Jurnal Komunikasi
Vol. 3 No. 4 April 2025, hal. 161-167 e-ISSN: 2988-1331

THE IMPACT OF BIG DATA ON INDIVIDUAL PRIVACY: LEGAL ANALYSIS AND PROTECTION POLICIES

Gunawan Widjaja
Senior Lecturer Faculty of Law Universitas 17 Agustus 1946 Jakarta
widjaja_gunawan@yahoo.com

Hotmaria Hertawaty Sijabat
Doctoral Student Faculty of Law Universitas 17 Agustus 1945 Jakarta,
sijabathotmaria@gmail.com

Abstract

The development of big data technology has had a significant impact on various aspects of life, including individual privacy. This phenomenon allows for the collection, analysis, and dissemination of large amounts of data, which often involves personal information. This impact poses serious challenges in protecting individual privacy rights due to the unauthorised use of data which can lead to the misuse of information. This study explores the dynamics and implications of big data on individual privacy, including an analysis of existing policies and legal regulations. Several regulations such as the GDPR in the European Union, the CCPA in the United States, and the Personal Data Protection Act in Indonesia have become an important foundation for the protection of individual rights in the management of personal data. However, the effective implementation of regulations remains a major challenge given the rapid pace of technological development and data growth. Thus, this study emphasises that privacy protection in the big data era requires a holistic approach that includes strict regulation, the application of security technologies such as encryption and anonymisation, and public education about the importance of data privacy. Only with global collaboration and continuous efforts can people enjoy the benefits of big data while maintaining the privacy rights of each individual.

Keywords: Impact, Big Data, Individual Privacy, Legal Analysis, Protection Policy.

Introduction

The rapid development of technology has brought significant changes in various aspects of human life. One technological innovation that has had a major impact is Big Data. Big Data is a very large and complex set of data that cannot be managed with traditional data processing methods. This data can come from various sources, such as social media, online transactions, IoT sensors, and so on. With the right analysis, Big Data can provide deep insights that are useful for decision making in various sectors such as business, health, education, and government (Friedman, 2019).

The development of Big Data technology is inseparable from the ability to collect, store, and process very large amounts of data from various diverse sources. In the last decade, the growth of social media, Internet of Things (IoT) devices, and online business transactions has resulted in a surge in data in various formats, from text,

images, videos, to sensor data. The volume of data generated from these various activities continues to increase exponentially, presenting both challenges and opportunities for many industry sectors (Solove, 2008).

Advances in computing and storage technologies, such as Hadoop, Spark, and cloud computing, enable Big Data processing to be more efficient and widely accessible to various organisations. In addition, the development of machine learning and artificial intelligence algorithms has paved the way for more in-depth and predictive data analysis (Zarsky, 2017). The implementation of Big Data is now not only limited to data analysis for operational improvement, but is also used to create product and service innovations, understand consumer behaviour, and optimise overall business decisions. Thus, Big Data technology continues to experience rapid development, having a significant impact on various aspects of human life (Spiekermann & Korunovska, 2017).

However, behind the great potential offered by Big Data, there are growing concerns regarding individual privacy. The collection, storage, and analysis of data on a large scale often involves sensitive personal information. This poses various risks, including data misuse, identity theft, and privacy violations. In this digital era, individuals are beginning to realise that their personal data is a valuable asset that needs to be protected from unethical exploitation (Felten & Schneider, 2000).

Personal data plays a very important role in maintaining the security of individuals and organisations. Personal data, such as names, addresses, identification numbers, and financial information, can be used to uniquely identify a person and protect their identity from misuse. Proper management and protection of personal data reduces the risk of identity theft, fraud, and increasingly prevalent cybercrime (Lepri & Staiano, 2017). In addition, regulations such as the GDPR (General Data Protection Regulation) in Europe and the Personal Data Protection Act in various countries aim to ensure that personal data is processed safely and ethically. By recognising the importance of personal data and taking steps to protect it, individuals and organisations can increase trust in a digital environment that is increasingly complex and vulnerable to security threats (Contissa et al., 2017).

