Al-mishbah
jurnal ilmu dakwah dan komunikasi
P-ISSN : 1978-2513 E-ISSN : 2442 - 2207
JURNAL HOME PAGE HTTPS://ALMISHBAHJURNAL.COM/INDEX.PHP/AL-MISHBAH/INDEX

Public Perception of Personal Data Privacy in the Digital Era

Afdhal[1], Syaifullah MS[2]
[1]University of Muhammadiyah Palu
[2]State Islamic University Datokarama Palu
Email: afdhalzainal@gmail.com

Keywords
Personal Data Privacy, Digital Era

Abstract

Public perception of personal data privacy in the digital era shows that there is a growing awareness of the importance of protecting personal information. People are beginning to understand that personal data is a valuable asset that is vulnerable to misuse in various forms, such as fraud, identity theft, and commercial abuse. However, this awareness has not been fully accompanied by concrete actions in maintaining data security, because there are still many individuals who neglect the use of social media, applications, and other digital services. In addition, some people view that personal data protection is not only an individual responsibility, but also requires strong regulations from the government and a commitment to transparency from digital service providers. This emphasizes that efforts to maintain personal data privacy must be carried out collaboratively between individuals, the community, the government, and the private sector. Thus, it can be concluded that although the public has an awareness of the importance of personal data privacy, the biggest challenge lies in the consistency of safe digital behavior and the strengthening of regulations that are able to provide comprehensive protection in an increasingly complex digital era.

Kata kunci
Privasi Data Pribadi, Era Digital

Abstrak

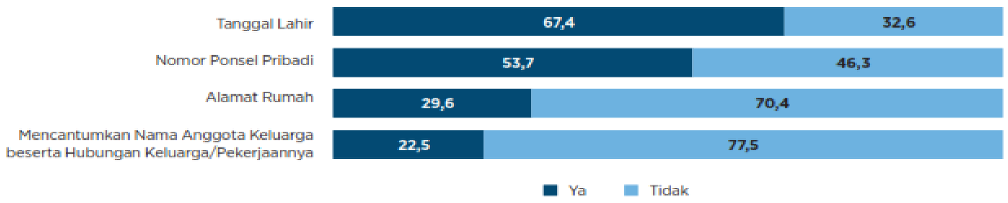
Persepsi masyarakat terhadap privasi data pribadi di era digital menunjukkan adanya kesadaran yang semakin meningkat mengenai pentingnya perlindungan informasi pribadi. Masyarakat mulai memahami bahwa data pribadi merupakan aset berharga yang rentan disalahgunakan dalam berbagai bentuk, seperti penipuan, pencurian identitas, maupun penyalahgunaan komersial. Namun, kesadaran tersebut belum sepenuhnya diiringi dengan tindakan konkret dalam menjaga keamanan data, karena masih banyak individu yang abai dalam penggunaan media sosial, aplikasi, maupun layanan digital lainnya. Selain itu, sebagian masyarakat memandang bahwa perlindungan data pribadi tidak hanya menjadi tanggung jawab individu, tetapi juga memerlukan regulasi yang kuat dari pemerintah serta komitmen transparansi dari penyedia layanan digital. Hal ini menegaskan bahwa upaya menjaga privasi data pribadi harus dilakukan secara kolaboratif antara individu, masyarakat, *pemerintah, dan pihak swasta. Dengan demikian, dapat disimpulkan bahwa meskipun masyarakat telah memiliki kesadaran akan pentingnya privasi data pribadi, tantangan terbesar terletak pada konsistensi perilaku digital yang aman serta penguatan regulasi yang mampu memberikan perlindungan menyeluruh di era digital yang semakin kompleks.*

Introduction

In 2019, the Indonesian Internet Service Users Association (APJII) recorded that 196.71 million people in Indonesia had accessed the internet. This figure covers 73.7% of Indonesia's total 270 million population. Java is the island with the most users, reaching 55.7% of the internet user population in Indonesia. The use of technology makes it easier for people to carry out various activities, ranging from communication, transportation to digital transactions. The use of internet technology has implications for the vulnerability of users' personal data. Each user should be able to determine whether their data can be used and disseminated by social media managers or applications. It also has the right to determine the requirements that apply within a community regarding the use of data.[1]

