Journal of Central Banking Law and Institutions, Vol. 1 No. 2, 2022, pp. 353 - 366
e-ISSN: 2809-9885
https://doi.org/10.21098/jcli.v1i2.18

PROTECTION OF DATA PRIVACY IN THE ERA OF ARTIFICIAL INTELLIGENCE IN THE FINANCIAL SECTOR OF INDONESIA

Sinta Dewi Rosadi,[a] Siti Yuniarti,[b] Rizki Fauzi[c]
[ac]Faculty of Law, Universitas Padjadjaran,
[b]Faculty of Law, Universitas Bina Nusantara, Indonesia
e-mail: : sinta@unpad.ac.id (corresponding author);. yuniarti@binus.ac.id; rizkifau01@gmail.com

Abstract

The concept of privacy has broad ramifications, and it is implemented in several disciplines, ranging from philosophy to computer science, political science, and legal science. This paper covers the impact of artificial intelligence on privacy protection, especially in the finance sector. Privacy protection is associated with control over information about personal data, also known as private information. This research is normative legal research of analytical nature, and it is conducted by studying and interpreting theoretical matters relating to the principles, conceptions, doctrines and legal norms pertaining to the problems. The results of this research show that the concept of privacy in the era of artificial intelligence in Indonesia is best achieved by combining comprehensive rules with self-regulation to serve as a balancing agent between laws and technology to control and fulfill the protection of personal data in the era of artificial intelligence.

Keywords: *privacy, artificial intelligence, financial sector*

I. INTRODUCTION

Artificial Intelligence (AI) is a critical aspect of the fourth industrial revolution, and, today, it has rapidly developed around the globe. In recent years, AI tools are not best utilised by non-public sector, the public sector is likewise making use of them, such that AI is now used in many of the apps that drive the digital workplace, stimulating increased data collection, analysis & exploitation activities[1]. AI is also being utilised by the financial industry, and financial institutions around the world are making large-scale investment in AI. AI has become a practical reality and is quickly becoming a competitive necessity in meeting the demands and expectations of consumers, who want more

[1] Sinta Dewi Rosadi, Andreas Noviandika, and Helitha Novianty, "Legal Protection of Privacy Rights of Personal Data Against Algorithmic Profiling, A Comparative Study of Privacy Protection in EU & Indonesia: Exploring Challenges and Opportunities," *International Journal of Innovation, Creativity and Change* 4, no. 5 (2020): 1-2.

convenient, cheaper, and smarter products and services. For businesses, AI is helping to streamline and optimise processes, ranging from credit decision to quantitative trading and financial risk management, which has provided a positive impact on businesses. AI is also used in fighting fraud and has provided an opportunity for businesses to deploy due diligence, prudence, and care[2]. According to a report released by World Economic Forum there are five sector-specific opportunities that could be enabled by the deployment of AI in financial institutions, the advanced of AI that enabled the deployment of AI in financial institutions, for example the utilising of AI will be able to provide faster operation, tailor product and advice, ubiquitous presence and could processes smarter decision making and able to provide new value of proposition [3]. The financial sector uses AI in at least six sub-sectors[4] such as deposit and lending, insurance payments, investment managements, capital market and market infrastructure.

As artificial intelligence evolves, it magnifies the potential to use personal information in methods which could intervene on privacy by elevating the evaluation of personal information to new levels of strength and speed[5]. There are different privacy issues in the society arising from the use of AI; one of them is user profiling. Profiling is defined as a form of automated processing of personal data that provides businesses with new possibilities of storing and processing data. In addition, user profiling is described as the recording and analysis of someone's emotional and behavioral characteristics, in an effort to determine or predict their abilities in a sure sphere or to assist in identifying categories of human beings.[6] User profiling has some advantages as it provides recommendation of needed products to users. Therefore, the user can easily search for the required information. However, user profiling raises security and privacy issues because it reflects the user's identity. Profiling or categorization of persons can be done through different parameters, such as gender, age, and location. Some of the privacy issues caused by the phenomenon of

---

[2] Alyssa Schroer, "AI and the Bottom Line: 20 Examples of Artificial Intelligence in Finance AI," builtin.com, 2021, accessed on 5 December 2021, https://builtin.com/artificial-intelligence/ai-finance-banking-applications-companies

[3] World Economic Forum Report, *The New Physics of Financial Services, Understanding How Artificial Intelligence is Transforming the Financial Sector*, 2018, 18.

