International Journal of Society Reviews (INJOSER) e-ISSN: 3030-802X
Vol. 2 No. 11, September 2025, pages: 2233~2244

DATA PRIVACY POLICY IN THE DIGITAL AGE: IMPLICATIONS, IMPLEMENTATION, AND IMPACT ON USERS

Gunawan Widjaja
Senior Lecturer Faculty of Law Universitas 17 Agustus 1945 Jakarta
widjaja_gunawan@yahoo.com

Abstract

The development of digital technology has brought significant changes in the management of personal information, making data privacy policies a crucial issue in the modern era. This study aims to analyse the implications, implementation, and impact of data privacy policies on users, emphasising the global and national contexts, particularly after the enactment of the Personal Data Protection Law (PDP Law) in Indonesia. The research approach used is descriptive qualitative with literature analysis. The results show that data privacy policies have broad implications, including strengthening fundamental individual rights, increasing corporate transparency, and creating new data security standards. However, their implementation faces challenges in the form of low digital literacy among the public, high compliance costs for companies, and potential user resistance to the complexity of the policies. The impact on users is twofold: on the one hand, it provides legal protection and a sense of security, but on the other hand, it creates a dilemma regarding ease of use and limited access to services. Therefore, the success of privacy policies requires synergy between adaptive regulations, digital corporate compliance, and increased digital literacy among the public in order to create a digital ecosystem that is secure, transparent, and fair.

Keywords: Data Privacy Policy, Digital Age, Implementation, Implications, Impact on Users, PDP Law.

Introduction

The development of digital technology over the past two decades has brought about major changes in social interaction patterns, economic transactions, and information management. The presence of the internet and digital devices has not only facilitated access to information, but also created new spaces for human activities in various fields of life (AM Junaedi, 2025) . The digital era has redefined the concepts of space and time because data can be transferred, processed, and distributed instantly across countries and even continents. In this context, data privacy has become one of the most widely discussed issues because the increasing dependence of humans on digital technology will always be directly proportional to the accumulation and exploitation of users' personal data (DNirwana, 2024) .

Data privacy is essentially a fundamental right of individuals that is closely related to freedom, security, and control over the personal information that each person possesses. However, in practice, the digital era has given rise to various major challenges, because personal data is often viewed as a "new commodity" that has high

economic value (KRA Suari, 2023b) . Global technology companies such as Google, Facebook, and Amazon, as well as most digital startups in Indonesia, use user data as the foundation for developing business strategies, marketing, and innovation artificial intelligence-based technology. This situation raises fundamental questions about the extent to which privacy policies can protect individual rights when faced with such dominant economic interests (DK Mohsin, 2020) .

Data privacy policies are an important instrument in providing clarity on the rules governing how personal data is collected, stored, used, and shared by digital service providers. On the one hand, these regulations serve as a legal protection instrument for users, but on the other hand, they also serve as guidelines for companies to conduct business activities while still paying attention to ethical and legal aspects (A. Natamiharja, 2024) . In other words, data privacy policies are not merely about the technical aspects of data storage, but also concern the power relations between users, service providers, and the state. These complex relations mean that the debate on data privacy is not only technological in nature, but also involves legal, ethical, economic, and even global political perspectives (SD Rosadi, 2018b) .

At the international level, the emergence of the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States became important milestones in the history of data privacy policy. These regulations became ideal models that were later adopted or modified by many countries, including Indonesia. With the enactment of the Personal Data Protection Law (PDP Law) in Indonesia in 2022, our country now officially has a more robust legal framework for regulating the protection of personal data. The PDP Law serves as a normative foundation that is expected to harmonise individual protection with the development of the digital economy in the country (OECD, 2024) .

However, the implementation of data privacy policies does not always run smoothly due to various obstacles, both in terms of user awareness and company readiness. Most users in Indonesia still have limited digital literacy, so they often do not understand the consequences of granting data access to certain applications or digital platforms (E. Muzairoh, 2024) . On the other hand, many digital companies, including start-ups, still find it difficult to meet privacy compliance standards due to limited resources, capital, and technical understanding. This shows that good policies do not necessarily guarantee effective data protection (A .

