Jurnal Pembaharuan Hukum
Volume 11, Number 1, March 2024
E-ISSN : 2355 – 0481 (Print)
ISSN : 2580 – 3085 (Online)

THE SOCIAL MEDIA ALGORITHMS & PERSONAL DATA PROTECTION: THE COMPARATIVE STUDY OF EUROPEAN UNION, CHINA & INDONESIAN LAW

Reni Budi Setianingrum
Muhammadiyah Yogyakarta University, Indonesia
reni.setianingrum@law.umy.ac.id

Mukti Fajar ND.
Muhammadiyah Yogyakarta University, Indonesia
muktifajar_umy@yahoo.co.id

Anis Mashdurohatun
Universitas Islam Sultan Agung, Indonesia
anism@unissula.ac.id

ARTICLE INFO

Keywords:
Algorithms; Personal Data; Privacy; Protection; Social Media

ABSTRACT

The social media utilize algorithms to increase productive and targeted promotions which regulate the flow of information circulating in the system, and usually record user habits and monitor their personal activities for business profits. This phenomena raise issues amongst academia about the importance of user confidentiality governance in social media. This research is a normative research using conceptual approach and statutory approach, aims to examine whether an algorithms system breach of personal data protection law in European Union, China and Indonesia. The result of this research is the use of algorithm is not explicitly prohibited in European Union States, China and Indonesian Law. Normatively, algorithms utilization do not breach the data protection law in these three countries as long as it uses with user permission, uses for legal reason, provide explanation and protection to the user personal data.

A. INTRODUCTION

The development of information technology and the internet today has changed the way people communicate. One of them is through social media which has now become part of the activities in obtaining, sharing and disseminating information.[1] Social media is one of the most popular media because it provides convenience and speed that allows a person to create and distribute information. With the increasing use of social media, issues related to information security and privacy have also become important. The leaking of confidential information through social media has become a

1 Mesra Betty Yel and Mahyuddin K. M. Nasution, "Keamanan Informasi Data Pribadi Pada Media Sosial," *Jurnal Informatika Kaputama* 6, No. 1 (2022): 92–101.

common occurrence. The spread of privacy data can be caused by both user and service provider negligence.[2]

The conflict between the necessary or gathering and analysis of personal data and the privacy rights is at an historical peak. The most controversial example is the disclosure that US intelligence agencies frequently engage in "bulk collection" of civilian "metadata" detailing telephonic and other types of communication and activities, with the purpose of monitoring and thwarting terrorist activity.[3] These are followed by other compelling examples, including in medicine (patient privacy vs. preventing epidemics), marketing (consumer privacy vs. targeted advertising), and many other domains.[4]

Algorithms now play a significant role in our daily lives. They make it possible for us to conduct efficient searches on the internet and help the government identify social security fraud and make tax-related judgments.[5] Companies utilize algorithms to determine prices and hire new employees. In a nutshell, algorithms are excellent tools. Nonetheless, we have to realize that algorithms have a dark side from a perspective of fundamental rights since they are human inventions that are neither impartial or transparent.

Algorithms already an important marketing tool for digital marketers which utilize social media algorithms with the aim of producing effective and targeted promotions.[6] Algorithms regulate the flow of information circulating in the system, and the algorithms used by social media platforms usually record user habits, so that when a user searches with the keyword "buying and selling cars", the average content that appears on his social media will be related to buying and selling cars.[7] Algorithms select information that can be used as a tool to measure the level of engagement of followers with their influencers and are divided into three elements: interest, timeline and relationship.[8]

The use of e-commerce and social commerce platforms by Indonesians today is also inseparable from Algorithmic Decision Making (ADM) technology. ADM is a certain type of algorithm intended to support decision making. Faiz Rahman, stated that the use of ADM can help e-commerce or social media platforms to provide and maximize services to users, both sellers and buyers, based on the data entered by these users.

2 Hendro Gunawan, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Dalam Sosial Media," *Jurnal Muara Sains, Teknologi, Kedokteran Dan Ilmu Kesehatan* 5, No. 1 (May 2021): 1.

3 Michael Kearns et al., "Private Algorithms for the Protected in Social Network Search," *Proceedings of the National Academy of Sciences* 113, No. 4 (January 2016): 913–18

4 *Ibid*

5 Janneke Gerards, "The Fundamental Rights Challenges of Algorithms," *Netherlands Quarterly of Human Rights* 37, No. 3 (September 2019): 205–9

6 Itsrys, "Cara Manfaatkan Algoritma Media Sosial Bagi Pemasar Digital," ITS Online, 2020.

7 *Ibid*.