[4] *Ibid.*

[5] National Institute of Standards and Technology, NIST Big Data Interoperability Framework: Volume 1, 2015, 5.

[6] Daniel Ruckers, Tobias Kugler (*ed*), *New European General Data Protection Regulation, A Practitioner's Guide, Ensuring Compliant Corporate Practice* (Germany: Nomos Publication, 2018), 264-265.

profiling during its application include de-individualisation and stereotyping, information asymmetry, discrimination, inaccuracy and abuse.[7]

Along with the development of technology and information in this modern era of globalisation and economic digitalisation, the digitalisation of financial transactions, especially in the banking sector, accelerated in response to the (Corona Viruse Disease 2019) COVID-19 pandemic. Effective consumer protection is now more important than ever. As (Organisation of Economic Cooperation and Development) OECD pointed oput that "the policies and approaches developed and adopted by financial consumer protection authorities evolve and adapt to the changing environment".[8] Digitalisation can bring many low-cost benefits to financial consumers, such as greater access to a variety of services, but it also comes with new online risks, such as personal data breach due to lack of privacy and digital security[9]. Further, it is noted that financial consumer protection means a regime that "generally designed to ensure fair and responsible treatment of financial consumers in their purchase and use of financial products and their dealings with financial services providers".[10]

This study uses the normative legal studies method to look at more closely the privacy protection mechanism associated with the use of AI in the financial sector. The look at additionally assesses the quantity of impact with the aid of the privacy protection mechanism at the privacy of the personal data of the consumer. Data evaluation turned into performed with the aid of qualitative approach, involving legal understanding and synchronisation of the related regulations. Data collection was done by library research, and essential parts of the law on enforcement of the right to privacy of personal data in the use of AI had been selected. Numerous legal materials, ranging from primary to secondary and tertiary legal materials, were used. Such legal materials include legal instruments as well as journal articles relevant to the subject.

II. PRIVACY CONCEPT

The concept of privacy is broad, and its implementation encompasses several disciplines, such as philosophy, computer science, political science, and legal science. The idea became first delivered by using American legal professionals, Warren and Brandeis, who wrote a piece of writing within the Harvard Law

---

[7] Rosadi, Noviandika and Novianty, "Legal Protection of Privacy Rights", 1.

[8] OECD, "Financial Consumer Protection Policy Approaches in the Digital Age: Protecting consumers' assets, data and privacy," OECD, 2018, accessed on 10 December 2021, https://www.oecd.org/daf/fin/financial-education/G20-OECD-report-on-financial-consumer-protection-and-financial-inclusion-in-the-context-of-covid-19.pdf

[9] *Ibid.*

[10] *Ibid.*

Review entitled "The Right to Privacy.[11] They stated that "privacy is the right to enjoy life and the right to be left alone, and this development of law was invaluable and demanded legal recognition". Claiming privacy is the right to enjoy life, which need to be included through the law, in keeping with Warren and Brandeis, because of technological, economic and political tendencies, emerging rights have not been protected through US regulation.