Personal data regarding full names, e-mails, social media accounts, and even account numbers are required by various application services, one of which is to ensure the legitimacy of users and the accuracy of services. However, there is no guarantee that such personal data will be avoided from misuse. Contact numbers, bank accounts, and home addresses can be used by malicious parties, such as to commit cell phone fraud, hack bank accounts, and rob homes. The 2020 Indonesian Digital Literacy Status Research by the Katadata Insight Center (KIC) revealed that public understanding of the importance of personal data confidentiality is not yet high. As many as 67.4% of internet users in Indonesia share their date of birth, and 53.7% write their phone number on social media.

Grafik 1.1 Informasi yang dicantumkan di media sosial (%)
"Apakah di akun media sosial anda tercantum informasi berikut?" [SA]
Basis: seluruh responden



SUMBER: KATADATA INSIGHT CENTER

The protection of privacy and personal data is a factor that determines the level of online trust. The lack of protection causes privacy data to be spread to irresponsible parties, so that it can be financially detrimental, even threatening the safety of its owners. Indonesia has a number of regulations regarding the protection of personal data, but they

[1] Gunawan, "Measurement of Information Security and Privacy Awareness in Social Media," J. Muara Sains, *Teknol. Medicine and Health Sciences*, vol. 5, no. 1, p. 1, 2021, doi: 10.24912/jmstkik.v5i1.3456.

are spread across several laws. Therefore, the government and the House of Representatives are preparing a Personal Data Protection Bill (PDP Bill).[2]

The Public Perception Survey on Personal Data Protection aims to map public perception of the right to personal data protection in 34 provinces of Indonesia. This primary data collection is expected to illustrate the public's understanding of personal data, its misuse, awareness of the right to protect personal data and the Personal Data Protection Bill (PDP Bill).

Method

The type of descriptive method carried out is literature research Literature research is an activity of observing various literature that is related to the subject matter raised, whether it is in the form of books, papers or writings that are helpful so that they can be used as guidelines in the research process. According to Kartini Kartono in the book Introduction to Social Research Methodology, the purpose of library research is to collect data and information with the help of various materials in the library, the results are used as the basic function and main tool for research practice in the field. Because using library research means that data sources are taken from various data sources that are relevant to the topic raised

Results and Discussion (12 pt bold)

In the ever-evolving digital world, personal data protection is not only a hot issue, but also a must for every professional. In the midst of the convenience offered by technology, we need to be smarter in managing our personal information. Along with the increasing use of digital technology, the risk of data breaches is also getting higher. Starting from financial information to health history, it is often a target for cybercriminals. Therefore, understanding how to protect your data is an important step in maintaining personal and professional security. For example, a user of a health app who stores his or her medical data in the app. If the app experiences a data leak, its sensitive health information could fall into the wrong hands, potentially causing financial or reputational losses.[3]

Privacy refers to the English equivalent of privacy is the ability of one or a group of individuals to keep their lives and personal affairs from the public, whereby one controls the flow of information about oneself. Another depiction of privacy is the individual's right to determine whether and to what extent a person is willing to open himself or herself to others.

1. There are three privacy functions, namely:
   a. Regulators and controllers of interpersonal interactions that mean the extent to which relationships with others are desired
   b. Plan and create strategies for connecting with others, which includes intimacy or distance in connecting with others.

[2] I. T. Islamy, S. T. Agatha, R. Ameron, B. H. Fuad, Evan, and N. A. Rakhmawati, "The Importance of Understanding the Application of Privacy in the Era of Information Technology," *J. Technol. Inf. and Computer Science.,* vol. 11, no. 2, pp. 21–28, 2018.

[3] T. Agustin, "Information System Security Analysis of Personal Data on Social Media," 2020.

c. Clarify the identity of the source.[4]

2. Data Privacy

It can be said that personal data if the data can be used to recognize or identify a person, an example of personal data is the student's identity number and the student's name on the attendance record. The identity number can be used as a way to identify the student. However, if the attendance is only a collection of student identity numbers without being equipped with the student's name, then it is only called data. The reason is that the data cannot be used to identify a person.[5]

3. Communication Privacy

Communication is the sending and receiving of messages or news between two or more people so that the message in question can be understood. Communication Privacy in information technology discusses how a person can communicate with each other through information technology without being monitored by third parties. Since everyone has private limitations, therefore we must also respect those limitations. Only through certain laws and methods can restrictions on the privacy of communication be ignored.