Another issue that is gaining traction is the increase in cases of personal data leaks affecting millions of users across various digital platforms. Data leaks not only cause material losses, but also undermine public trust in digital services. In recent years, Indonesia itself has been in the public spotlight due to repeated data leaks from large institutions, both private and government, which have raised serious questions about the effectiveness of the digital security systems implemented (A . This fact reinforces

the urgency of research on data privacy policies, particularly to assess the extent to which existing regulations are truly capable of providing real protection for users.

In addition to data leaks, another challenge is the emergence of data misuse for purposes that exceed its original utility, such as user profiling, behaviour-based advertising, and political opinion manipulation through micro-targeting. The phenomenon of data-based political manipulation, as seen in the Cambridge Analytica scandal, shows how personal data can be used to influence the social and political behaviour of society. This proves that the impact of data privacy policies is not limited to the individual sphere, but also touches on the stability of democracy and the social system as a whole (A .

On the other hand, overly strict privacy regulations also have their own consequences, namely the potential to hamper digital innovation and data-driven economic growth. Many digital companies argue that highly restrictive privacy policies will slow down the development of big data, artificial intelligence, and the Internet of Things (IoT) technologies, due to limited access to user data, which is a key requirement for these technologies. This dilemma has sparked academic and practical debate: how to balance the protection of user rights with the needs of the data-driven digital industry (KRA Suari, 2023a) .

Based on this reality, this study is relevant to further explore the implications, implementation, and impact of data privacy policies on users amid the dynamics of the digital era.

Research Method

The research method used in this study is a descriptive qualitative approach utilising literature analysis as the main source of data. Data was collected through document review, scientific journals, legal regulations such as the Personal Data Protection Act (PDP Act), as well as reports on data breaches and the implementation of privacy policies in several digital companies (Eliyah & Aslan, 2025) . The analysis technique was carried out using a *content analysis* approach to identify patterns, implications, and challenges in the implementation of privacy policies, which were then compared with international practices such as the GDPR and CCPA to obtain a more comprehensive picture. The validity of the research was maintained through source triangulation by confirming the findings from various different references so that the results of the study could be academically accountable (Green et al., 2006) .

Results and Discussion

Implications of Data Privacy Policy in the Digital Age

Data privacy policies in the digital age have fundamental implications for the management of users' personal information in cyberspace. At the very least, they serve as a legal instrument that regulates how data is collected, processed, distributed, and

destroyed after it is no longer used. Thus, the existence of this policy not only provides normative protection, but also provides clear binding rules for digital companies operating within a specific legal scope. The first clear implication is the formation of a more robust legal foundation for protecting individual rights amid the increasingly massive flow of digitalisation (J .

Data privacy as a fundamental right of individuals is no longer merely an ethical issue, but has become a global legal issue. The implementation of the General Data Protection Regulation (GDPR) in the European Union, for example, has placed data privacy as an important part of human rights. The implication is that every company operating in Europe must be fully committed to high standards of protection, without exception, even if the company is based outside Europe. This shows that data privacy policies have extraterritorial implications that can affect cross-border business practices (DNovira, 2024) .

In the Indonesian context, the enactment of the Personal Data Protection Act (PDP Act) in 2022 has brought both positive implications and new challenges. On the positive side, the Act provides stronger legal protection for citizens in maintaining authority over their personal data (I Lutrianto, 2025) . However, on the other hand, there are significant consequences for electronic system operators who are required to adjust their internal policies, security infrastructure, and service standards to the new regulations. This indicates that privacy policies not only affect users, but also the operational strategies of companies (SD Rosadi, 2018a) .

One important implication of privacy policy is the increased obligation of transparency for digital companies. Every service provider is required to clearly inform the type of data collected, its purpose of use, third parties who have access rights, and the storage period. This openness demands a change in corporate culture, where companies can no longer hide data processing practices behind complicated clauses. As a result, users are given the legitimacy to assess the extent to which privacy protection is actually implemented by service providers (R Dhianty, 2022) . In addition to transparency, privacy policies also have implications for improving data security standards. Digital companies no longer have the option of simply storing data, but are required to maintain its security through encryption systems, multi-layered authentication, and regular security audits. The implementation of high security standards certainly requires significant investment, so for small companies or digital startups, this can be an additional burden. However, the consequences must be complied with because negligence in protecting user data now has legal implications, including significant fines (W .

