

Study on Risks for Consumers Due To Algorithmic Decision- Making and Profiling by e-Commerce and Social Media Platforms in Indonesia





Author



Faiz Rahman

Anisa Pratita Kirana Mantovani

Amelinda Pandu Kusumaningtyas

Nadya Olga Aletha

Jasmine N. A. Putri

Reviewer



Mulya Amri, PhD.

Designer



M. Fattah Fachrial Al F.

Disclaimer



Implemented by



This publication was prepared with the support of the “Consumer Protection in ASEAN” (PROTECT) project, which is implemented by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH and funded by the Federal Ministry for Economic Cooperation and Development (BMZ) of Germany.

→ Contents

i	Contents
ii	List of Tables
iii	Executive Summary
1	Introduction
6	Practices of Algorithmic Decision-Making, Profiling, and Targeted Advertising in Indonesia
13	Initiatives to Ensure Data Protection in Social Commerce and E-Commerce
16	Challenges in The Practice of ADM, Profiling, and Targeted Advertising in e-Commerce and Social Commerce
17	● Potential Risks to Consumer Privacy and Data Protection
21	● The Risk of Algorithmic Bias and Dark Patterns
23	Analysis of Regulations related to Algorithmic Decision-Making, Profiling, and Targeted Advertising: State and Platforms Policies
24	● Mapping and Analysis of Indonesia's Laws and Regulations
24	● Legal Framework on Consumer Protection
28	● Legal Framework on Trade
31	● Legal Framework on Electronic Information and Transaction
34	● Personal Data Protection Bill
37	● Summary of the Laws and Regulations Analysis

40	● Mapping and Analysis: Algorithms for Advertising and Rules of the Game in Digital Platforms
41	● Instagram
42	● Facebook
44	● Bukalapak
45	● Shopee
48	● Summary of Digital Platforms' Community Guidelines, Terms and Conditions, and/or Policies related to User Data Utilization
50	Conclusions and Recommendations
51	● Conclusion
52	● Recommendations

→ List of Tables

37	Table 1.	Summary of Laws and Regulations Related to Algorithmic Decision-Making, Profiling, and Targeted Advertising in Indonesia
48	Table 2.	Summary of Selected Platforms' Community Guidelines, Terms and Conditions, and/or Policies related to User Data Utilization

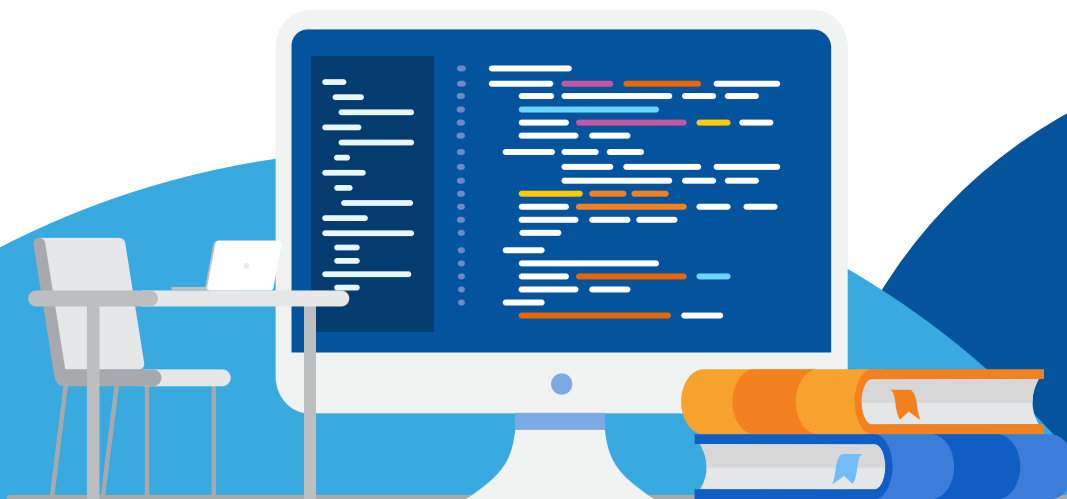
→ Executive Summary

This study examines the risks of Algorithmic Decision Making (ADM) on the e-commerce and social commerce for consumers in Indonesia. It studies thoroughly how the digital technology used by the business may harm consumers' rights in the decision making process on their purchasing behavior. The questions raised along this research were how businesses process consumers' behavior to generate personalized services, including giving the options for them. Indeed, this system provides easy solutions for consumers. However, it may also limit the alternatives. This study finds that such technology usage by the business may lead to the *dark pattern* phenomenon. Furthermore, the questions of how businesses collect, process, and store users' personal data are concerned. Although personal data are not the main variables on ADM, Indonesians reckon Personal Data Protection (PDP) regulation may, to some extent, safeguard consumers' rights. Therefore, the call for legalization of the PDP Bill in Indonesia is amplified.