The right to privacy is related to the non-secular needs of people, that is, the need for humans' emotions and thoughts to be respected, and the right to enjoy one's life, additionally called the right to be let alone. On this regard, Warren later proposed that privacy must be recognised as a right that must be protected[12]. Modern communication modes, such as social media, e-mails, and running a blog, carry new perspectives to privacy, helping to outline a new realm of online privacy. One scholar defines privacy as "the control over or the autonomy of the intimacies of personal identity". The right to privacy is articulated in all the global and regional human rights instruments. The notion of privacy in online or internet communication includes the notion of intrusion or self-control over internet access to oneself to maintain solitude. Privacy is a qualified fundamental human right.[13]

Afterward, this concept was extended to data privacy law, which applies to a situation where personal data is subjected to certain forms of processing such as collection, recording, organization, storage, adaptation, alteration, transmission, erasure, and destruction[14]. All of us has the right to decide whether to change or share their personal data or not and to specify below that condition such data must be shared. Lloyd found that data privacy laws generally cover the use of personal data, the regulatory framework, and the right of an individual or data subject to claim that the processing of their personal data is against the basic principles of data privacy, which are common under global privacy standards. Alan Westin for the primary time defined privacy as the right of the individual to decide underneath what situations and to what extent their personal data can be exposed to others, and his concept is known as information privacy or data privacy[15]. After Westin, people divided privacy into several facets[16]:

---

[11] Samuel Warren and Louis Brandeis, "The Right to Privacy" *Harvard Law Review* 4 (1980): 10.

[12] Graham Greenleaf, *Asian Data Privacy Laws, Trade and Human Rights Perspectives*, (United Kingdom: Oxford University Press, 2014), 5.

[13] Rosadi, Noviandika and Novianty, "Legal Protection of Privacy Rights", 5.

[14] Ian Llyod, *Information Technology Law*, (United Kingdom: Oxford University Press, 2014), 52.

[15] Alan Westin, *Privacy and Freedom*, (New York: Antheneum Press, 1967), 21.

[16] David Banisar, "Privacy & Human Rights An International Survey of Privacy Laws and Developments," *The John Marshal Journal of Computer & Information Technology*, Vol. 18, (1999): 6.

1. Bodily privacy concerns the protection of human's physical conditions in opposition to invasive process
2. Territorial privacy
3. Communication privacy
4. Information privacy

Consistent with Greenleaf several international legal instruments in the shape of conventions and guidelines have established across the world recognised data privacy principles that have laid the foundation for maximum contemporary national data privacy laws. Some of the conventions and recommendations encompass OECD's 1980 Privacy Guidelines and the Convention for the Protection of Individuals in regard to Automatic Processing of Personal Data, 1981 (Council of Europe); they were used as a version to regulate data privacy in lots of jurisdictions[17]

The Guidelines have described personal data as "any information relating to an identified or identifiable individual"; an identifiable individual may be identified immediately or indirectly, especially with reference to identification numbers or other elements specific to their social, mental, physical, cultural, economic, or physiological identities.[18]

According to Graham Greenleaf, the Guidelines have been an early influence on the development of data privacy laws in Asia. Even though the Guidelines are voluntary and not legally binding, they are recognised by many countries as the premise of the norms governing data privacy; they are recognised by both the government and private corporation. There are many interpretations regarding what exactly constitutes personal data. However the essential factor is that data connected to individuals have to be protected either alone or while mixed with other information. Personal data includes a person's name, address, sex, age, education, and/or medical history. Those examples are not exhaustive, and many different sorts of information may additionally nevertheless as personal data.[19]

The guidelines establish that the following principles should be adopted as the main principles in the processing of personal data:

1. Personal data collection must be limited: One of the key factors of data privacy is that the gathering and processing of personal data have to be carried out in a lawful and fair manner. Consent is an important mechanism to limit the gathering of personal data.
2. Data quality: Institutions handling the personal data of individuals have an duty to ensure that the data are relevant and do not harm the data subject

[17] Greenleaf, *Asian Data Privacy Laws*, 10.
[18] Privacy International Report, 2013, 15.
[19] Greenleaf, *Asian Data Privacy Laws*.

due to lack of accuracy or completeness. Additionaly, the data must be updated with current information regularly.