4. Online Privacy

A wide range of data and information are collected with increasing frequency and in different contexts, making individuals more transparent. In fact, sometimes a person easily spreads his opinion through social networking accounts that are familiar and loved by teenagers. The social and financial costs incurred to obtain and analyze this data increase sharply as technology advances. This phenomenon poses problems including privacy. There are concerns that the Internet could erode privacy and that privacy issues in offline or face-to-face social interactions are increasingly magnified in online interactions. There are a number of specific threats when making transactions online related to privacy. For example, the influence of surfing through internet media means that when we are online, we indirectly leave data in the form of digital footprints in many areas of our lives that were previously considered "offline." Very rapid developments with computing power, such as processing speeds, increased storage capacity, wider communication connectivity, and the size of connection capacity at low cost all ultimately affect privacy.[6]

Therefore, there are important privacy issues related to online activities. Of course, there are also benefits to technological advancements described such as (personalized service, convenience, improved efficiency). Users can provide valuable information about themselves to take advantage and benefits. The *American Life Survey* reports that more than two-thirds of users are willing to share their personal information under some circumstances. In some situations, expressive privacy can be obtained through the loss of information privacy to third parties. For example, a person may disclose personal information and credit card information for the convenience of

[4] D. Revilia and N. Irwansyah, "Social Media Literacy: Millenial's Perspective of Security and Privacy Awareness," *J. Penelit. Komun. Dan Opini Publik,* vol. 24, no. 1, pp. 1–15, 2020, doi: 10.33299/jpkop.24.1.2375.

[5] L. Rizkinaswara, "Pahami Kebijakan Privasi di Media Sosial untuk Lindungi Data Pribadi," https://aptika.kominfo.go.id/, 2019

[6] M. M. Amanda Lenhart, "Social Networking Websites and Teens: An Overview," 2008.

completing an online transaction. In this way, this private collection, privacy information can be considered a "double-edged sword".[7]

5. Freedom of Information

Freedom is a fundamental thing, which generally experts have the same conception that freedom exists in every human being. Ecryptically, freedom always has limits to both internal and external weaknesses. Basically, freedom does not mean doing the will of the heart, but there is a limit to recognizing and respecting the rights and obligations of every human being in general. Information has introduced a new ethics, that every party who has information has an instinct that always disseminates to other parties, and vice versa. Information technology promises that the 21st century community will have communication networks and multi-media technology as the backbone. Respect for privacy in the globalized information community is vastly different in a fiscal environment, as well as in the interest of data privacy. The need to maintain the confidentiality of data and personal information seems to be a priority to put trust in the communication interaction network.[8]

6. Anonymity in Online Activities

Anonymity is anonymity. For example, for the people participating in the election, of course, when voting they do not write their names on the ballot paper. This is to ensure confidentiality during the election. Privacy and anonymity are 2 things that are very closely related and similar. But the principle is that anonymity is for privacy while privacy does not necessarily require anonymity, although it usually does. Privacy can be obtained by implementing securities such as encryption. For example, when sending an e-mail with an address and name, but the content is shuffled to prevent others from seeing the contents of the e-mail.[9] In digital media such as the internet, no matter what service is used, at least one person has opened his or her own identity. How and what about a person can be known by others. Here are steps that can be taken to maintain privacy when surfing cyberspace.

a. Change your privacy or security settings. Understand and use these security setting features to the best of your ability.
b. Make your password as strong as possible. When registering online, you should do a combination of uppercase and lowercase letters, numbers, and symbols so that they are not easily tracked.
c. Keep your password confidential.
d. Don't use questions about your date of birth, address, mother's name because they are almost always used as security questions for bank and credit card databases. This provides an opportunity for hackers to steal identities and steal money.
e. Always log out. Always remember to log out of your account, especially if you are using a public facility computer.