In relation to regulatory review, it is worth mentioning that Indonesia has no specific laws and regulations governing the utilization of ADM, profiling, and targeted advertising and its potential risk of data breach and data abuse. However, there are many provisions scattered in various laws and regulations relevant to ADM, profiling, and targeted advertising, such as regulations on consumer protection, obligations of PSE, and personal data protection. Furthermore, the analysis of various legal frameworks shows that the only means to minimize the potential risks of ADM, profiling, and targeted advertising is through enforcement of personal data-related provisions, considering data is the 'fuel' of the machine that makes those technologies work. On the other hand, both social media and e-commerce platforms already have a variety of rules of the game related to data privacy and advertising.

Particular gaps and differences between how the state and platforms regulate and protect the consumer's rights to data protection regarding the advertising techniques should be acknowledged, especially by setting a clear legal basis on advertising techniques and their risks as a standard for social media and e-commerce platforms.

Conclusively, in order to minimize the potential risks of ADM on e-commerce and social commerce in Indonesia, a set of aforementioned recommendations that addressed the involvement of multi-stakeholders actors are proposed. In summary, the need to ensure data protection in transactions requires policymakers to provide a legal framework, notably through the enactment of the PDP Bill, and reformulate regulations on online advertising. Social media platforms, e-commerce platforms, and businesses shall also be transparent about the data they collect from their users and provide the option for them to make customized decisions when using their service. Innovative approaches to make privacy policies or community guidelines more concise and easily understandable can also be considered. Lastly, there need to be concerted efforts, together with consumer associations and other CSOs, to raise awareness of the potential risks of ADM and be mindful of the data they share when transacting online.







Introduction

In recent years, Indonesia has been experiencing a massive expansion in its e-commerce sector. This is possible due to the increase of internet usage in the country, which enables the high utilization of the internet in buying everyday goods and services. E-commerce allows its users to conduct transactions from the comfort of their own homes, with the process of buying and selling products online being as simple as it can be. Hence, it is not surprising that there has been a peaking number of e-commerce platforms and users in the country, as people rely more on online platforms to fulfill their daily needs due to the Covid-19 pandemic. Other than e-commerce, there is also an interest surrounding the usage of social media in selling and buying goods online – also known as social commerce. Social commerce is not necessarily a new phenomenon, as it is similar to previous practices of commercial transactions via online platforms (Primawan, 2022). However, the inclusion of social media such as instant messaging features, now adds to the attractiveness of social commerce as the preferred online platform to sell or buy products. Despite its numerous benefits, there are risks in e-commerce and social commerce. One of the main concerns has been the use of algorithms to assist online buying and selling of products, and its subsequent risks for consumers.

This paper studies algorithmic decision making (ADM) and profiling by e-commerce and social media platforms in Indonesia and its risks for the platforms' consumers. This will be done through the analysis of regulations related to the ADM systems, the explanation of the ADM systems' practices in Indonesia through multi-stakeholders perspectives, international experiences regarding ADM systems, and challenges that arise from the ADM systems on e-commerce and social media platforms. The explanation and definition regarding ADM, profiling and targeted advertising will be also provided in the upcoming chapters. The

study will be concluded by recommendations that will be addressed to relevant stakeholders regarding this matter.

In this study, we find that ADM can be beneficial and presents many opportunities for companies to improve both their user experience and expand the platforms' services. However, it also comprises threats and challenges if the technology is not used wisely especially for consumers, such as biases and discriminations stemming from the data inputted to the algorithmic system (Castelluccia and Le Métayer, 2019), lack of transparency in the systems, and personal data breach if the systems are attacked by malicious softwares. In addition to that, it requires a comprehensive and firm regulation to guide the utilization, and thus, the scope of consumer protection should accommodate these growing services in the platforms.