3. Personal data collection must be in accordance with its original purpose. The processing of personal data must also be determined including restrictions on the use of such personal data.
4. Use limitation: Data should not be disclosed, become available or used for other purposes other than those specified except (a) with the consent of the subject data; (b) with the aid of the authority of law.
5. Security safeguards: It is obligatory for the data processor and controller to implement appropriate technical measures against accidental loss, modification, use, disclosure, and destruction.
6. Openness: Both the data controller and processor should provide a general policy that depicts how personal data are used and how privacy is protected. These principles will enable an organisation to build trust among the data subject.
7. Individual participation: In the big data era, this principle is very important, and it gives the data subject the right of access and rectification regarding their personal data.
8. Accountability: This requires that organisations show the steps that they have taken in implementing privacy protection, and they must be able to demonstrate compliance with these principles.

Many multinational corporations abide with the aid of those data protection principles as a way of ensuring minimum compliance in jurisdictions where data protection laws either do not provide stringent sufficient protection or do not exist.

III. PRIVACY AND ARTIFICIAL INTELLIGENCE

Issues regarding privacy and its philosophy have been widely discussed. Philosophically, according to Solove[20], there are six points of view on the concept of privacy: (1) the right to be let alone, which was proposed by Warrend and Brandeis; (2) limited access to someone (the ability to protect oneself from misuse of access to someone by others); (3) confidentially (hiding one's problems from others); (4) control of personal information (the ability to control information about oneself); (5) personality (protecting one's personallity, individuality, and dignity);and (6) intimacy (restricted control or access to one's privacy originated from the western society, privacy has been embraced in the Asian Region.

[20] Daniel Solove, *Understanding Privacy*, Cambridge, (Massachusetts USA: Harvard University Press, 2008), 51.

There are two major factors that influenced the privacy protection development in Asia, specifically in Indonesia[21]. First, privacy in Indonesia considered a part of fundamental rights. Indonesia has entered to human rights's international instruments, such as the Universal Declaration of Human Rights and International Covenant of Civil and Political Rights that in Second, due to the development of information technology, the privacy awareness in the Asian region increased. The information technology has capability to collect, analyse and disseminate information. This new development worldwide became an enabling factor to other sector industries, such as telecommunication, financial, media. It also has increased the level of information to generated to individual.

This development necessitated the need for regulation, mainly in Indonesia due to the fact of the emergence of numerous legal problems related to privacy, such as: (1) the emergence of the complaints from the public good delivered individually or in groups or organisations, because of disruption of individual privacy through both print and electronic media; (2) complaints from the public because the identity and personal data are not maintained by the party that provided the trust, such as in banking, health, education, administration, informatics and telecommunication; (3) several cases of wiretapping information that has not only reason of legal interests, yet been exploited by political interest group competition; (4) increasing percentage of cybercrime.

This new development also has increased the activities of law enforcement agencies in storing, collecting and analysing information about suspects resulting in increasing and systemic invasions of privacy in the name of law and order[22].

Societal concern in Indonesia arises when the law enforcement agencies do not obtain a warrant and gather information about innocent people or for other purposes than prosecuting the criminals. To acquire evidence, law enforcement officers often conduct wiretapping and recording conversation of the suspect from the government side. The recorded conversation can be the strongest evidence. However, this conduct should be done in accordance with the law because it is very important that the suspects understand their rights and the reason why their conversation is recorded in accordance with the

[21] Sinta Dewi Rosadi, "Balancing Privacy Rights and Legal Enforcement: Indonesia Practices," *International Journal of Liability and Scientific Enquiry* 5 no. 3-4 (2013): 233.

[22] Alan Davidson, *The Law of Electronic Commerce,* (Cambridge University Press, New York USA, 2009), 216.

prevailing laws[23]. In this case government plays an important role in ensuring the balance between the protection of privacy rights and security.[24]

The connectivity features of the Internet allow for an interactive two-way communication, whose impact on people's lives is more intimately than other media [25] The Internet connects people to places and people to people, giving rise to information privacy threats. This rapid progress in ICT means that information is obtained and processed more efficiently and cheaply. Such information can be collected, stored and exchanged, including data that may be considered sensitive by the individuals concerned. Thus, large databases and information such as internet records of financial and credit histories of individuals, medical records, purchases, and so on are very vulnerable to unauthorized access.