The implications of privacy policies are also evident in the changing relationship between users and service providers. Before strict regulations were put in place, many users felt powerless when their data was harvested and used for business purposes without their explicit consent. Now, with the existence *of consent* mechanisms, users

have a stronger bargaining position to determine who has the right to access their data. The concept *of informed consent* has become an important instrument that respects individual sovereignty over data (Syafiq Muhammad Al Fahri, 2023a) .

On the other hand, data privacy policies have led to increased public awareness of the importance of personal data protection. These policies educate users that digital data is not limited to names and addresses, but also includes shopping preferences, search histories, and location traces. This awareness encourages changes in digital behaviour, such as being cautious in granting access permissions to applications or the habit of using double security features. In other words, data privacy policies can create a healthier digital literacy culture (Syafiq Muhammad Al Fahri, 2023b) .

However, this increased awareness also brings consequences in the form of user resistance to corporate practices. Many users are now more selective in choosing digital services and are questioning the legality of applications that are not transparent about their use of data. This is forcing companies to review their business approaches based on data exploitation. The commercial implications are clear: a company's reputation and sustainability are now largely determined by the extent to which they comply with privacy regulations (RNatamiharja, 2024) .

Data privacy policies also have implications for global competition between technology companies. Companies that are able to comply with strict privacy standards will gain greater trust from users and regulators, thereby gaining a stronger competitive edge. Conversely, companies that fail to comply or are involved in data breach scandals will face financial and reputational losses. These implications create *a* new *competitive advantage*, where privacy compliance becomes a key factor in building customer loyalty (HPazhohan, 2023) .

In the political sphere, privacy policies have important implications for maintaining democratic stability. Regulations that restrict data access for political purposes can prevent opportunities for public opinion manipulation through micro-targeted political advertising. Thus, data privacy is not only a matter of individual rights, but also collective protection of political integrity. This means that the government has a great responsibility to ensure that privacy policies are implemented fairly without curtailing freedom of expression in the digital space (G .

In the economic sector, privacy policies can have paradoxical implications. On the one hand, they restrict excessive commercial practices based on data exploitation, but on the other hand, they encourage the creation of new opportunities in the cybersecurity industry, compliance consulting, and encryption technology. This new market creates a business ecosystem focused on privacy protection solutions, thereby opening up new job opportunities while balancing the economic losses that may arise from restrictions on data utilisation (IEEE, 2025) .

Another equally important implication is the emergence of a new ethical dimension in technological innovation. For example, in the development of artificial

intelligence or big data, researchers and developers must now consider privacy aspects from the design stage, known as the principle *of privacy by design*. This paradigm shift means that ethical aspects are no longer an addition, but a fundamental part of every innovation. Thus, the implications of privacy policy are not only legal, but also touch on moral and professional dimensions (RSegijn et al., 2024) . Furthermore, at the international level, privacy policy has implications for cooperation between countries in managing cross-border data flows. Bilateral and multilateral agreements on data protection are increasingly needed to ensure that cross-border data transfers do not threaten individual privacy. With the increasing globalisation of digital activities, uniform regulations on privacy are urgently needed to prevent legal conflicts between different jurisdictions (AK Conduah, 2025) .

Overall, the implications of data privacy policy in the digital age are vast and multidimensional, covering legal, social, economic, political, and ethical aspects. Its presence is not merely a technical instrument, but part of efforts to create a more equitable, secure, and responsible digital ecosystem. However, these implications also require the alignment of interests between the state, companies, and society so that no single party benefits at the expense of others. In other words, the success of data privacy policies depends not only on the quality of regulations, but also on collective awareness to respect privacy values amid the rapid pace of global digitalisation.

Implementation and Impact on Users

The implementation of data privacy policies in the digital age is not only a matter of formulating rules, but also concerns how these rules are implemented by various parties involved in the digital ecosystem. Regulations such as the Personal Data Protection Law (PDP Law) in Indonesia or the GDPR in the European Union provide a clear legal framework, but their effectiveness is largely determined by the compliance of digital service providers in managing user data. Good implementation will increase public trust in digital services, while poor implementation will damage the company's image and create new vulnerabilities (J .

One of the most striking aspects of implementation is information disclosure or transparency to users. Digital companies are required to formulate privacy policies that are simple, clear, and easy to understand. However, in practice, many companies still use legal language or technical terminology that is quite complicated, making it difficult for ordinary users to understand. This has an impact on the low level of public awareness of their rights, because even though information about data usage is available , this information is not always accessed or fully understood (A .