8 Hutchinson in Fanny Briliansa Setiyanto, "Pengaruh Algoritma Instagram Terhadap Keterikatan Yang Lebih Tinggi Dalam Penggunaan Instagram," in *Geliat Investasi Dalam Pusaran Pandemi: Membaca Celah Pemulihan Ekonomi Nasional Di Era New Normal* (Universitas Tidar, 2021): 250

However, there are also negative impacts of using ADM[9], if not used wisely, especially for consumers, such as bias and discrimination stemming from the data fed into algorithmic systems, lack of transparency in the system, and personal data breaches if the system is attacked by malicious software. There is also a need for comprehensive and rigorous regulation to guide their use, and the scope of consumer protection should therefore be adapted to these emerging services.[10]

The bargaining position of the user as a data subject tends to be more vulnerable than the platform provider, business actor or data controller in the digital industry. The legal framework on personal data protection is thus important to guarantee users' fundamental right to security when using social media and transacting without the need to be based on the presence or absence of material losses experienced. For the sake of the security and convenience of the community and the country, personal data taken from the process of using smart devices is considered personal data that must be protected by law.

B. RESEARCH METHODS

This research uses normative juridical method which focused on examining positive law[11] and it was using a conceptual approach, a statutory approach by examining all laws and regulations related to legal issues and a comparative approach by examining the European Union, China regulation on Data Protection and Artificial Intelligent and Indonesian Personal Data Protection Act. This normative research used secondary data, namely data obtained from the results of a literature review of various library materials related to research problems or materials, including scientific journals[12] and was described how law regulate about the using of social media algorithm and personal data protection and aims to investigate about algorithms from the perspective of European Union, China, and Indonesian Law.

C. RESULTS AND DISCUSSION

1. The Algorithm & Social Media

The 2000s was a boom period for technology companies. However, most of these businesses did not achieve real profitability to justify the high investment in this sector. Search and content sites on the Internet then developed subscription systems or adverts that appear on users' screens when entering certain websites to get profits.

9 "Digiring Oleh Algoritma: Pasrah Atau Balik Arah," Center for Digital Society, 2022.

10 Faiz Rahman et al., "Study on Risks for Consumers Due To Algorithmic Decision-Making and Profiling by e-Commerce and Social Media Platforms in Indonesia," *The Center for Digital Society*, (2022): 3

11 Johnny Ibrahim, *Teori & Metodologi Penelitian Hukum Normatif*, 3rd ed. (Malang: Bayumedia Publishing, 2007): 295

12 Mukti Fajar and Yulianto Achmad, *Dualisme Penelitian Hukum-Normatif Dan Empiris* (Yogyakarta: Pustaka Pelajar, 2015).

However, most Internet users are reluctant to pay for content and see pop up adverts as a nuisance.[13]

McChesney and Van Dijck state that the way out of the above impasse is to track Internet users through cookies, files that are downloaded when visit certain sites, and collect data about the user's path. From that data, it is possible to track user profiles and offer them personalised advertising.[14] By filtering the content that users see, social media platforms have the ability to influence users' perceptions and decisions, from their choice of where to eat to their voting preferences.[15] This mechanism is called algorithm.

More than ever, the operation of artificial intelligence processes can increase the invading parties' influence and privacy violations. An increasing number of online operations, ranging from straightforward picture and information searches on search engines to intricate algorithms sorting news feeds and other content on social media, incorporate big data and machine learning. [16]

The cores of underlying algorithms technology are Artificial Intelligence (AI), which is a machine learning systems that capable of performing tasks that normally require human intelligence, for example the using of virtual assistant such as Siri by Apple and Bixby by Samsung; Blockchain Technology, is a technology that supports digital currency and transactions, which secures, validates and processes transactional data; Internet of Things (IoT), is the inter-networking of 'smart' physical devices, vehicles, buildings, etc. that enable these objects to collect and exchange data; Behavioral and Predictive Analytics, are analysis of large and diverse data sets to uncover hidden patterns, unknown correlations, customer preferences, etc. to help make informed decisions. These four technologies are intimately linked AI provides the algorithms, blockchain the data storage and processing infrastructure, IoT the data devices, and behavioural/predictive analytics are important for (human) behaviour analysis.[17]

In this digital era, business actors have an interest in controlling consumer data, people's behavior patterns, and their communications in cyberspace for business benefits. In this case, business actors utilize algorithms on social media to examine consumer behavior and transaction patterns. The level of the algorithm is measured by analyzing the input and output of user audience social media content

13 Carlos Figueiredo and Cesar Bolano, "Social Media and Algorithms: Configurations of the Lifeworld Colonization by New Media," *International Review of Information Ethics* 26 (2017): 29

14 *Ibid*.

15 Sarah H Cen and Devavrat Shah, "Regulating Algorithmic Filtering on Social Media," Cornell University, (2020)

16 Jaroslav Denemark, "Strengthening the European Union By Regulating the Digital Single Market," *Acta Universitatis Carolinae Iuridica* 69, No. 2 (2023): 107–23,

17 Jeremy Barnett, Adriano Soares Koshiyama, and Philip Treleaven, "Algorithms and the Law," core.ac.uk, n.d.

and the suitability between things they often click/access/search for and things/content that often appear on their accounts.