[7] N. Senthil Kumar, K. Saravanakumar, and K. Deepa, “On Privacy and Security in Social Media - A Comprehensive Study,” Phys. Procedia, vol. 78, no. December 2015, pp. 114–119, 2016, doi: 10.1016/j.procs.2016.02.019.

[8] N. Aldhafferi, C. Watson, and S. A.S.M, “Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices,” *Int. J. Secur. Priv. Trust Manag.,* vol. 2, no. 2, pp. 1–17, 2013, doi: 10.5121/ijsptm.2013.2201.

[9] N. L. Leech and A. J. Onwuegbuzie, “A typology of mixed methods research designs,” *Qual. Quant*., vol. 43, no. 2, 2009, doi: 10.1007/s11135- 007-9105-3.

f. Wi-FI. Create a password to use wi-fi, otherwise there may be an intruder entering the network.
g. Don't share sensitive information, i.e. avoid sharing personal information.
h. Make it difficult to log in to your account by choosing a strong and unique password, and turning on two-factor authentication.
i. Use an application with end-to-end encryption This is a feature in the chat application to keep personal data safe on social media.
j. Always check the application, which is to make sure you understand the various accesses needed by the application.
k. Six main points to consider when using an online application system related to data privacy are security and data protection, user awareness, control settings, risk management, transparency, and ethics.[10]

Challenges Faced

1. Data Breaches**:** Data breaches have become everyday news. This incident can result in identity theft and financial losses. We need to be vigilant and prepare for this potential risk. The data leak cases experienced by large companies such as Equifax, which resulted in more than 147 million personal information being exposed, show how vulnerable our personal data can be.
2. Data Monetization**:** Many companies collect and leverage your data to their advantage. Without realizing it, you may have shared very personal information. Many social media platforms collect user behavior data to target ads. Users are often unaware that their activities are being tracked and used to generate revenue for the company.
3. Lack of Awareness**:** Many people are still unaware of how much data they are sharing online. Without enough knowledge, we all risk becoming easy targets for cybercriminals. A person may upload vacation photos to social media without realizing that the location and other personal information are also attached in the image's metadata.
4. Privacy Regulations**:** With increasing concern for data privacy, governments in various countries have started to enforce stricter rules. This can be tricky, especially for small and medium-sized companies that may struggle to keep up with these rules. Small companies unfamiliar with data protection regulations may struggle to effectively manage their customer information, risking hefty fines in the event of a breach.[11]

To protect yourself and your organization, here are some strategies that can be implemented:

1. Use *Strong* Passwords: **Make sure** your *passwords* are unique and complex. Enable two-factor authentication for an additional layer of security. This is a simple step that can make a big difference. Using a combination of uppercase, lowercase, number, and symbols in your *password* such as "P@ssw0rd2024!" can reduce the risk of *passwords* being guessed.

[10] John W. Creswell and Vicki L. Piano Clark, "Designing and Conducting Mixed Methods Research," Aust. N. Z. *J. Public Health,* vol. 31, no. 4, 2007, doi: 10.1111/j.1753- 6405.2007.00096.x.

[11] H. P. Yuwinanto, "Privasi online dan keamanan data," *Palimpsest* (Iowa. City)., no. 031, p. 11, 2015.

2. Data Encryption**:** Make sure your sensitive data is well protected, both when it is sent and stored. This is an effective way to protect information from unauthorized access. Use messaging apps that encrypt end-to-end data, such as WhatsApp or Signal, to make sure your conversations stay secure.
3. Make use of a VPN: A VPN can hide your IP address and encrypt your internet connection. This is especially useful when you're using public Wi-Fi that may not be secure. When using Wi-Fi in a café, a VPN helps prevent cybercriminals who are on the same network from stealing your data.
4. Choose a Privacy-Focused Browser**:** Browsers like Mozilla Firefox or Brave can help you protect your personal information by blocking trackers. Using Brave, which automatically blocks ads and trackers, can improve browsing speed while protecting your privacy.
5. Update Devices Regularly**:** Make sure your devices and apps are always up to date. These updates often contain security *patches* to protect you from the latest threats. If your *smartphone* notifies you about a software update, update it immediately to make sure you're protected from newly discovered vulnerabilities.
6. Improve Your Knowledge**:** Take the time to understand what data you share and how it's being used. Knowledge is power, and in this case, knowledge can protect you. Keeping up with news and articles about data protection can help you stay up-to-date on the latest cyber threats.
7. Comply with Privacy Rules**:** If you run a business, make sure you comply with existing rules. Compliance with the law not only protects consumers but also your business's reputation. Providing a clear privacy policy on your *website* informs customers about how their data will be used and protected.[12]