The spotlight has been shone on the relationship between privacy and AI. This is interesting because with respect to data protection, there are different opinions regarding the relationship between privacy and use of AI. On the one hand, experts argue that AI poses a threat to privacy over the internet and allows personal data to be misused with great effect. On the other hand, there are entities that develop technologies with the aim of improving privacy and protecting personal data over the internet through AI systems. Greenburg is of the opinion that attention should be paid to the achievements of AI; for example, AI applications are being developed to go through the privacy policies of organizations and produce a readable summary.

AI is divided into four main categories, namely, how a system can think like humans in general, understand a pattern of problems, provide solutions to problems, and how an existing system can think rationally based on computations - certain computations that provide valid and reliable results. An artificial intelligence system is required to act like humans and must have several capabilities that meet the required standards.

---

[23] Richard G. Schott, JD., "Warrantless Interception of Communications: When, Where, and Why It Can Be Done," *FBI Law Enforcement Bulletin* Vol 72 Issue 1, (2003): 25.

[24] World Economic Forum Report, *The New Physics of Financial Services, Understanding How Artificial Intelligence is Transforming the Financial Sector.*

[25] Karen Sparck Jones, *Privacy: What's different now?*, (University of Cambridge William Gates Building, JJ Thomson Avenue, Cambridge, Computer Laboratory, 2003), 10.

Figure 1. The Four Main Categories of AI

Thinking Humanly The exciting new effort to make computers **think**… machines **with minds**, in the fill and literal sense. (Haugeland, 1985). "[The automation of] activities that we associate with **human thinking**, activities such as **decision-making, problem solving, learning**..." (Bellman, 1978)	**Think Rationally** "The study of mental faculties through the use of **computational models**." (Charniak and McDermott, 1985) "The study of the computations that make it possible to **perceive, reason, and act**." (Winston, 1992)
Acting Humanly "The art of creating machines that perform functions that **require intelligence** when performed by people." (Kurzweil, 1990) "The study of how to make **computers do things** at which, at the moment, people are better." (Rich and Knight, 1991)	**Acting Rationally** "Computational Intelligence is the study of the design of intelligent agents." (Poole et al., 1998) "AI . . . is **concerned with intelligent behavior** in artifacts." (Nilsson, 1998)

Source: Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach Third Edition.* (New Jersey USA: Prentice Hall, Englewood Cliffs, 2016), 2.

The following are some examples of the mandatory capabilities that must be met by an artificial intelligence system[26]:

1. Natural Language Processing: the system is expected to be able to communicate in any language used by humans.
2. Knowledge representation: the system is expected to be able to store various information that will be used in a core process in artificial intelligence.
3. Automated Reasoning: the system can use the stored information to answer a given question or draw a new conclusion.
4. Machine Learning: a system that can adapt to a new situation and create new patterns that are used to solve a problem.

The discussion on privacy in the previous section suggests that the privacy framework must compromise between the following: (1) the desired level of privacy, (2) loss of information, as measured by data utility metrics, (3) the complexity and practical feasibility of the proposed system. The privacy framework shall also include two things that influence individual disclosure behavior: the benefits and risks of privacy from other mechanisms. The disclosure of a person's behavioral information is influenced by three factors as follows: the type of data collected, the purposes of data collection and usage, and the entity(s) that collects and uses the data and the autonomous determination that create number of privacy potential problems hence the

[26] Siddharth Gulati, Sonia Sousa, and David Lamas. "Modelling trust in human-like technologies." (Paper presented at Proceedings of the 9th Indian Conference on Human Computer Interaction, India, Association for Computing Machinery, New York, NY, USA, 16 December 2018), 1–10. https://doi.org/10.1145/3297121.3297124

organization will have to shaping privacy policies, governance and strategies, there are at least five determinant factor that have to be consider [27]:

1. Increased automation can't be rendered to less privacy protection.
2. Explainability needs more accountability.
3. Ethical data processing is built on privacy
4. Privacy is protecting who we are
5. Stronger encryption and de-identification help address privacy

Besides Regulation, ethical also having important factors and based on the Declaration on Ethics and Data Protection in Artificial Intelligence, there are six guiding principles of AI development. Following are the principles:

1. Fairness principle.
2. Continuous attention and vigilance.
3. System clarity and transparency.
4. Ethics by design.
5. Reducing bias and/or discrimination.