Algorithm is a logical sequence of systematic problem solving steps, a mathematical tool for manipulating data or calculating problem solving.[18] Algorithm as the power of Artificial Intelligence, goes beyond the capacity of human intelligence to analyze data and make decisions. Algorithms are designed to replace humans in making decisions and are ubiquitous; they are used to guide commercial transactions, analyze credit applications, control autopilot cars and robot surgeons.[19] Gillespie defined algorithm as an encoded procedure that aims to change input data into the desired output, based on a specified calculation.[20]

The use of algorithms is increasing in decision making systems, where it would analyze large amounts of personal data sets. The purpose is to obtain the necessary information so that a decision can be made.[21] This can be used extensively, like the financial sector, business and health care which allow the creation of decisions by automated data systems.[22] Castelluccia and Le Métayer define social media algorithm as Algorithm Decision Making (ADM, some researcher mention it as ADS, Algorithm Decision System) as "a specific type of algorithm aimed at supporting decision-making".[23] Algorithms have become not only a method of filtering data, but also a way of obtaining external data regarding decision making from humans to software bots.[24] It has the power to affect consumer decision-making in the private sector.[25]

However, while the automation of decisions that humans normally make through algorithms has generated many benefits, their use also poses challenges to regulation.[26] In example, Zuboff accuses Google of being the pioneer of surveillance capitalism with search engine features to the Android system embedded in most smartphones in the world. A user's search history, voicemail, travel map route trace, or contacts in email are converted into data that then becomes a commodity for other digital companies. The case of Facebook, whose data was used by Cambridge Analytica, is evidence of the dark side of social media influencing the quality of the 2016 US Presidential Election. This was a clear evidence of how developed countries like the United

18 Ed Finn, *What Algorithms Want Imagination in the Age of Computing* (The MIT Press, 2018).
19 Woodrow Barfield, ed., *The Cambridge Handbook of the Law of Algorithms* (Cambridge University Press, 2020), https://doi.org/10.1017/9781108680844. p.3
20 Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot, eds., *Media Technologies* (The MIT Press, 2014).
21 Rahman et al., "Study on Risks for Consumers Due To Algorithmic Decision-Making and Profiling by e-Commerce and Social Media Platforms in Indonesia." : 7
22 *Ibid*.
23 Claude Castelluccia and Daniel Le Métayer, "Understanding Algorithmic Decision-Making: Opportunities and Challenges" (European Parliament, 2019).
24 *Ibid*.
25 Rahman et al., "Study on Risks for Consumers Due To Algorithmic Decision-Making and Profiling by e-Commerce and Social Media Platforms in Indonesia.": 11
26 Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot, eds., *Media Technologies* (The MIT Press, 2014).

States have succeeded in using millions of personal data of their citizens on Facebook to influence politics.[27]

In fact, consumers today deal with individualized digital services as algorithms identify which products or information they are most likely to click on, from search results to social media to content suggestions. The pervasiveness of customization raises concerns about freedom of choice. If everything we encounter online is personalized, including the options that are made available to us and the information that is given to us, does freedom of choice still exist? Therefore, it should be illegal to personalize prices based on an algorithmic evaluation of a person's lifestyle, attitudes, values, habits, beliefs, and interests, as this greatly increases the possibility of discrimination and exploitation.[28]

The facts above make us realize that by accessing the internet, all our activities and all the sites we have visited will be recorded, these information becomes a digital footprint. Since user preferences are heavily utilized to inform choices or to target them with material they are likely to be interested in, the capacity of these platforms to offer these services also raises the issue of consumer protection, data privacy and any potential of a threat to breach of personal data security. Public is also debating platforms that conduct internet monitoring, there is also an issue regarding the ethical risk of collecting personal data. Data protection against misuse by third parties is indeed a sensitive issue and is not easy to resolve. The easy and fast dissemination of information through technology creates threats to privacy by providing great opportunities for those who have access to such personal information.[29]

2. The Social Media Algorithm & Personal Data Protection

The phrase "data protection" was initially used to describe legal regulations governing the safeguarding of personal data in the 1970s by Germany and Sweden. Personal data protection was established at that time because computers were being utilized to store population data, particularly for population census activities. Nonetheless, there have been several infractions in its implementation by the public and private sectors. Therefore, in order to prevent misuse, personal data protection measures are crucial.[30]

The issue that arises is privacy protection. Is the personal data of internet users protected? In case there are parties who secretly use it in

27 Subiakto, Henri. "Perlindungan Data Pribadi Dan Tantangannya," n.d. https://bappeda.kaltimprov.go.id/.

28 Bureau Européen Des Unions De Consommateurs, "Towards European Digital Fairness Beuc Framing Response Paper For The Refit Consultation," *Bureau Européen Des Unions De Consommateurs*, (2023): 14

29 Sinta Dewi, "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia," *Yustisia Jurnal Hukum* 5, No. 1 (2016): 22–30.

