number helps in supporting digital-based public services.

The development of information technology has caused a borderless world and caused significant social changes (Hermawanto & Anggraini, 2020). One of the developments in information technology occurs in the field of population and civil registration, the importance of population data is one of the useful pieces of information for sustainable development planning (Hastuti, 2020). In the digital era, population data is very important data so that it must be stored, maintained, kept correct, and protected confidentially. The use of population data must be followed by clear regulations regarding the security of ownership of population data (Grantz et al., 2020).

The Ministry of Home Affairs through the Population and Civil Registration Office in improving digital-based services in population administration, launched an innovation called Digital KTP (ID). Based on Permendagri No.72 of 2022 concerning Standards and Specifications for Hardware, Software, and Electronic Identity Card Forms and the implementation of Digital Population Identity, the Digital KTP program or IKD (Digital Population Identity) is electronic information used to present population documents and reverse data in digital applications via smartphones. This innovation was developed by the government to assist in the integration of population data, facilitate and accelerate public and private service transactions in digital form, safeguard ownership of digital population identities through authentication systems to prevent falsification and data leakage. Digital KTP is the transfer of e-ID cards owned by Indonesian residents into mobile phones in the form of photos, or QR Codes.

Indonesia as a state of law guarantees the protection of human rights in the country's constitution. In fact, as many as 337 million data allegedly came from the Population and Civil Registration Service, Ministry of Home Affairs, a total of 337,225,465 data on the darkweb is quite complete, ranging from NIK, full name, date of birth, birth certificate number, blood type, religion, to marital status. The data leak that occurred represents that the security of personal data owned by the government is still weak (Pratama & Pati, 2021).

In 2021, as many as 279 million Indonesian citizens' data was leaked and traded online, showing the weak protection of personal data security in Indonesia. Director General of Population and Civil Registration of the Ministry of Home Affairs, Zudan Arif Fakrulloh said the data leak came from advertisements on the website, there were individual data links that could be downloaded as data samples, the data that had been downloaded was in the form of CSV (comma separated value) files and after import amounted to 1,000,000 rows. The total data claimed to provide is 279 million population data. A total of 20 million of them are included with photo data (Stevens et al., 2020).

Personal data leaks are often repeated in Indonesia due to cyber hack attacks. From the data leak graph according to information from the Ministry of Communication and Information above, since 2019 there have been 79 cases related to data theft in the country. From January

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

to June 2023, there were 35 cases, which exceeded the number of data leakage cases that occurred every year, from 2019-2021.

The data leak that occurred in the SIM Card Data of the Republic of Indonesia occurred in 2022, as many as 1.3 billion SIM Card Data leaked amounting to 87 GB claimed to contain NIK, mobile phone number, provider, telecommunication, and registration date, the data was sold for Rp. 743.5 million. The data leak case in Indonesia involving Bank Syariah Indonesia (BSI) occurred on May 8, 2023. Prior to the leak of Bank Syariah Indonesia customer data, there were complaints of disruption of transaction services on May 8, 2023, then the attack of personal data theft against Bank Syariah Indonesia as much as 1.5 TB of data, data leakage included names, telephone numbers, addresses, account balances, account numbers, transaction history, account opening dates, to work (Marcelliana, et al., 2023).

Dealing with cybercrime is a challenge because of the increasing sophistication of a country's response mechanism or citizens receiving information technology, protection against security vulnerabilities in cyberspace makes one of the government's concerns. Public connectivity and social media have an impact on increasing dependence on information communication technology, which encourages the government to formulate laws to supervise cyberspace. The government bureaucracy is expected to have a dedicated IT department responsible for building virtual protection systems (Bowen et al., 2020). Private users or the public are also encouraged to manage software with anti-virus and malware on their respective devices so that they can help in the security of personal data, this must be encouraged by increasing knowledge related to the level of cyber threats in cyberspace.