IV. EXISTING REGULATION

Indonesia does not have any specific regulation on privacy, and the Constitution of Indonesia has not explicitly mentioned the word privacy rights. However, Article 28 G (1) of the Constitution Amendment Four implicitly regulates privacy and states that '…each person is entitled to protection of self, his family, honor, dignity…"

This article was adopted from Article 12 of UDHRC and Article 17 of ICCPR. Furthermore, since Indonesia has ratified the International Covenant on Civil and Political Rights with Law No. 12, 2005, privacy rights enjoy legal protection, and the government of Indonesia has the responsibility to adopt legislative and other measures to safeguard privacy protection. At the same time, the government must make sure that they do not engage in interferences that are inconsistent with Article 17 of ICCPR. Based on those three regulations, there is no doubt that privacy rights in Indonesia are essentially has already protected and have protected the basic rights under human rights principles. Privacy rights should be used as guiding principles by the government in drafting relevant laws and regulations to ensure its congruity with privacy rights. However, as privacy is not absolute, when it is against other rights, the government must ensure a balance between privacy and other rights within the society. The government has a duty to ensure effective legal enforcement[28].

Due to the sectoral approach privacy regulation in Indonesia the Ministry

[27] David Hoffman and Riccardo Massuci, *Intel AI's Privacy Policy White Paper*, (Intel Corporation, 2018), 5.
[28] Fred H. Cate, *Privacy in the Information Age,* (Washington D.C: Brookings Institution Press,1997), 102.

of Infocom in the process of discussion of Personal Data Bill with the parliament and the model of regulation is comprehensive law with the possibility supplement with self-regulation.

V. ONLINE PRIVACY REGULATION

Globalisation of information has placed Indonesia as a part of the world information society: therefore, Indonesia has the obligation to harmonise the legislation with international regulation. The government of Indonesia through its Information and Electronic Transaction Act, 2008 has committed to support the development of information technology through laws and regulations so that the utilisation of information technology would be secured to ensure the safety of the society[29]. For the first time, the word "privacy" is introduced in the elucidation of the act in connection with the protection of personal data implicitly. Article 26 states that usage of individual's personal data is subject to the individual prior approval, unless otherwise stipulated by the laws. Individual may proceed to file a lawsuit for the incurred loss to any party who infringed such stipulation.

The term "privacy", which is implied within Article 26, is clearly divided as follows: (a) the right to enjoy individual life that is free from all kinds of disturbances; (b) the right to communicate freely with any other persons without being spied; (c) the right to control the access of one's personal data. Privacy rights are also regulated by the Freedom of Information Act, 2008. The exemption chapter states that information relating to a person is exempted from this act, such as non-public information relating to the history and conditions of their own family, health (physical and mental), monetary conditions (e.g., assets, income, and account), and evaluation result on education. Two years ago, the Indonesian government began drafting the Personal Data Bill. Unfortunately, the bill has not been passed yet up until this paper is written; therefore, Indonesia presently does not have a personal data act yet.

VI. CONCLUDING REMARKS

Privacy regulation in Indonesia should be more comprehensive, support the free flow of data, technologically neutral and implement the international principles of privacy rights as global standard. Also, privacy regulation should be supplemented with self-regulation that encompass both data uses and

[29] Law No. 11 of 2008 as amended by Law No. 19 of 2016 on Electronic Information and Transactions, Article 26.

technologies that fall outside current existing sectoral laws. Legal entities (person and/or organization) should embrace risk-based accountability approaches, putting in place technical or organizational measures to minimise privacy risks in the use of AI to minimise access to personal data and enhance protection of privacy.