30 Muhammad Na'im Al Jum'ah in Giosita Kumalaratri and Yunanto, "Urgency of the Personal Data Protection Bill on Privacy Rights in Indonesia," *Jurnal Hukum Unissula* 37, No. 1 (2021): 1–13

the context of mobilization, commodification, manipulation and even digital crime,[31] Philip N. Howard, reminded that IoT offers great potential for community empowerment, transparency and accountability in the exercise of power and political participation, but also brings serious problems of breaching privacy, social engineering and manipulation of people's behavior.[32]

Considering that algorithm has significant impact on society, it being the subject of public debate. The discussion about algorithm must be carried out meticulously and without obscuring any of the important problems, including the initial concern about the legality of using an algorithm on social media from personal data protection perspective.

The use of ADS might endanger data security and privacy in a variety of ways. The first has to do with the extensive accumulation of private information needed to equip algorithms. With varying effects on people (financial, psychological, physical, etc.), personal data can be the target of attacks launched by various parties (data controllers themselves, their employees, cybercriminals, states, etc.). Even in the absence of an actual attack, the suspicion that someone's personal information is being gathered might be harmful to them. Numerous studies have demonstrated the chilling impact brought on by worries about online surveillance.[33]

Countries and international organizations have developed legal frameworks for data processing in response to the challenges raised by the misuse of the algorithms. The widespread use of internet technology in the world is a substantial factor contributing to the increase in data processing because the internet makes the exchange of information between individuals easier and more massive. Various types of user data, including encoded user behaviors (likes, shared posts, written comments, search terms, connections and interactions with others, etc.), as well as other types of user information (like age and occupation), are used to create and constantly redefine the algorithms of social media platforms.[34] There is continuous circulation of individual information via internet resulting in unfair data processing activities between consumers who use the internet and companies that perform digital data processing.[35] Algorithms can be utilised to play essential role in the data mining endeavour, it can be used as the profiling engine to identify trends, relationships and hidden patterns in disparate groups of data.[36]

31 Agus Sudibyo, "Perlindungan Data Pengguna Internet: Menelaah Gdpr Uni Eropa," in *Jagat Digital, Pembebasan Dan Penguasaan* (Jakarta: Kepustakaan Populer Gramedia, 2019).

32 *Ibid*.

33 Castelluccia and Métayer, "Understanding Algorithmic Decision-Making: Opportunities and Challenges." : 12

34 Livia Norström, Anna Sigríður Islind, and Ulrika M. Lundh Snis, "Algorithmic Work: The Impact of Algorithms on Work with Social Media," *ECIS 2020 Research Paper*, (2020): 2

35 Jacqueline Klosek, *Data Privacy in the Information Age* (Praeger, 2000): 1

36 Bernhard Anrig, Will Browne, and Mark Gasson, "The Role of Algorithms in Profiling," in *Profiling the European Citizen: Cross-Disciplinary Perspectives*, (2008): 65

Digital data are translations of individuals, objects, behaviors, and relationships into information that computers can store, process, and visualize.[37] Any sort of data that has been digitized is technically referred to as digital data. Digital data, however, does not necessarily have to be large in quantity, moving quickly, or having a wide diversity. Entirety digital data is displaying great variety, such as numerical (such as records from sensors), textual (such as social media posts or digitized archive records), images (such as pictures uploaded by users on Instagram), videos (such as videos uploaded by users on YouTube), spatial (such as latitude and longitude records), temporal (such as time records attached to social media posts), relational data (such as retweets, mention or response tracks), experimental data from (large-scale) online experiments (such as recorded choices actions and interactions), emojis (used on social media to express emotions non-verbally), and program code (provided openly accessible through platforms such as GitHub).[38]

Data protection is considered as part of privacy protection and it is implemented in regulations on personal data protection. Discussing data protection as part of privacy is in line with the notion that privacy is a form of confidentiality, or the right to disclose or publish information, or the right to restrict access or control over personal information.[39]

Privacy right is one of the fundamental rights.[40] Protection of personal data is important because personal data can be misused and harm the rights of the owner of the personal data.[41] Privacy rights are also part of human rights, namely rights that belong to humans solely because they are human beings based on their human dignity.[42]

In general, personal data is data in the form of a person's identity, code, symbols, letters or numbers. Indonesian Law Number 27 of 2022 concerning Protection of Personal Data (PDP Act) Article 1 defines Personal Data as data about individuals who are identified or can be identified separately or combined with other information either directly or indirectly through electronic or non-electronic systems. The European Union in the General Data Protection Regulation (GDPR) Article 4 Paragraph (1) defines the term 'personal data' as any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to

37 Kitchin in Rocco Bellanova, "Digital, Politics, and Algorithms," *European Journal of Social Theory* 20, No. 3 (August 2017): 329–47

38 Viktoria Spaiser, "Digital Data and Methods," in *Research Handbook on Analytical Sociology*, ed. Gianluca Manzo (Elgar, 2021): 354