On the other hand, several studies and our interviews conceal that digital literacy is fundamental to equip society with the ability to protect themselves as consumers. A recent study shows that the combination of contextual and behavioral targeting increases purchase intent, brand favorability and awareness among consumers by up to 70% (Noh, 2017). Bureau Européen des Unions de Consommateurs (BEUC) also mentions that behavioral advertising may have the potential to increase information asymmetries between the consumer and the professional; the consumer is in a weak position as the business knows far more about him/her than he/she knows about the business.

The use of algorithms, profiling and targeted advertising also contributes to the phenomenon of *dark patterns* (Wahyuningtyas, 2021). As cited in the paper, dark pattern is defined as user interfaces used by some online businesses to lead consumers into making decisions that they would not have otherwise made if fully informed and capable of selective alternatives (Mathur, et al 2021). Mathur et al.

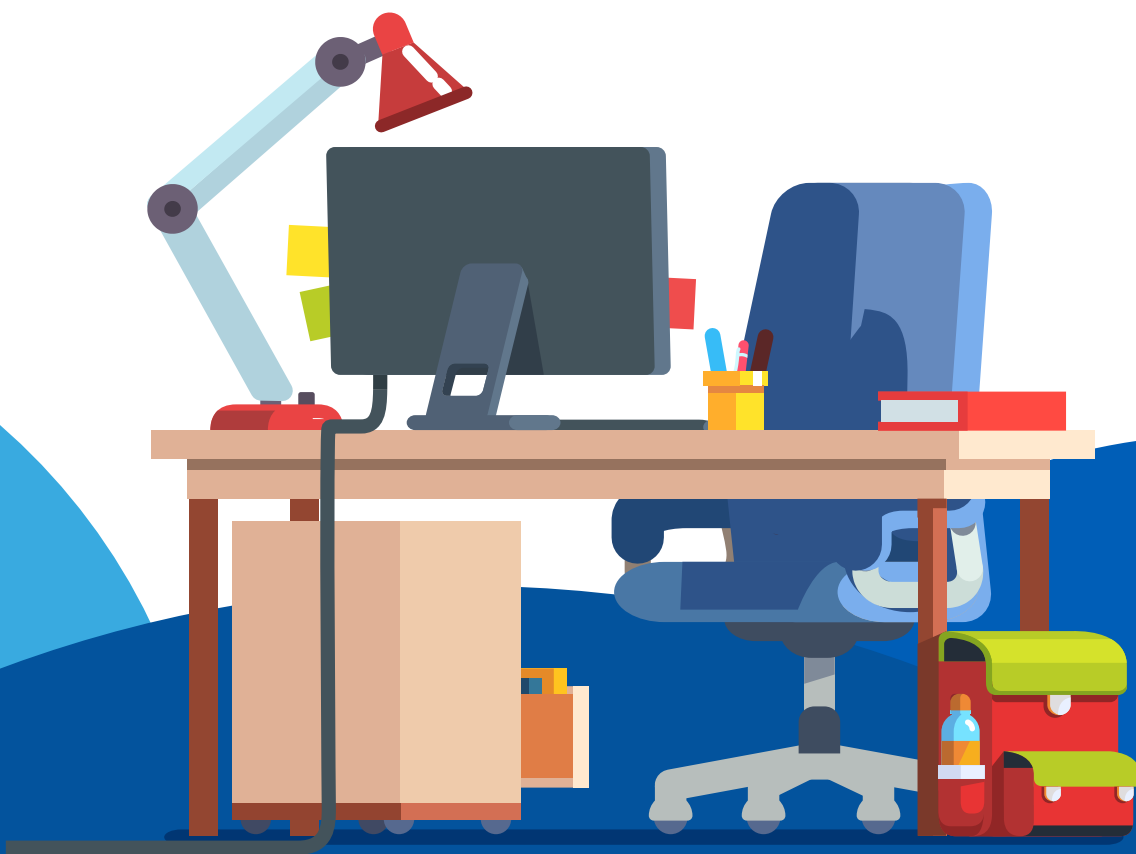
(2021) also explain that dark patterns are user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions.

Regarding the issues of ADM, ADS, and dark patterns in Indonesia, there is still limited academic literature which studies the matter. A recent study by GIZ shows how dark patterns are found in e-commerce platforms. Combining several dark patterns by Brignull (2000), Mathur (2021), Luguri & Strahilevitz (2019), the author did a survey for Indonesian consumers. The survey shows that: 1) Dark patterns practices are identified in Indonesian e-commerce platforms, even though not many of the respondents know the concept of dark pattern itself; (2) consumers are aware of the harmful effects of dark patterns; (3) consumers understand their rights to submit complaints. However, most of them submit their complaints to the e-commerce platform, and there are still blurry roles of consumer protection agencies.