In today's digital era, the use of communication and information technology is increasingly rapid and changes people's daily life activities. However, the rapid development of digital technology also has negative impacts, one of which is a threat to the security of our personal data Personal data such as ID card numbers, passports, bank account books, and others are very important and must be kept confidential. If the personal data falls into the wrong hands, it can be used to commit criminal acts such as identity theft or fraud. Therefore, the protection of personal data is very important in this digital era. The House of Representatives of the Republic of Indonesia has made a personal data protection law in 2022 as an effort to provide protection or protection and provide a sense of security to the public.

Threats to Personal Data in the Digital Era

In today's digital era, our personal data can fall into the wrong hands if it is not properly maintained. Here are some threats that can threaten the security of our personal data in the digital age:

1. Hacking
   Hacking is the act of hacking or breaking into a computer system or network without permission. If a hacker manages to break into the system, then he could access our personal data and use it to commit criminal acts.

[12] R. T. Rust, P. K. Kannan, and N. Peng, "The customer economics of internet privacy," *Journal of the Academy of Marketing Science*, vol. 30, no. 4. 2002, doi: 10.1177/009207002236917.

2. Phishing
   Phishing adalah tindakan penipuan online yang dilakukan dengan cara membuat fake websites or send fake emails that resemble the official website or email of a particular company or institution. The goal is to steal personal information such as usernames, passwords, credit card numbers, and others.
3. Malware
   Malware is a malicious program designed to damage or steal data from our computer or mobile device. Malware can get into the system through fake emails, fake websites, or unofficial apps.
4. Social Engineering
   Social engineering is a psychological manipulation technique used by cybercriminals to gain access to confidential information such as passwords and credit card numbers of their victims.
5. Wi-Fi Network Security
   An unsecured Wi-Fi network can be an entry point for cybercriminals to access our personal data. If we connect to an unsecured Wi-Fi network, hackers could access our personal data. Those are some of the threats that can threaten the security of our personal data in the digital era. Next, we will discuss personal data protection laws and tips and tricks to keep them safe.[13]

Tips and Tricks to Protect Personal Data

Here are some tips and tricks that can be done to keep our personal data safe in the digital era:

1. Ensuring Data Is Encrypted
   Make sure that our personal data is encrypted when stored or transmitted over the internet. This may prevent unauthorised access to our personal data.
2. Be Careful When Using Wi-Fi Networks
   Avoid using public Wi-Fi networks that are not secure, as hackers can access your personal data through these networks. Use a secure Wi-Fi network or use a VPN to encrypt our internet connection.
3. Beware of Phishing Links
   Never click on links that are suspicious or come from unknown sources, as they could lead us to fake websites designed to steal our personal information.
4. Creating Hard-to-Guess Passwords
   Use passwords or passwords that are difficult to guess and avoid using the same password for different accounts. Use a combination of uppercase letters, numbers, and symbols to make passwords stronger.
5. Using Incognito Mode
   Use incognito mode when browsing the internet so that your browsing history is not stored in your browser. This may prevent others from viewing your browsing history.

[13] D. Puspa, A. Soegiharto, A. Nizar Hidayanto, and Q. Munajat, "Data Privacy, What Still Need Consideration in Online Application System?," *J. Sist. Inf.,* vol. 16, no. 1, pp. 49–63, 2020, doi: 10.21609/jsi.v16i1.941.

6. Always Be Careful in Granting Permissions
   Avoid granting access permissions to unknown or untrusted apps or websites. Read the terms and conditions carefully before granting access permission.[14]

By applying the tips and tricks above, we can keep our personal data safe in the digital age. In addition, we must also always be vigilant and careful in sharing personal information on social media or other online platforms. Avoid sharing ID card numbers, passports, boarding passes, bank account books, and any form of personal data on social media or other online platforms. Thus, we can minimize the risks to the security of our personal data in the digital age.