39 Dewi, "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia." *Yustisia Jurnal Hukum* 5, No. 1 (2016): 22–30

40 Charter of Fundamental Rights of The Eropean Union) (2012/C 326/02) Article 8

41 *Ibid*

42 Rhona K. M. Smith, *Hukum Hak Asasi Manusia*, ed. Knut D Asplund, Suparman Marzuki, and Eko Riyadi (Yogyakarta: PUSHAM UII, 2008): 11

one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[43] In fact, this refers to all information that is or can be shared to a person. Personal data includes things like a person's phone number, credit card number, personal identification number, account information, license plate number, phone number, and client addresses.[44] Since the definition refers to "any information," it means that the word "personal data" should be used as broadly as possible. This is also supported by case from the European Court of Justice, which has ruled that even less explicit information—such as work time logs that include details about an employee's activities at the workday is considered as personal data.[45]

Next big question is, does algorithm utilization breach the law? We will discuss from European Union, China and Indonesian regulation related to personal data perspective. Some expert said that the collection and distribution of personal data is a violation of privacy, because privacy rights include the right to determine whether or not to provide personal data.[46] But how about algorithm? For the first time in history, a judge has ruled that the use of an algorithm violates citizens' human rights. It happened in the Netherlands in February 2020 when a judge ordered the Dutch Government to stop using an Artificial Intelligence (AI) based system designed to predict the possibility of a citizen committing tax evasion.[47]

Algorithm is a profiling tool, profiling in GDPR is defined as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[48]

Article 5 GDPR regulate that Personal data shall be processed with lawfulness, fairness and transparency; collected for specified, explicit and legitimate purposes ('purpose limitation'); adequate, relevant and limited to what is necessary ('data minimisation'); accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data accurate ('accuracy'); kept in a form which permits identification of data subjects for no longer than is necessary for the purposes ('storage limitation'); and processed in a

43 The European Union in the General Data Protection Regulation (GDPR) Article 4 Paragraph (1)

44 "GDPR Personal Data," Intersoft Consulting, n.d.

45 *Ibid*

46 "CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation." UN Human Rights Committee, 1988. https://www.refworld.org/docid/453883f922.html.

47 Isabella Galeano, "This Algorithm Is a Breach of Human Rights," Do Better by esade, accessed 2020. See also Library of Congress. Netherlands: Court Prohibits Government's Use of AI Software to Detect Welfare Fraud, accessed 2020, https://www.loc.gov/

48 The European Union in the General Data Protection Regulation (GDPR) Article 4 Paragraph (4)

manner that ensures appropriate security of the personal data (‘integrity and confidentiality’).

Article 21 GDPR regulate that the data subject shall have the right to object, where personal data are processed for direct marketing purposes, in the context of the use of information society services, and for scientific or historical research. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims. Related to ADS, Article 22 DGPR regulate that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The EU published its draft proposals of the Artificial Intelligence (AI) Act (AIA) in April 2021, it reached on a Digital Services Package (DSP) in the spring of 2022, including restricted regulatory control over and access to platform algorithms.[49] The emphasis on maintaining core person rights including privacy, ethical decision-making, and data security is what sets European law for AI and algorithms different from China. For instance, the draft AIA includes clear prohibitions on decision-making algorithms in situations where they endanger "safety, livelihoods, and human rights." From a consumer's standpoint, Europe's regulatory approach is superior to China's since it prioritizes privacy and fundamental rights more strongly.[50]

In China, the Provisions on the Management of Algorithmic Recommendations in Internet Information Service[51] article 4 regulate that the provision of algorithmic recommendation services shall obey laws and regulations, respect social mores and ethics, obey commercial and professional ethics, follow the principles of equity and fairness, openness and transparency, being rational and reasonable, and good faith. Further, related to personal data protection, China’s government also oblige the providers of algorithmic recommendation services must not use algorithmic recommendation services to engage in activities that are prohibited by laws and administrative regulations, shall implement entity responsibility for algorithm security, establish and complete management systems and technical measures such as technology ethics reviews, data security and personal information protections, shall optimize the transparency and explainability of rules and shall not

49 “AI Act: A Step Closer to the First Rules on Artificial Intelligence,” European Parliament News, accessed 2023.

50 “China’s Regulations On Algorithms: Context, Impact, and Comparisons with the EU,” Friedrich Ebert Stiftung, accessed 2023.

51 “China Provisions on the Management of Algorithmic Recommendations in Internet Information Services,” accessed 2022.

restrict other internet information service providers, or implementing a monopoly or unfair competition.[52]

The providers shall inform users in a prominent style of the circumstances of the algorithmic recommendation services in an appropriate manner, shall protect the laborers' lawful rights. They also shall protect the consumers' rights to fair transactions, must not use algorithms to carry out unreasonable discrimination and set up convenient and effective portals for user appeals and public complaints or reports.[53] Furthermore, China's government also oblige the protection of the elderly from fraud and other harmful practices, and ban algorithm developers from creating addicting content for kids.[54]

China also regulates that algorithm service providers are under government supervision and if they use improper tactics such as providing false materials in filing, and refusing for correction, the government will order a suspension of information updates and give a concurrent fine of between 10,000 and 100,000 RMB.[55]