Singapore is one of the countries that participate in advancing the technology sector due to the times that make people switch to the Internet of Things (IoT), where everything will be connected to the presence of information technology that is easily available. Utilization of information communication technology (ICT) to drive the economy and overcome problems such as the provision of health services and infrastructure development. Singapore's Prime Minister Lee Hsien Loong launched the Smart Nation Initiative in 2014, making Singapore one of the most advanced ICT countries in Asia-Pacific. The challenges faced in cyber security are of particular concern so that it presents a challenge for Singapore in security issues. Singapore established the Cyber Security Agency in April 2015 and released a cyber security strategy in October 2016 (Vu & Rajaratnam, 2016).

Privacy and data protection are priorities for countries that have developed information technology. In the development of digitalization, data is a very important asset. Data protection challenges are also faced by the United States, where they must take strict action against all forms of data theft. Data security starts from an assessment of how to secure Internet of Things (IoT) devices, the government seeks to approach these problems and create incentives for companies to be able to secure their respective IoT. There are three essential elements of a comprehensive data protection plan: data inventory, public projections of privacy and data protection policies, and response to events. The protection efforts carried out by the United States will be able to ensure an effective and strategic response when an incident does occur.

The importance of data security can prevent misuse of personal data by irresponsible parties, avoiding potential defamation (kominfo.go.id). According to the Directorate General of Applications and Information Technology (Aptika) Kominfo, personal data is included in the human rights and privacy listed in the 1948 Universal Declaration of Man Article 12, so that the importance of personal data encourages strengthening personal data protection to continue. This reason encourages the author to conduct research on how to protect personal data in the

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

use of Digital KTP and find out how efforts are made to prevent misuse of personal data from cyber hack attacks.

Methods

The author uses a qualitative descriptive approach, this study uses literature studies, namely data collection techniques by conducting a review study of books, literature, notes, and reports that have something to do with the problem discussed. This research also uses a fact approach, a case approach to data misuse by *cyber hackers*, and a statutory approach. The type of data used is secondary data.

The theory used by the author is TAM Theory (Technology Acceptance Model), this theory was first proposed by Davis in 1986. The purpose of TAM theory is to provide an explanation of the determinants of computer acceptance in general. TAM suggests external factors influence intention and actual use through centric effects on perceived benefits and ease of perceived benefits (Nugraha, 2020)

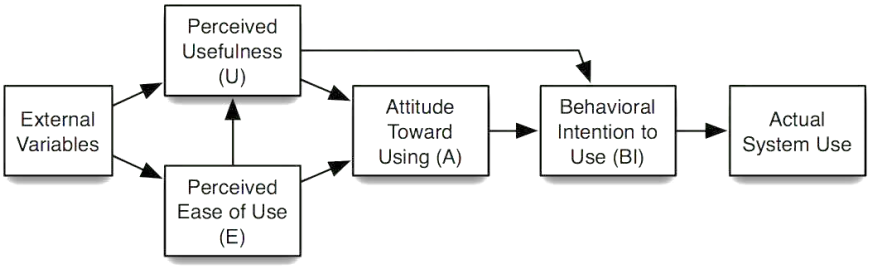

Figure 1. TAM Theory

Source: Based on Saleh et al. (2022)

Based on these figures, the TAM theory model expresses two beliefs: (1) Perceived usefulness, namely the extent to which a person believes that using a certain system will improve his work performance; (2) Perceived ease of use, that is, the degree to which one believes that using a particular system will be free of effort (Saleh et al., 2022).

Results and Discussion

Protection of personal data in the use of Digital KTP

Law Number 27 of 2022 concerning Personal Data Protection, Article 53 regulates officials and officers who carry out personal data protection functions where officials or officers who carry out personal data protection functions are required to have professionalism, knowledge of the law, personal data protection practices, and the ability to fulfill their duties. Officers or officers performing personal data protection functions may originate from inside and/or outside the personal data controller or personal data processor. For violations that occur against the provisions of personal data processing, sanctions are given as written in article 57 in the form of written warnings, temporary suspension of personal data processing activities, deletion or destruction of personal data and/or administrative fines. Administrative sanctions apply to administrative fines as referred to, which is a maximum of 2 (two) percent of annual income or annual receipts for variable violations.