In addition to transparency, the implementation of privacy policies also includes mechanisms for user consent. The principle *of informed consent* means that users have the right to know in detail how their data will be used before giving their permission. On many global digital platforms, *consent management* is implemented through pop-ups,

checkboxes, or notifications that require users to give explicit consent. As a result, users now have more bargaining power. However, on the other hand, some users feel burdened by the repeated requests for consent, which leads to "*privacy fatigue*" (TY Manurung, 2024) .

The implementation of privacy policies has a direct impact on how companies design their digital security systems. Many companies now incorporate encryption systems, double authentication, and *end-to-end encryption* features into their services. This significantly improves the security of users' personal data, but also adds technical complexity to the use of services. As a result, some users feel that their digital experience has become less convenient, especially when they have to go through multiple security procedures for simple activities (WD Cahyani, 2024) .

From the user's perspective, the implementation of privacy policies has an impact on increasing the sense of security in using digital platforms. Personal data is no longer completely vulnerable to exploitation due to the existence of legal standards that protect it. However, this sense of security is often illusory if implementation is not accompanied by strict supervision. For example, even though companies have included data protection clauses, many cases of data leaks still occur due to weak security infrastructure or weak audit mechanisms (E Muzairoh, 2024) .

In Indonesia, the implementation of the PDP Law has important consequences for users, namely the existence of new rights that they can claim. These rights include the right to access personal data, the right to correct data errors, the right to withdraw consent, and the right to *be forgotten*. The implementation of these rights in practice is still limited, but at least it provides a new perspective that users are not merely passive objects, but subjects who have authority over their own data (A . However, the impact on users also includes negative aspects. The implementation of privacy policies often results in restricted access to certain features if users refuse to give data permission. This situation forces some users to surrender their personal data even though they are uncomfortable doing so, just to gain full access to the service. Thus, although privacy policies strengthen individual rights, in practice there is still a dilemma between privacy compliance and convenience in using digital applications (J .

In addition, the implementation of privacy policies has had a significant impact on the digital literacy of the public. Through socialisation and campaigns regarding the Personal Data Protection Act (PDP Act) or similar regulations , users have become increasingly aware that personal data is a valuable asset. The impact of this is a growing sense of caution, such as being more selective in using public Wi-Fi networks, being more diligent in changing passwords, or refusing to give permission to overly invasive applications. The long-term implication of this impact is the creation of a more prudent and responsible digital culture (AK Conduah, 2025) .

On the corporate side, the implementation of privacy policies also creates an unavoidable additional burden. Adjusting security systems, establishing compliance

units, and recruiting data security experts incur high operational costs. As a result, some companies pass on the additional costs to users by raising service prices or offering paid packages with better data protection. This impact is then felt by users, who are often faced with the choice between free ad-based services and premium services with higher privacy (RSegijn et al., 2024) .

Another impact of implementing privacy policies is increased public trust in services that comply with regulations. Companies that are considered capable of protecting user data tend to be more trusted, thereby increasing customer loyalty. This trust is valuable social capital, especially in an era of information openness when data breach issues quickly spread through mass media and social media. In other words, a company's compliance with privacy policies has a direct impact on the reputation of its services in the eyes of users (G .

However, user trust is also very fragile. A single case of data leakage that is exposed to the public can destroy an image that has been carefully built up over many years. For users, the real impact of implementation failures is increased vulnerability to identity theft, digital fraud, and the exploitation of personal data for economic or political gain. Therefore, even the smallest weakness in the implementation of privacy policies can have serious consequences for the public trust that has been so hard to earn (HPazhohan, 2023) .

The implementation of privacy policies also has an impact on the relationship between countries, companies, and individuals. Countries have an obligation to monitor companies to ensure they comply with regulations, while companies are required to comply with the rules without compromising service quality. For users, the impact of this relationship is the emergence of new opportunities for participation, for example through official complaint mechanisms when personal data is misused. The existence of these mechanisms makes users feel more protected, although their effectiveness still depends on the law enforcement system (R Natamiharja, 2024) . In addition, the implementation of data privacy policies opens up new discussions related to business ethics and corporate social responsibility. For users, the impact is a clearer expectation that companies are not only profit-oriented but also have a moral responsibility to protect the dignity and rights of individuals. Companies that are able to demonstrate an ethical commitment to privacy will gain public support , while companies that are negligent will be abandoned by their users (Syafiq Muhammad Al Fahri, 2023b) .