Conclusion

In today's digital era, the security of personal data is becoming increasingly important. Our personal data could fall into the wrong hands if it is not properly maintained. Therefore, we need to make efforts to protect our personal data. The personal data protection law has been created as an effort to provide protection or protection and provide a sense of security to the public. However, as users of digital technology, we must also remain vigilant and careful in providing our personal information.

Some tips and tricks that can be done to keep our personal data safe in the digital era include ensuring data is encrypted, being careful when using Wi-Fi networks, being aware of phishing links, creating passwords that are difficult to guess, using incognito mode, and always being careful in giving permissions. In an increasingly digital world, becoming smarter about data privacy is a crucial step for every professional. By implementing data protection strategies and improving digital skills, your data will not be misused.

References

D. Puspa, A. Soegiharto, A. Nizar Hidayanto, and Q. Munajat, “Data Privacy, What Still Need Consideration in Online Application System?,” J. Sist. Inf., vol. 16, no. 1, pp. 49–63, 2020, doi: 10.21609/jsi.v16i1.941.

D. Revilia and N. Irwansyah, “Social Media Literacy: Millenial’s Perspective of Security and Privacy Awareness,” J. Penelit. Komun. Dan Opini Publik, vol. 24, no. 1, pp. 1–15, 2020, doi: 10.33299/jpkop.24.1.2375.

Gunawan, “Pengukuran Kesadaran Keamanan Informasi Dan Privasi Dalam Sosial Media,” J. Muara Sains, *Teknol. Kedokteran dan Ilmu Kesehatan*, vol. 5, no. 1, p. 1, 2021, doi: 10.24912/jmstkik.v5i1.3456.

H. P. Yuwinanto, “Privasi online dan keamanan data,” Palimpsest (Iowa. City)., no. 031, p. 11, 2015.

[14] N. Aldhafferi, C. Watson, and S. A.S.M, “Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices,” Int. *J. Secur. Priv. Trust Manag.*, vol. 2, no. 2, pp. 1–17, 2013, doi: 10.5121/ijsptm.2013.2201.

John W. Creswell and Vicki L. Piano Clark, “Designing and Conducting Mixed Methods Research,” Aust. N. Z. J. Public Health, vol. 31, no. 4, 2007, doi: 10.1111/j.1753-6405.2007.00096.x.

L. Rizkinaswara, “Pahami Kebijakan Privasi di Media Sosial untuk Lindungi Data Pribadi,” https://aptika.kominfo.go.id/, 2019

M. M. AMANDA LENHART, “Social Networking Websites and Teens: An Overview,” 2008.

N. Aldhafferi, C. Watson, and S. A.S.M, “Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices,” Int. J. Secur. Priv. Trust Manag., vol. 2, no. 2, pp. 1–17, 2013, doi: 10.5121/ijsptm.2013.2201.

N. Aldhafferi, C. Watson, and S. A.S.M, “Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices,” Int. J. Secur. Priv. Trust Manag., vol. 2, no. 2, pp. 1–17, 2013, doi: 10.5121/ijsptm.2013.2201.

N. L. Leech and A. J. Onwuegbuzie, “A typology of mixed methods research designs,” Qual. Quant., vol. 43, no. 2, 2009, doi: 10.1007/s11135- 007-9105-3.

N. Senthil Kumar, K. Saravanakumar, and K. Deepa, “On Privacy and Security in Social Media - A Comprehensive Study,” Phys. Procedia, vol. 78, no. December 2015, pp. 114–119, 2016, doi: 10.1016/j.procs.2016.02.019.

R. T. Rust, P. K. Kannan, and N. Peng, “The customer economics of internet privacy,” Journal of the Academy of Marketing Science, vol. 30, no. 4. 2002, doi: 10.1177/009207002236917.

T. Agustin, “Analisis Keamanan Sistem Informasi Terhadap Data Pribadi di Media sosial,” 2020.

T. Islamy, S. T. Agatha, R. Ameron, B. H. Fuad, Evan, and N. A. Rakhmawati, “Pentingnya Memahami Penerapan Privasi di Era Teknologi Informasi,” *J. Teknol. Inf. dan Ilmu Komput.,* vol. 11, no. 2, pp. 21–28, 2018.