In general, regulations in Indonesia in the PDP Act are not much different from the provisions of the GDPR and China, where the Indonesian government allows providers to carry out data processing after obtaining written or recorded consent from users.[56] Data processing of minors must be authorized by a guardian and processing of disability data must specially done.[57] The government also requires that personal data controllers must protect users' personal data, both from unauthorized access and from unlawful use, must supervise each party involved and conduct an impact assessment of Personal Data Protection in the event that the processing of Personal Data has a high potential risk.[58]

The PDP Act also provides rights for users to obtain data usage information, improve data accuracy, obtain copies, end processing, delete and/or destroy Personal Data about themselves, withdraw processing consent, request delays and restrictions on processing of Personal Data. Further, users also have right to file objections of decision-making actions based solely on automated processing, including profiling, which result in legal consequences or have a significant impact.[59]

In another Indonesian regulation, namely Act Number 19 of 2016 regarding Electronic Information and Transactions, it is stated that

52 "China Provisions on the Management of Algorithmic Recommendations in Internet Information Services." Article 6-15
53 "China Provisions on the Management of Algorithmic Recommendations in Internet Information Services." Article 16-21
54 "China's Regulations On Algorithms: Context, Impact, and Comparisons with the EU."
55 "China Provisions on the Management of Algorithmic Recommendations in Internet Information Services." Article 33
56 Article 22 Act Number 7 of 2022 regarding Personal Data Protection Act (PDP Act)
57 Act Number 7 of 2022, Article 25 and 26
58 Act Number 7 of 2022, Article 34
59 Act Number 7 of 2022, Article 10

personal rights contain rights to enjoy private life and be free from all kinds of disturbances; rights are rights to be able to communicate with other people without spying; and rights to monitor access to information about a person's personal life and data.[60]

Furthermore, privacy rights in cyberspace cover 3 (three) aspects that need attention, namely acknowledgment of a person's right to enjoy his private life and be free from disturbances; the right to communicate with other people without supervision (spying on the part of other parties); and the right to be able to monitor and control personal information that can be accessed by others[61]

Based on the description and explanation above, there is no explicit prohibition for the use of algorithms in social media, both in the European Union, China and in Indonesia. Algorithms are prohibited when they access data without user permission, used for illegitimate reasons and carried out without fulfilling the principles of fairness, openness and transparency, being rational and reasonable, and good faith.

The Organisation for Economic Co-operation and Development (OECD) through Recommendation of the Council on Digital Security Risk Management regulate that concerning Human rights and fundamental values, every stakeholder should manage the risk associated with digital security in a transparent manner that complies with basic principles and human rights. Therefore, the parties involved should,[62] First, implement digital security in a manner that is consistent with and supports human rights obligations and fundamental values recognised by democratic societies, including the freedom of expression, the free flow of information, the confidentiality of information and communication, the protection of privacy and personal data, freedom of association, non-discrimination, openness and fair process, and second, base their digital security on ethical conduct which respects and recognises the legitimate interests of others and of the society as a whole.[63] In order to control the risk of digital security, both public and commercial organizations should have a general policy of transparency regarding their methods and processes.[64]

International human rights law recognizes the fundamental right to privacy. Article 12 of the Universal Declaration of Human Rights (UDHR), for instance, declares that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence …. Everyone has the right to the protection of the law against such interference or attacks." International human rights law requires that any interference with the right to privacy must be subject to legality,

60 Explanation of Act Number 19 of 2016 regarding Electronic Information and Transactions (ITE Act)

61 Mieke Komar Kantaatmadja, *Cyberlaw: Suatu Pengantar* (Bandung: ELIPS, 2002): 118

62 "OECD/LEGAL/0479: Recommendation of the Council on Digital Security Risk Management," OECD Legal Instruments, 2022.

63 "OECD/LEGAL/0479: Recommendation of the Council on Digital Security Risk Management."

64 "OECD/LEGAL/0479: Recommendation of the Council on Digital Security Risk Management."

necessity, and proportionality.[65] Governments, standards organizations, and industry efforts are currently creating ethical guidelines for AI. For instance, the IEEE's Global Initiative on Ethics of Autonomous and Intelligent Systems contains a section on privacy-related topics called "Personal Data and Individual Access Control in Ethically Aligned Design."[66]

Based on research results on social media activities which managed by Meta (Instagram, Facebook), on their privacy policy page, Meta has practices transparancy, legally and proportionality by clearly define the rights of users and the obligations of providers, including explaining what kind of data will be used by Meta, confidentiality guarantees and protection of user's personal data, as well as what steps can be taken by the user if the user wants to limit the data access by Meta. Users are deemed to have agreed to these rules and requirements by signing up and having a social media account on Meta. If the users object to the service, users can stop the service at any time by closing their social media accounts.[67] Thus, its found that ADS which use in social media managed by Meta is not breach the European Union, China and Indonesian law because it already met all requirements regulated by the governments related to fairness, openness and transparency, being rational and reasonable, and good faith, its also giving objection rights for user and guarantee the secrecy and protection of user personal data.