Overall, the implementation of data privacy policies has a broad and ambivalent impact on users. On the one hand, it provides increased protection and strengthens individuals' bargaining position in managing their personal data. However, on the other hand, it also poses challenges in the form of limited access, increased service costs, and technical complexities that make it difficult for some users. This shows that the successful implementation of privacy policies requires a balance between legal

compliance, ease of use, and public awareness, so that the digital ecosystem can develop in a fair, sustainable, and human-protection-oriented manner.

Conclusion

Data privacy policies in the digital age play a central role in maintaining a balance between protecting individual rights and the interests of the digital industry. The implications of these policies are evident in the strengthening of legal legitimacy, increased demands for transparency, and the emergence of new security standards that companies are required to implement. However, privacy policies also create ethical and practical dilemmas, especially when data protection potentially conflicts with big data and artificial intelligence-based innovations. Thus, the existence of privacy policies not only provides legal certainty, but also presents new challenges at the global, regional, and local levels.

From an implementation perspective, privacy policies have a tangible impact on users and service providers. Users now have stronger rights over their personal data, including the right to know, control, and even delete data that is no longer relevant. As a result, public awareness of digital issues has begun to increase, although it is still limited to certain groups. On the other hand, digital companies face enormous pressure as they are required to adapt their infrastructure, *consent* mechanisms, and data security to stricter standards. This shows that the implementation of privacy policies does not always run smoothly, but requires harmony between regulations, corporate readiness, and public digital literacy.

Overall, data privacy policies in the digital age have a broad impact, legally, socially, economically, and ethically. Their success depends on three main factors: solid and adaptive regulatory quality, consistent implementation by companies, and increased digital literacy among the public as users. Without synergy between these three factors, privacy policies will merely be legal texts that are ineffective in protecting users. Therefore, a shared commitment between the state, companies, and society is needed to build a digital ecosystem that is secure, transparent, fair, and continues to support innovation amid the rapid pace of global technological development.

References

A. F. Yamin, A. R., R. A. Pratama, J. K. Wijaya. (2024). Perlindungan Data Pribadi dalam Era Digital: Tantangan dan Solusi. *Meraja Journal*. https://merajajournal.com/index.php/mrj/article/download/352/297/

A. Fujimori-Smith. (2024). *Analysis of Global Data Privacy Regulations and Enforcement*. https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1696&context=chtlj

A. Natamiharja. (2024). *Protection of Privacy Rights in The Digital Era Between Indonesia and France*. https://doi.org/10.22437/home.v7i1.349

A. Putri. (2025a). Pentingnya Perlindungan Data Pribadi di Era Digital: Studi Kasus Desa Pematang Jering. *Jurnal Pengembangan Dan Inovasi*. https://journal.stmiki.ac.id/index.php/jpni/article/view/1097

A. Putri. (2025b). *Perlindungan Data Pribadi di Era Digital: Studi Kasus Desa Pematang Jering*. https://journal.stmiki.ac.id/index.php/jpni/article/view/1097

AK Conduah. (2025). Data Privacy in Healthcare: Global Challenges and Solutions. *PMC*. https://doi.org/10.1371/journal.pmed.12138216

AM Junaedi. (2025). Urgensi Perlindungan Data Pribadi dalam Era Digital. *Jurnal Knowledge*. https://doi.org/10.31258/knowledge.5269

D. Nirwana. (2024). Studi Kasus Implementasi Perlindungan Data Pribadi di Era Digital. *Jurnal Ilmu Ilmu Politik (JIIP)*.

D. Novira. (2024). *Legal Protection of Children's Personal Data in the Digital Era*. https://doi.org/10.36713/ijsr.v15i8.2195

DK Mohsin. (2020). *Right to Privacy in Digital Era*. https://doi.org/10.2139/ssrn.3678224

E Muzairoh. (2024). *Analisis Perlindungan Hukum Terhadap Privasi Data Pribadi di Era Digital*. https://journal.unimma.ac.id/index.php/blastal/article/view/11824

E. Muzairoh. (2024). *Perlindungan Privasi Data Pribadi: Perspektif Hak Asasi Manusia*. https://journal.unimma.ac.id/index.php/blastal/article/view/11824

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

G. Greenleaf. (2023). *Global Data Privacy Laws 2023: 162 National Laws and 20+ Trends*. https://doi.org/10.2139/ssrn.4426146

Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing Narrative Literature Reviews for Peer-Reviewed Journals. *Chiropractic & Manual Therapies*, 52–57.