The Directorate General of Dukcapil of the Ministry of Home Affairs through the Population and Civil Registration Service innovates digital-based electronic ID card services. The latest innovation of Digital KTP encourages people to switch from electronic KTP which is in physical form and usually inserted in pockets or wallets to Digital KTP stored on mobile

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

phones. The change of Electronic KTP to Digital KTP will minimize the occurrence of Electronic KTP reprint submissions due to damaged/lost/changes in biodata elements or changing domicile addresses.

Digital KTP is the transfer of Electronic KTP currently used by Indonesian residents into mobile phones, either in the form of photos, or QR Codes. The launch of the Digital KTP program as part of efforts to improve the efficiency of public administration. The requirements that must obtain a Digital KTP according to Article 18 Paragraph 2 of Permendagri No. 72 of 2022 are: (1) Have a mobile phone (smartphone); (2) Have a physical e-ID card or have never had a physical e-ID card but have recorded an ID card; (3) Have an *email* and *mobile number*.

Security that has been adapted by KTP Digital is a screen capture prevention feature (screenshot), it helps minimize misuse of information. Shared QR codes are always fickle and are only valid for 90 seconds. Director General of Population and Civil Registration (Dukcapil) of the Ministry of Home Affairs (Kemendagri) Zudan Arif Fakrulloh emphasized that Digital KTP is safe to use with a security system on Digital KTP almost the same as digital applications commonly used by the public, such as e-banking or mobile banking which is used for money transfers, shopping and so on.

The security system on Digital KTP is carried out using PIN encryption (personal identification number), and so on. Digital KTP also implements the ISO 27001 security system, which is an international standard framework that contains information security standards. The security strength that encryption has built up also depends on the encryption algorithm and key strength. According to the Executive Director of the Cyber Communication and Information System Security Research Center, Pratama Persada, Dukcapil still needs to improve security on the server. There are many standards in securing information in servers and networks, such as ISO 27001, COBIT (Information Technology Management Practice Guidelines), and information security management standards made by the National Cyber and Encryption Agency (BSSN). Security standards must be followed and coupled with good defense tools, monitored access to the system, and structured monitoring and tests that will help improve the security of the Dukcapil server. Factors causing data leakage can be sourced externally or internally, including the following:

One of the data leaks can be caused by *human error*. Human error is a mistake or action taken by a human individual that results in personal data being leaked. Examples of *human error* in the case of data leakage are carelessness in data management, lack of training and awareness, and neglect of security protocols. *Malware* (*Malicious Software*) is a program specifically designed to damage by infiltrating computer systems. The intrusion can enter through *email*, *internet downloads, or infected programs. Malware* can also cause damage to computer systems and allow information theft, some examples include viruses, *spyware*, and *ransomware*.

System security weaknesses are gaps or vulnerabilities in technology and software infrastructure that manage, store, or access Digital KTP data. This weakness can be exploited by unauthorized parties to access or steal Digital KTP data illegally or unlawfully. These system security weaknesses can occur due to a variety of factors, including poor design, lack of maintenance, late software updates, or negligent actions in the implementation of security policies. *Insider threats* refer to threats originating from individuals or entities that have internal access or proximity to systems, data, or information related to Digital ID cards, but intentionally or unintentionally take adverse actions to disclose, steal, or misuse such data. Insider threats can arise from within organizations that manage Digital ID card data, including employees, or other parties who have limited access to systems or data.

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

Another cause of data leakage is that people who manage or have access to Digital KTP data do not have sufficient understanding or attention to the importance of maintaining the security of personal information contained in Digital KTP. Lack of awareness of data security can cause actions that lead to leakage of Digital KTP data so that data will be revealed to unauthorized parties. The Impact of Digital KTP Data Leakage results in losses to individuals, some of the impacts that occur as a result of Digital KTP data leakage are as follows:

The emergence of access to Digital KTP can result in irresponsible individuals committing identity fraud. The proceeds of identity theft can be opening fake accounts, applying for loans, or carrying out other criminal activities. Digital ID card data leakage in the development of an increasingly digitally connected society can threaten individual privacy. Misused personal information may result in loss of control over confidential information

Criminals who gain access to Digital KTP data enable identity abuse by pretending to be the original owner to carry out illegal transactions. Digital KTP data leakage is also vulnerable to being misused to apply for online loans *in* applications or services that have poor security systems, data theft can access bank accounts, make *online* purchases, or break into other important accounts belonging to victims. National security threats in the case of Digital ID Card data leakage refer to potential risks to the stability and security of a country due to sensitive and important information in Digital ID cards falling into the hands of irresponsible people. The impact of threats includes use for criminal activities and terrorism, the creation of false identities for espionage, and decreased trust in the government.