From regulation perspective, algorithms are not violate the law if they are fulfilled the data protection regulations, but the use of algorithms still leaving some ethics problems, The privacy problem is the primary one here. Users' personal statements are collected during a period when they are particularly exposed. They frequently provide private information on their location, well-being, and needs, whether those of others or oneself. According to Crawford and Finn,[68] consent cannot be compromised in the name of "the greater good." Alexander also mentioned the privacy concern as an ethical risk element.[69] The using of algorithms limited representativeness of data, it is problematic because algorithms capture and reproduce biases.[70]

65 "Privacy and Freedom of Expression In the Age of Artificial Intelligence," Privacy International, 2018.

66 "Privacy and Freedom of Expression In the Age of Artificial Intelligence."

67 "Privacy Policy What Is the Privacy Policy and What Does It Cover?," META, 2023.

68 Kate Crawford and Megan Finn, "The Limits of Crisis Data: Analytical and Ethical Challenges of Using Social and Mobile Data to Understand Disasters," *GeoJournal* 80, No. 4 (2015): 491–502

69 David E. Alexander, "Social Media in Disaster Risk Reduction and Crisis Management," *Science and Engineering Ethics* 20, no. 3 (2014): 717–33, https://doi.org/10.1007/s11948-013-9502-z.

70 Emily M. Bender et al., "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?," *FAccT 2021 - Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, (2021): 610–23

D. CONCLUSION

Information security and privacy concerns have become more crucial with the growth of social media use online. Through the usage of social media, a lot of information pertaining to a person's privacy has unintentionally been exposed online. Both service providers and social media users might be negligent, which can lead to the spread of personal data. The value of personal information must be preserved. The limits of data privacy are becoming increasingly hazy with the development and widespread usage of data access. Additionally, algorithms, a mathematical technique employed by corporations to analyze customer behavior and transaction patterns, are frequently used by social media platforms nowadays. This raises the question of whether service providers are legally permitted to access and observe the actions of their clients. According to the discussion above, using algorithms in social media is not explicitly forbidden in the European Union, China, or Indonesian Law as long as they adhere to the rules and requirements outlined in the legislation. Nomratively, algorithms used on social media platforms such as Instagram and Facebook are legal because they adhere to the principles of fairness, openness, transparency, reason, and good faith which regulated in European Union, China and Indonesian Law. This is reflected in the use of authorised access, which provides explanation and protection to users. These principles are also expressly stated in the social media terms and conditions that users agree to. But practically, there still some ethics problems left by the using of algorithms, so that the good faith of social media platforms in algorithms utilizations are extremely needed.

BIBLIOGRAPHY

Journals:

Alexander, David E. "Social Media in Disaster Risk Reduction and Crisis Management." *Science and Engineering Ethics* 20, No. 3 (2014): 717–33.

Anrig, Bernhard, Will Browne, and Mark Gasson. "The Role of Algorithms in Profiling." In *Profiling the European Citizen: Cross-Disciplinary Perspectives*, (2008).

Barnett, Jeremy, Adriano Soares Koshiyama, and Philip Treleaven. "Algorithms and the Law." core.ac.uk, n.d.

Bellanova, Rocco. "Digital, Politics, and Algorithms." *European Journal of Social Theory* 20, No. 3 (August 2017): 329–47.

Bender, Emily M., Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell. "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?" *FAccT 2021 - Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, (2021), 610–23.

Castelluccia, Claude, and Daniel Le Métayer. "Understanding Algorithmic

Decision-Making: Opportunities and Challenges." *European Parliament*, (2019).

Cen, Sarah H, and Devavrat Shah. "Regulating Algorithmic Filtering on Social Media." *Cornell University*, (2020).

Crawford, Kate, and Megan Finn. "The Limits of Crisis Data: Analytical and Ethical Challenges of Using Social and Mobile Data to Understand Disasters." *GeoJournal* 80, No. 4 (2015): 491–502.

Dewi, Sinta. "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia." *Yustisia Jurnal Hukum* 5, No. 1 (2016): 22–30.

Denemark, Jaroslav. "Strengthening the European Union By Regulating the Digital Single Market." *Acta Universitatis Carolinae Iuridica* 69, No. 2 (2023): 107–23.

Figueiredo, Carlos, and Cesar Bolano. "Social Media and Algorithms: Configurations of the Lifeworld Colonization by New Media." *International Review of Information Ethics* 26, (2017).

Gerards, Janneke. "The Fundamental Rights Challenges of Algorithms." *Netherlands Quarterly of Human Rights* 37, No. 3 (September 2019): 205–9.

Gillespie, Tarleton, Pablo J. Boczkowski, and Kirsten A. Foot, eds. *Media Technologies*. The MIT Press, 2014. https://doi.org/10.7551/mitpress/9780262525374.001.0001.

Gunawan, Hendro. "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Dalam Sosial Media." *Jurnal Muara Sains, Teknologi, Kedokteran Dan Ilmu Kesehatan* 5, no. 1 (May 2021): 1.

Kearns, Michael, Aaron Roth, Zhiwei Steven Wu, and Grigory Yaroslavtsev. "Private Algorithms for the Protected in Social Network Search." *Proceedings of the National Academy of Sciences* 113, No. 4 (January 2016): 913–18.