H. Pazhohan. (2023). *Global Data Protection Standards: A Comparative Analysis of GDPR and Other International Laws*. https://doi.org/10.56937/jlsda.v1i1.17

I Lutrianto. (2025). *Legal Problems of Personal Data Protection in The Digital Era*. https://doi.org/10.38035/gijlss.v3i2.429

IEEE. (2025). *Global Adoption of Data Privacy Laws and Regulations*. https://digitalprivacy.ieee.org/publications/topics/global-adoption-of-data-privacy-laws-and-regulations/

J. Jamal. (2023). *Data Privacy and Protection in the Digital Era*. https://doi.org/10.4172/2324-9307.1000276

J. Wang. (2021). *Managing Privacy in the Digital Economy*. https://doi.org/10.1016/j.dig.2021.100155

KRA Suari. (2023a). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi. *Jurnal Analisis Hukum*. https://journal.undiknas.ac.id/index.php/JAH/article/download/4484/1337/12318

KRA Suari. (2023b). *Studi Implementasi Kebijakan Privasi Data di Era Digital*. https://journal.undiknas.ac.id/index.php/JAH/article/download/4484/1337/12318

OECD. (2024). *Privacy and Data Protection*. https://www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html

R Dhianty. (2022). Kebijakan Privasi, Platform Digital, Data Pribadi. *Scripta: Jurnal Kebijakan Publik Dan Hukum*. https://doi.org/10.36588/scripta.v2i1.16

R. Natamiharja. (2024). *Guarding Privacy: Comparative Analysis Indonesia—France*. https://doi.org/10.22437/home.v7i1.349

R Natamiharja. (2024). Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France. *Jambe Law Journal*. https://doi.org/10.22437/home.v7i1.349

R. Segijn et al. (2024). *Enforcement and Challenges of Data Privacy Laws around the World*. https://wjarr.com/sites/default/files/WJARR-2024-0369.pdf

SD Rosadi. (2018a). *Legal Framework in Protecting Data Privacy in Digital Era*. https://doi.org/10.21776/ub.blj.2018.005.01.09

SD Rosadi. (2018b). Protecting Privacy On Personal Data In Digital Economic Era: Legal Framework In Indonesia. *Brawijaya Law Journal*, 5(1), 143–159. https://doi.org/10.21776/ub.blj.2018.005.01.09

Syafiq Muhammad Al Fahri. (2023a). *Implementasi Kebijakan Privasi Terhadap Data Pribadi Pengguna E-Commerce Ditinjau Dari UU No 27 Tahun 2022 (Studi Kasus Lazada)* [Fakultas Syariah dan Hukum, UIN Syarif Hidayatullah Jakarta]. https://repository.uinjkt.ac.id/dspace/bitstream/123456789/73052/1/SYAFIQ%20MUHAMMAD%20AL%20FAHRI%20-%20FSH.pdf

Syafiq Muhammad Al Fahri. (2023b). *Implementasi Kebijakan Privasi Terhadap Data Pribadi Pengguna E-Commerce Ditinjau Dari UU No 27 Tahun 2022 (Studi Kasus Lazada)* [Fakultas Syariah dan Hukum, UIN Syarif Hidayatullah Jakarta]. https://repository.uinjkt.ac.id/dspace/bitstream/123456789/73052/1/SYAFIQ%20MUHAMMAD%20AL%20FAHRI%20-%20FSH.pdf

TY Manurung. (2024). Analisis Hukum tentang Kebijakan Privasi Data di Era Digital. *Jurnal Fakum*. https://coursework.uma.ac.id/index.php/fakum/article/view/1257

WD Cahyani. (2024). *Analisis Kebijakan Perlindungan Data Pribadi Di Kota*. https://doi.org/10.62379/s5424t73

W.D. Cahyani. (2024). *Kebijakan Perlindungan Data Pribadi di Kota*. https://doi.org/10.62379/s5424t73