REFERENCES

Banisar, David. "Privacy & Human Rights An International Survey of Privacy Laws and Developments," *The John Marshal Journal of Computer & Information Technology*, Vol. 18, (1999): 6.

Cate, Fred H. *Privacy in the Information Age*. Washington D.C: Brookings Institution Press, 1997.

Davidson, Alan, *The Law of Electronic Commerce,* New York USA: Cambridge University Press, 2009.

G. Schott, JD., Richard. "Warrantless Interception of Communications: When, Where, and Why It Can Be Done," *FBI Law Enforcement Bulletin* Vol 72 Issue 1, (2003): 25.

Greenleaf, Graham. *Asian Data Privacy Laws, Trade and Human Rights Perspectives*. United Kingdom: Oxford University Press, 2014.

Gulati, Siddharth, Sonia Sousa, and David Lamas. "Modelling trust in human-like technologies." Paper presented at Proceedings of the 9th Indian Conference on Human Computer Interaction, India, Association for Computing Machinery, New York, NY, USA, 16 December 2018. 1–10. https://doi.org/10.1145/3297121.3297124

Hoffman, David and Riccardo Massucci, *Intel AI's Privacy Policy White Paper*, Intel Corporation, 2018.

Llyod, Ian. *Information Technology Law*. United Kingdom: Oxford University Press, 2014.

National Institute of Standards and Technology, NIST Big Data Interoperability Framework: Volume 1, 2015.

OECD. "Financial Consumer Protection Policy Approaches in the Digital Age: Protecting consumers' assets, data and privacy." *OECD*, 2018. https://www.oecd.org/daf/fin/financial-education/G20-OECD-report-on-financial-consumer-protection-and-financial-inclusion-in-the-context-of-covid-19.pdf

Privacy International Report, 2013.

Rosadi, Sinta Dewi, Andreas Noviandika, Helitha Novianty. "Legal Protection of Privacy Rights of Personal Data Against Algorithmic Profiling, A Comparative Study of Privacy Protection in EU & Indonesia: Exploring

Challenges and Opportunities," *International Journal of Innovation, Creativity, and Change,* Vol 4, Issue 5, (2020): 1.

————. Balancing Privacy Rights and Legal Enforcement: Indonesia Practices, *International Journal of Liability and Scientific Enquiry*, Vol 5, Issues 3-4, (2013): 233.

Ruckers, Daniel, Kugler, Tobias (*ed*). *New European General Data Protection Regulation, A Practitioner's Guide, Ensuring Compliant Corporate Practice* (Germany: Nomos Publication, 2018), 264-265.

Russell, Stuart J., and Peter Norvig, *Artificial Intelligence: A Modern Approach Third Edition*. New Jersey USA: Prentice Hall, Englewood Cliffs, 2016.

Schroer, Alyssa. "AI and the Bottom Line: 20 Examples of Artificial Intelligence in Finance AI," *Builtin,* 2021. https://builtin.com/artificial-intelligence/ai-finance-banking-applications-companies

Solove, Daniel. *Understanding Privacy*, Cambridge. Massachusetts USA: Harvard University Press, 2008.

Sparck Jones, Karen. *Privacy: What's different now?*. University of Cambridge William Gates Building, JJ Thomson Avenue, Cambridge, Computer Laboratory, 2003.

Warren, Samuel, Brandeis, Louis. The Right to Privacy" *Harvard Law Review,* Vol 4, (1890): 10.

Westin, Alan. *Privacy and Freedom*. New York: Antheneum Press, 1967.

World Economic Forum Report, *The New Physics of Financial Services, Understanding How Artificial Intelligence is Transforming the Financial Sector*, 2018.

REGULATION

Indonesia, Law Number 11 Year 2008 and Law Number 19 Year 2016 on Electronic Information and Transactions.

This page is intentionally left blank