In addition, existing privacy protection regulations and policies are often considered inadequate or lagging behind technological developments. Although some countries have taken steps forward by adopting stricter regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, many other countries, including Indonesia, still face challenges in drafting and implementing effective policies (Lyon, 2007).

This challenge is compounded by the conflict between technological innovation and privacy protection. On the one hand, technology companies continue to push the boundaries of innovation to improve services and operational efficiency. On the other hand, the importance of protecting individual privacy must be maintained. Therefore, a

careful balance is needed between utilising the potential of Big Data and protecting individual privacy rights (Narayanan & Shmatikov, 2008).

Therefore, seeing the urgency of this problem, this study aims to analyse the impact of Big Data use on individual privacy and evaluate existing legal regulations and policies.

Research Methods

The study in this research uses the literature method. The literature research method is a research approach that collects, reviews, and analyses existing scientific works and written sources to group and understand information relevant to a particular research topic. This method is used to identify gaps or deficiencies in the literature, explore existing perspectives and findings, and build a strong conceptual framework based on the evidence gathered (Boote & Beile, 2005); (Carnwell & Daly, 2001). This process involves a systematic search of the literature through academic databases, a critical assessment of the quality and relevance of the sources found, and a synthesis of information to draw conclusions that can support or challenge the initial research hypothesis. Overall, literature research helps to form a solid theoretical basis for further research and ensures that the latest research is based on existing knowledge (Boote & Beile, 2005).

Results and Discussion

The Impact of Big Data Use on Individual Privacy

Big Data, which refers to the collection, storage, and analysis of large amounts of data, has revolutionised various sectors such as business, healthcare, and government. However, its use also raises serious concerns about individual privacy. The main impact of Big Data use on individual privacy can be seen from various perspectives, including data collection, data storage, and data analysis and use (Kosinski et al., 2013).

First, in terms of data collection, Big Data often involves massive data retrieval from various sources, including social media, financial transactions, IoT (Internet of Things) devices, and so on. This process is sometimes carried out without the knowledge or explicit consent of individuals, which poses a risk of privacy violations. Individuals may not be aware of how much data is collected about them and how it is used (Tene & Polonetsky, 2012).

Second, storing large volumes of data also carries its own risks. Insecure storage can lead to massive data leaks when accessed by irresponsible parties. Data leaks can result in identity theft, fraud, and a variety of other cybercrimes that can harm individuals both financially and emotionally (Rost & Bock, 2011).

Third, Big Data analysis allows organisations to identify patterns, trends and individual behaviour with a high degree of accuracy. While this can be used for beneficial purposes, such as consumer preferences or personalised healthcare, there is also

potential for misuse. Predictive analytics can lead to highly detailed profiles of individuals that can be used for discrimination, manipulation or unfair decision-making (Nissenbaum, 2004).

Fourth, the use of analysed data can violate individual privacy in various ways. For example, companies can sell or share personal data with third parties without permission. With this highly detailed data, marketing companies can target advertisements in ways that individuals may find offensive. Furthermore, governments that have access to Big Data can misuse it to conduct invasive surveillance (World Economic Forum, 2011).

Fifth, transparency and individual involvement in how their data is processed are often inadequate. Many users do not have full control or sufficient information about how their data is collected, stored, analysed and used. Complex and difficult-to-understand privacy policies also contribute to the lack of user involvement and understanding (Sweeney, 2002).

Sixth, there are also issues related to data anonymity. Although data can be anonymised to protect privacy, there are cases where anonymised data can be identified using certain techniques. This shows that data anonymisation is not fully effective and that the risk to privacy still exists even after attempts to remove personally identifiable information (Zarsky, 2017).