Although there are several regulations that are related to the advisory of e-commerce practices in Indonesia, such as the Law No. 8 of 1999 on Consumer Protection and Law No. 11 of 2000 on Electronic Information and Transaction, there is no specific provisions explicitly regulating the use of ADM, profiling, and targeted advertising. Therefore, the existence of regulations governing the use of ADM, profiling, and targeted advertising is important to reduce potential risks that come with the innovation and ensure the safety of various parties involved in online commerce, especially consumers.

From the findings above, this study will focus on the mapping of risks for consumers caused by the use of the ADM system by e-commerce and social media platforms in Indonesia. Center for Digital Society (CfDS) through the support of Deutsche Gesellschaft

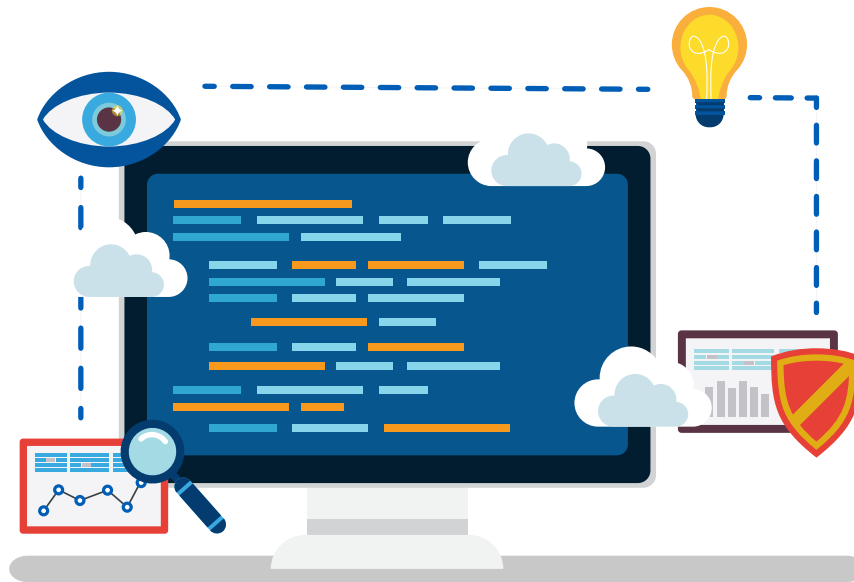
für Internationale Zusammenarbeit (GIZ) GmbH conducted this study through extensive desk research regarding the topic and also through in-depth interviews with relevant stakeholders. Interviews with relevant stakeholders are conducted to dig deeper into the perspective and experience of each stakeholder in regarding the usage of the ADM systems by e-commerce and social media platforms and its implications on consumers in Indonesia. The study aims to formulate an accommodative and holistic mechanism to approach this issue in Indonesia.





Chapter I

Practices of Algorithmic Decision-Making, Profiling, and Targeted Advertising in Indonesia



Algorithms have been utilized increasingly in decision-making systems, where it would analyze large amounts of personal data sets to derive useful information to make decisions. This can be used extensively, such as in the financial, business, health sector, and allow algorithmic data systems to make decisions. Castelluccia and Le Métayer (2019) consider ADM as algorithmic data systems (ADS), which is “a specific type of algorithm aimed at supporting decision-making”. This term is used to emphasize the need of algorithms to be studied in a general setting. Human involvement in ADS varies according to the needs of the system. EPRS explains that ADS could take the form of either semi-automatic or fully automated decision-making process. An example of semi-automatic ADS will be disease identification, where the ADS results should be coupled with medical doctors’ opinion. Fully-automated ADS can be seen in transportation systems such as metro train systems.

Castelluccia and Le Métayer (2019) categorized ADS into three classes:

- The first is ADS to improve general knowledge or technology, where algorithms are utilized to help analyze very large datasets to discover new knowledge. This class is usually implemented in science, such as to improve climate forecasts and detect diseases.