Kumalaratri, Giosita, and Yunanto. "Urgency of the Personal Data Protection Bill on Privacy Rights in Indonesia." *Jurnal Hukum Unissula* 37, No. 1 (2021): 1–13.

Norström, Livia, Anna Sigríður Islind, and Ulrika M. Lundh Snis. "Algorithmic Work: The Impact of Algorithms on Work with Social Media." *ECIS 2020 Research Paper*, (2020).

Setiyanto, Fanny Briliansa. "Pengaruh Algoritma Instagram Terhadap Keterikatan Yang Lebih Tinggi Dalam Penggunaan Instagram." In *Geliat Investasi Dalam Pusaran Pandemi: Membaca Celah Pemulihan Ekonomi Nasional Di Era New Normal*. Universitas Tidar, (2021).

Spaiser, Viktoria. "Digital Data and Methods." In *Research Handbook on Analytical Sociology*, edited by Gianluca Manzo. Elgar, (2021).

Yel, Mesra Betty, and Mahyuddin K. M. Nasution. "Keamanan Informasi Data Pribadi Pada Media Sosial." *Jurnal Informatika Kaputama* 6, No. 1 (2022): 92–101.

Books:

Barfield, Woodrow, ed. *The Cambridge Handbook of the Law of Algorithms*. Cambridge: Cambridge University Press, 2020.

Fajar, Mukti, and Yulianto Achmad. *Dualisme Penelitian Hukum-Normatif Dan Empiris*. Yogyakarta: Pustaka Pelajar, 2015.

Finn, Ed. *What Algorithms Want Imagination in the Age of Computing*. The MIT Press, 2018.

Ibrahim, Johnny. *Teori & Metodologi Penelitian Hukum Normatif*. 3rd ed. Malang: Bayumedia Publishing, 2007.

Kantaatmadja, Mieke Komar. *Cyberlaw: Suatu Pengantar*. Bandung: ELIPS, 2002.

Klosek, Jacqueline. *Data Privacy in the Information Age*. Praeger, 2000.

Smith, Rhona K. M. *Hukum Hak Asasi Manusia*. Edited by Knut D Asplund, Suparman Marzuki, and Eko Riyadi. Yogyakarta: Pusham UII, 2008.

Websites:

"AI Act: A Step Closer to the First Rules on Artificial Intelligence." European Parliament News, Acessed 2023. https://www.europarl.europa.eu/

Bureau Européen Des Unions De Consommateurs. "Towards European Digital Fairness Beuc Framing Response Paper For The Refit Consultation." Bureau Européen Des Unions De Consommateurs, Acessed 2023. https://www.beuc.eu/sites/default/files/publications/

"CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation." UN Human Rights Committee, 1988. https://www.refworld.org/docid/453883f922.html.

"CHINA'S REGULATIONS ON ALGORITHMS: Context, Impact, and Comparisons with the EU." Friedrich Ebert Stiftung, Acessed 2023. https://library.fes.de/pdf-files/bueros/bruessel/19904.pdf.

"China Provisions on the Management of Algorithmic Recommendations in Internet Information Services," Acessed 2022. http://www.cac.gov.cn/

"Digiring Oleh Algoritma: Pasrah Atau Balik Arah." Center for Digital Society, 2022. https://cfds.fisipol.ugm.ac.id/

Galeano, Isabella. "This Algorithm Is a Breach of Human Rights." Do Better by

esade, 2020. https://dobetter.esade.edu/

"GDPR Personal Data." Intersoft Consulting, n.d. https://gdpr-info.eu/issues/personal-data/.

Itsrys. "Cara Manfaatkan Algoritma Media Sosial Bagi Pemasar Digital." ITS Online, Acessed 2020. https://www.its.ac.id/

"OECD/LEGAL/0479: Recommendation of the Council on Digital Security Risk Management." OECD Legal Instruments, Acessed 2022. https://legalinstruments.oecd.org/

"Privacy and Freedom of Expression In the Age of Artificial Intelligence." Privacy International, Acessed 2018. https://www.article19.org/

"Privacy Policy What Is the Privacy Policy and What Does It Cover?" META, Acessed 2023. https://privacycenter.instagram.com/

Rahman, Faiz, Anisa Pratita Kirana Mantovani, Amelinda Pandu Kusumaningtyas, Nadya Olga Aletha, and Jasmine N.A Putri. "Study on Risks for Consumers Due To Algorithmic Decision-Making and Profiling by e-Commerce and Social Media Platforms in Indonesia." *The Center for Digital Society*, Acessed 2022. https://cfds.fisipol.ugm.ac.id/

Subiakto, Henri. "Perlindungan Data Pribadi Dan Tantangannya," n.d. https://bappeda.kaltimprov.go.id/

Sudibyo, Agus. "Perlindungan Data Pengguna Internet: Menelaah Gdpr Uni Eropa." In *Jagat Digital, Pembebasan Dan Penguasaan*. Jakarta: Kepustakaan Populer Gramedia, Acessed 2019. https://www.dpr.go.id/