Seventh, despite data protection regulations and laws in various countries, their implementation is often not fast enough to keep pace with the development of Big Data technology. Regulations such as the GDPR in Europe are a good first step, but enforcement remains a challenge, especially in a global digital era involving complex cross-border jurisdictions (Solove, 2008).

Thus, the use of Big Data brings many potential benefits, but also great risks to individual privacy. It is important for all parties involved to consider and address these challenges seriously through more transparent policies, effective regulations, and privacy-protecting technologies, to ensure that the benefits of Big Data can be achieved without compromising individual privacy rights.

Legal Regulations Regarding Privacy in the Big Data Era

In the era of big data, legal regulations regarding privacy are becoming increasingly important due to the increasing volume, variety, and speed of data generated and processed. Personal data is now collected from various daily activities, from online shopping to the use of social media, health services, and IoT (Internet of Things) devices. This situation requires strict regulations to protect individual privacy rights and prevent the misuse of personal data (Acquisti et al., 2019).

One of the main regulations governing data privacy is the General Data Protection Regulation (GDPR) in the European Union, which came into effect in May 2018. The GDPR is a comprehensive regulation that requires companies to be

transparent in collecting, processing, and storing the personal data of European citizens. This includes explicit consent from individuals before their data is collected and the right to access, correct, or delete that data (Dwork, 2006).

In the United States, data privacy regulations are more fragmented with various federal and state laws. For example, the California Consumer Privacy Act (CCPA), which came into effect in January 2020, gives consumers the right to know what information companies collect, control the distribution of data, and request the deletion of their personal data. However, there is no federal regulation as comprehensive as GDPR in the US (Ziccardi, 2018).

Indonesia is also not lagging behind in responding to this development by passing the Personal Data Protection Law (PDP Law) in 2022. The PDP Law regulates the rights of individuals regarding their personal data, the obligations of data controllers, and sanctions for violations. This regulation aims to improve the protection of the collection, storage, and processing of personal data in Indonesia (Kukar & Kononenko, 1998).

One of the main challenges in implementing data privacy regulations is the global scope of business in this digital era. Many companies that operate internationally must comply with different regulations in each country or region, which sometimes conflict with each other. This requires closer international cooperation and a harmonised framework to ensure privacy protection without hampering the flow of data that is essential for the digital economy (Christl, 2017).

In addition to government regulations, the private sector is also taking steps to improve data privacy and security through the implementation of international standards such as ISO/IEC 27001 for information security management systems. These standards help organisations assess risk, establish security controls, and comply with applicable privacy regulations (Zuboff, 2015).

Technology also plays an important role in protecting data privacy. Methods such as encryption, tokenisation, and anonymisation can be used to protect personal data when it is processed and stored. Companies need to adopt this technology as part of their privacy compliance policies to ensure that data remains protected at every stage of its life cycle (Mayer-Schönberger, 2009).

Ultimately, education and public awareness of data privacy are equally important. Users must understand their rights to personal data and how to protect their information from misuse. With collaboration between the government, the private sector, and the general public, we can create a digital environment that is safe and respects individual privacy amid the development of big data.

Conclusion

The era of big data has presented significant challenges to individual privacy, where personal information is very easily collected, analysed and disseminated on an

unprecedented scale. Companies and organisations use large amounts of data to increase efficiency, create new products and services, and improve the consumer experience. However, without adequate regulation, this can lead to privacy violations that endanger individuals.

To address these challenges, various legal regulations have been introduced in various parts of the world. Regulations such as GDPR in the European Union and CCPA in the United States have established a strict framework to protect individual privacy by requiring transparency and explicit permission from individuals before their data is used. In Indonesia, the Personal Data Protection Act provides a basis for the protection of individual rights in the context of the collection and use of personal data. Collectively, these regulations play an important role in providing clear boundaries on how personal data should be processed and safeguarded.