Anticipate misuse of personal data from *cyber hack attacks*

The head of the *Cyber Communication &; Information System Security Research Center* (CISSReC), Pratama Persadha, emphasized the importance of personal data protection when the government implements Digital KTP, several things that need to be considered, namely: (1) The importance of data encryption where all stored data must be encrypted to prevent access by unauthorized parties; (2) Strong authentication, namely the Digital KTP system must have a strong authentication mechanism to ensure that only authorized users can access the Digital KTP; (3) Protection against attacks is something that must be considered where the system must be protected from attacks such as DDoS, SQL injection, and so on to ensure data security; (4) Digital KTP users must be trained and desensitized related to the importance of cyber security and data protection in order to minimize data leakage; (5) Upgrading Dukcapil's IT infrastructure must also be done as well as servers that are getting old, because data security will be better supported by the support of a better and latest IT system.

Personal data protection efforts against data leaks and data attacks from *cyber hacks* are very important to maintain individual security and privacy and prevent potential threats to national security. Some of the protective measures that can be taken are: (1) Changing passwords regularly, changing passwords regularly can help in minimizing data leakage because it can potentially have unauthorized access. Regular password changes can minimize the risk of *brute force* attacks or attempts to guess passwords by trying different password combinations. Prevention of data leakage by changing passwords can also minimize keyloggers*, which are types of software that can record every typing done, including passwords, periodic password changes can avoid passwords recorded by* keyloggers becoming useless after a certain period. Password changes must be accompanied by a password that is strong enough and encrypted; (3) Be careful in using applications or social media, in using applications on mobile phones people are urged not to carelessly download and even access sites that have security vulnerabilities, because when a virus has entered the cellphone, hackers can quickly access all data. The public must remain cautious in providing personal data; (4) Avoid uploading ID card

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

photos carelessly, avoid uploading ID card photos or important information carelessly, providing ID card information can be done more selectively, namely paying attention to sites accessed such as government agencies or services that have been officially verified only.

The role of students in overcoming Digital KTP data leakage is very important, especially with background knowledge and skills in information technology and *cyber* security. Some of the roles that can be performed by students are as follows: Students are able to follow or be involved in the *cyber* security community at university or *online*, students are expected to be able to share knowledge, experience, and the latest solutions related to data security to the public. Students are expected to have the potential to become cyber security advocates *by* educating the public regarding the risk of data leakage and steps that can be taken to protect their personal information. The community can hold workshops, seminars, or community empowerment events that aim to teach basic cyber security skills to the general public.

The government's role in overcoming the leakage of Digital KTP data is as follows: (1) The government bureaucracy is expected to have a dedicated IT department responsible for establishing *virtual* protection, surveillance and auditing systems to oversee the practice of using digital ID card data and conduct periodic audits on organizations that use such data to ensure regulatory compliance; (2) The development of data security technology, the government can invest in the development and improvement of security technology used in the Digital KTP system. This includes the use of strong encryption, *firewalls*, and detection systems; (3) Cooperation with third parties, the government can work with *cyber* security agencies and the private sector to improve the security of Digital KTP data. Cooperation with third parties may include the exchange of information about *cyber* threats as well as best data protection security practices; (4) In the development of an incident reporting system, governments can develop incident reporting systems that enable organizations to report data breaches quickly and effectively. This allows quick action to overcome cases of data leakage or data theft that occur.

The government conducts international cooperation, cyber-attacks that not only originate from Indonesia allow high opportunities in dealing with attacks from abroad, the government can strengthen international cooperation to overcome *transnational cyber* threats.