- The second ADS class is aimed to improve or develop new digital services. This class uses algorithms to make predictions, recommendations or decisions in many sectors such as information and finance. The usage of ADS is meant to optimize one of more criteria, such as time, energy, cost, etc. This ADS class can be used to address individuals in their decision-making process or private and public services. ADS in this category is usually linked to “optimization” of systems, where ADS can assist them in making their tasks easier or help expand the scope of their work.
- The last class is ADS which is integrated into cyber physical systems, whereby algorithms are utilized to reduce human supervision by applying them to physical objects. Physical objects with ADS, such as autonomous cars, robots and weapons, used algorithms to replace or assist human users in their operation and subsequently, decision-making process. A prime example will be robots that are made to help or replace humans in performing difficult tasks (e.g. robots in factory chains).

ADS in social commerce falls into the second class, where algorithms are used by e-commerce and social media platforms to determine the preferences of its users.

Article 4 of the General Data Protection Regulation (GDPR) elucidates ‘profiling’ as “any form of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.” Algorithmic profiling presents itself as a means to detect existing patterns, which then can be used to make predictions based on it. Mann and Matzner define algorithmic

profiling as “a method of inferential analysis that identifies correlations or patterns within datasets, that can be used as an indicator to classify a subject as a member of a group.” The scope of algorithmic profiling is broad as it can be applied in different sectors such as education, governance and security.

As for targeted advertising, Schlee (2013) defines it as “the compilation of detailed information about consumers and their preferences in using the Internet or consuming other media for the purpose of providing them with individualized advertisements.” Targeted advertising allows the data collection on a specific individual’s consumption behavior and pinpoints users’ consumption preferences as well. With the emergence of social commerce, targeted advertising can be seen as advertisements which are specifically targeted to a target audience based on their social and consumption behavior on the application. This is apparent in social commerce platforms such as Facebook, Instagram and Tiktok, which have been known to display contents (or in this case, advertisements) based on user preferences. These platforms analyze users’ behavior in the application in order to decide what advertisements are the most suitable to the users, ads that they are more likely to engage with.

There are many factors that influence consumer choices and behavior in social commerce platforms. Algorithmic systems, such as ADM, profiling and targeted advertising are some of the influencing factors on consumer choices in the platforms. Despite its goal of serving consumers better by providing specifically targeted contents, these systems have in some ways limited consumer choices on social media and e-commerce platforms. With a specific targeting on an individuals’ interest, this creates a narrow option for users in the contents displayed to them. ADM can limit the ability of users to decide on the platforms, as the algorithms are utilized to analyze a decision.

Profiling is used to detect patterns, which can be beneficial for consumers who purchase repeated or similar items. However, the biases that algorithmic profiling generates can also limit consumers, as it prioritizes patterns from prior purchases than other products in the market. Targeted advertisements restrict consumer choice as it only displays the individualized ads that the algorithms have provided, which limits the option of consumers in choosing the products they want to buy. The aforementioned systems can also increase the risk perception of consumers, which will dissuade them from purchasing and decrease consumers' purchase intention.

In the case of Indonesia, the use of ADM is known in the IT community as "recommender engine". It is created to help sort out data clustering and information overload (using AI/machine learning) in the current era, and has now become a necessity. While this should help people and the society to process the information they receive and decide what to do with it, unfortunately there are several excesses if not used carefully (Interview with Andry Alamsyah, 2022). Apart from that, the use of data in e-commerce and social-commerce platforms are gaining more attention from society. Adding to that idea, ADM is used by platforms to analyze the correlation or relationship of users behavior in the platform to produce information that can help users make decisions. Machine learning is used to understand consumers' behavior. ADM can be beneficial to present many opportunities for companies to improve both their user experience and expand the platforms' services (E-commerce platform, 2022).

ADM is also used for:

- To direct product search results to the sellers who are living in the nearby area as buyers.
- To provide Chatbots service.

- To determine competitive prices for goods.
- To promote the related goods and services that buyers search according to the geographical proximity.
- To detect any fraud or suspicious activity. Artificial Intelligence is used to check for transaction anomalies.
- To generate One Time Password (OTP).

In the private sector, ADM has the power to influence consumer decision-making processes. But it can reduce consumer trust on the platform on the perceived risk found in these ads. There are other concerns that entail these services. First, there may be biases and discriminations stemming from the data inputted to the algorithmic system (Interview with Alamsyah, 2022). This creates the potential to eliminate, introduce or increase discrimination, which depends of the software and data quality used in the algorithm. There is also the lack of transparency in these systems as it will be difficult to prove errors (i.e. biases and discriminations) in the systems.