However, the success of these privacy protection efforts requires global collaboration and the application of sophisticated security technologies. Technologies such as encryption and anonymisation can be essential tools for protecting data, while public education is needed to raise awareness of the importance of data privacy. Only with a holistic approach involving strict regulation, cutting-edge technology and public awareness can the negative impact of big data on individual privacy be minimised, enabling the benefits of big data to be enjoyed while maintaining individual privacy rights.

References

Acquisti, A., Gritzalis, S., & Lambrinoudakis, C. (2019). Digital Privacy: Theory, Technologies, and Practices. *ACM Computing Surveys*, *51*(1), 1–36. https://doi.org/10.1145/3318094

Boote, D. N., & Beile, P. (2005). Scholars Before Researchers: On the Centrality of the Dissertation Literature Review in Research Preparation. *Educational Researcher*, *34*(6), 3–15.

Carnwell, R., & Daly, W. (2001). Strategies for the Construction of a Critical Review of the Literature. *Nurse Education in Practice*, *1*(2), 57–63.

Christl, W. (2017). Corporate Surveillance in Everyday Life. *Cracked Labs Research Report*. https://doi.org/10.5281/zenodo.3243058

Contissa, G., Lagioia, F., & Sartor, G. (2017). The Ethical Knob: Ethically Customizable Automated Vehicles and the Law. *Artificial Intelligence and Law*, *25*(3), 365–378. https://doi.org/10.1007/s10506-017-9211-z

Dwork, C. (2006). Differential Privacy. *IEEE Symposium on Security and Privacy*, 1–12. https://doi.org/10.1109/SP.2006.36

Felten, E. W., & Schneider, M. A. (2000). Timing Attacks on Web Privacy. *ACM Conference on Computer and Communications Security*, 25–32. https://doi.org/10.1145/352600.352606

Friedman, B. (2019). *Value-Sensitive Design: Shaping Technology with Moral Imagination*. MIT Press. https://doi.org/10.7551/mitpress/12088.001.0001

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private Traits and Attributes are Predictable from Digital Records of Human Behavior. *PNAS*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

Kukar, M., & Kononenko, I. (1998). Cost-Sensitive Learning with Neural Networks. *IEEE Transactions on Neural Networks*, *10*(1), 155–166. https://doi.org/10.1109/72.737491

Lepri, B., & Staiano, J. (2017). The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good. *ACM Transactions on Management Information Systems*, *8*(4), 1–20. https://doi.org/10.1145/3093239

Lyon, D. (2007). *Surveillance Studies: An Overview*. Polity. https://doi.org/10.1111/j.1540-5931.2008.00382.x

Mayer-Schönberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press.

Narayanan, A., & Shmatikov, V. (2008). Robust De-anonymization of Large Sparse Datasets. *IEEE Symposium on Security and Privacy*, 111–125. https://doi.org/10.1109/SP.2008.33

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 119. https://doi.org/10.2307/1602638

Rost, M., & Bock, K. (2011). Privacy by Design and the New Protection Goals. *DuD - Datenschutz Und Datensicherheit*, *35*(2), 68–72. https://doi.org/10.1007/s11623-011-0123-0

Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

Spiekermann, S., & Korunovska, J. (2017). Towards a Value Theory for Personal Data. *Journal of Information Technology*, *32*(1), 62–84. https://doi.org/10.1057/s41265-017-0047-7

Sweeney, L. (2002). k-Anonymity: A Model for Protecting Privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(5), 557–570. https://doi.org/10.1142/S0218488502001648

Tene, O., & Polonetsky, J. (2012). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online*, *64*, 63. https://doi.org/10.2139/ssrn.2163735

World Economic Forum. (2011). *Personal Data: The Emergence of a New Asset Class*.

Zarsky, T. Z. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, *47*(4), 995–1020.

Ziccardi, G. (2018). Data Protection and Compliance in Context of Big Data: The General Data Protection Regulation's Principles. *IEEE Transactions on Big Data*, *4*(1), 55–63. https://doi.org/10.1109/TBDATA.2018.2809941

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5