Conclusion

KTP Digital implements the ISO 27001 security system, which is an international standard framework that contains information security standards. The security strength that encryption has built up also depends on the encryption algorithm and key strength. Various efforts are still needed to develop data security and strengthen data security to anticipate attacks from cyber hacking. Factors causing data leakage can be external or internal, human error, malware, system security weaknesses, insider threats, lack of security awareness.

Anticipatory efforts that can be done by the student community and the government are changing passwords regularly, education and data security awareness, avoiding uploading ID card photos carelessly, conducting cyber security training, community empowerment, government bureaucracy is expected to have a special IT department responsible for building virtual protection systems, developing data security technology, cooperation with third parties, developing incident reporting data leakage or cyber hacking.

References

Ali, S., Zheng, Z., Aillerie, M., Sawicki, J. P., Pera, M. C., & Hissel, D. (2021). A review of DC Microgrid energy management systems dedicated to residential applications. *Energies*, *14*(14), 4308. https://doi.org/10.3390/en14144308

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

Bowen, T., Del Ninno, C., Andrews, C., Coll-Black, S., Johnson, K., Kawasoe, Y., ... & Williams, A. (2020). *Adaptive social protection: building resilience to shocks*. World Bank Publications.

Grantz, K. H., Meredith, H. R., Cummings, D. A., Metcalf, C. J. E., Grenfell, B. T., Giles, J. R., ... & Wesolowski, A. (2020). The use of mobile phone data to inform analysis of COVID-19 pandemic epidemiology. *Nature communications*, *11*(1), 4961. https://doi.org/10.1038/s41467-020-18190-5

Hastuti, S. H. D. (2020). Pentingnya pemanfaatan data kependudukan di era digital. *TEKNIMEDIA: Teknologi Informasi Dan Multimedia*, *1*(1), 18-21. https://doi.org/10.46764/teknimedia.v1i1.9

Hermawanto, A., & Anggraini, M. (2020, October). Globalization And Locality: Global Communication And Digital Revolution In The Borderless World Era. In *Proceeding Of Lppm Upn "Veteran" Yogyakarta Conference Series 2020–Political And Social Science Series* (Vol. 1, No. 1, pp. 9-16). https://doi.org/10.31098/pss.v1i1.84

Marcelliana, V., Zahra, S. M., Adzani, N. N., Massaid, H. N., Badriyyah, N., Benita, R., ... & Bayhaqi, T. A. R. (2023). Penerapan Perlindungan Konsumen Terhadap Nasabah Pt. Bank Syariah Indonesia Dalam Kasus Kebocoran Data Nasabah. *Deposisi: Jurnal Publikasi Ilmu Hukum*, *1*(2), 180-194. https://doi.org/10.59581/deposisi.v1i2.577

Nugraha, A. (2020). Sistem Pengelolaan Dokumen Elektronik untuk Digitalisasi pada Layanan Publik. Jurnal Komputer dan Informatika, 15(1), 274-281.

Pratama, A. M., & Pati, U. K. (2021). Analysis principles of personal data protection on COVID-19 digital contact tracing application: pedulilindungi case study. *Lex Scientia Law Review*, *5*(2), 65-88.

Saleh, S. S., Nat, M., & Aqel, M. (2022). Sustainable adoption of e-learning from the TAM perspective. *Sustainability*, *14*(6), 3690. https://doi.org/10.3390/su14063690

Stevens, E., Antiga, L., & Viehmann, T. (2020). *Deep learning with PyTorch*. Manning Publications.

Syafriyani, I. (2019, December). Implementasi E-Government dalam Menjawab Tantangan Pelayanan Publik di Kabupaten Sumenep. In *Prosiding: Seminar Nasional Ekonomi dan Teknologi* (pp. 216-221).

Thompson, P., & Laaser, K. (2021). Beyond technological determinism: revitalising labour process analyses of technology, capital and labour. *Work in the Global Economy*, *1*(1-2), 139-159. https://doi.org/10.1332/273241721X16276384832119

Todt, K. E. (2019). Data Privacy and Protection. *The Cyber Defense Review*, *4*(2), 39-46. https://www.jstor.org/stable/26843891

Vu, C., & Rajaratnam, S. (2016). *Cyber security in Singapore*. S. Rajaratnam School of International Studies.

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)