Therefore, the ability of these platforms to provide these services also raised the question of data privacy, as users preferences are extensively used to make decisions or to be targeted to contents that the system thinks they will engage. There is also the looming problem of personal data breach if the systems are attacked by malicious softwares. In this sense, consumer protection should be strengthened as their data is being used for these services. And thus, the scope of consumer protection should accommodate these growing services in the platforms. Related to personal data collection, there is also a question on ethical risk since there is a debate of platforms doing online surveillance is also getting more attention from the public.

The issue of personal data breach, particularly, becomes more complicated in the e-commerce platforms, as the issue comes from both ways, sellers and buyers (Interview with e-commerce platforms, 2022).

"Some cases show that sellers may engage in behaviors that are detrimental to the efforts on protecting consumer's data. When they found consumers give them a low star rating, they will disclose the consumer's contact information"

● *Interview with e-commerce platforms, 2022*

By 2021, Badan Perlindungan Konsumen Nasional (BPKN) has received 3,256 consumer complaints; mostly coming from the housing, financial services and e-commerce sector. Despite the large number, none of the complaints are related to the misuse of personal data on e-commerce platforms (Interview with BPKN, 2022). While this might suggest that there are no active cases of data breaches in e-commerce transactions, it might also indicate under-reporting due to a lack of consumer awareness of the issue as a potential violation of consumer rights. On the other hand, BPKN also raised the concern that the use of ADM may increase consumptive behavior among online consumers. (Interview with BPKN, 2022).



Chapter II

Initiatives to Ensure Data Protection in Social Commerce and E-Commerce

Apart from laws issued by the government (which will be discussed in the next chapter), there have been several initiatives from platforms and the government to ensure protection of consumer data in e-commerce and social commerce. For example, one e-commerce platform we interviewed shared their effort in order to adapt with the Data Protection Bill. Even though the bill itself has not been legalized in Indonesia, the platform is now examining their internal organization readiness to fit in the umbrella. For example, the creation of the Data Protection and Privacy Office is spurred as one of fundamental divisions inside the organization (E-commerce platform, 2022). Furthermore, platforms are expected to do proactive monitoring, scanning, and data discovery. To fulfill the task, the platform has encrypted all data that includes *personal identifiable information* (PII).

Several industries have initiatives to secure the system. As the awareness of data protection has been increasing in the society, industries are searching for some common grounds to secure the system. They understand the role of, not only a secure infrastructure, but also digital literacy of consumers. Some of the initiatives executed by the business:

- Sharing only relevant information to third parties (logistics, payment and fintech partners) and only for specified purposes (minimization of data).
- Awareness-raising for third parties to share the same responsibility as the e-commerce platform to protect the user's data (a data protection agreement is annexed to their contracts).
- Awareness-raising within their staff, especially for operational units or those who may have access to data in their daily work with different risks and control levels. They provide newsletters and privacy-related educational

contents as training platforms, as well as fun events.

- Proactive monitoring by database screening of their internal systems and providing guidance on personally identifiable information (PII) which needs to be encrypted.
- Conducting a privacy impact assessment on product launches (checking for consent and whether it is enough, who can access the data and for what purpose, etc).
- Integrating alert mechanisms in their monitoring tools for ease of taking actions.

Furthermore, from the public sector, BPKN has handed out around 210 recommendations to other ministries for issues relevant to consumer protection, many of them aimed to increase digital literacy of consumers. Together with the Ministry of Trade (Kemendag), the Indonesian E-Commerce Association (idEA), and the Ministry of Communication and Information Technology (Kominfo), BPKN conducted a focus group discussion (FGD) to contemplate consumer protection policy in e-commerce, among others the need for data protection in platforms (despite the current regulatory gap) and improving digital literacy of consumers.





Chapter III



Challenges in The Practice of
ADM, Profiling, and Targeted
Advertising in e-Commerce and
Social Commerce

As it has been explained in the previous chapter, the practices of ADM, profiling, and targeted advertising in Indonesian E-commerce and social commerce are not uncommon. Therefore, it is necessary to map out challenges that may present in the practices of ADM, profiling, and targeted advertising in Indonesia. From the data gathered through intensive desk research and interviews with representatives of multi-sector actors, two challenges were identified. First, ADM, profiling, and targeted advertising may put consumer privacy at risk. Second, the practices could enable hostile business practices. Each of these challenges will be further elaborated in the following subsections.

A Potential Risks to Consumer Privacy and Data Protection

By design, ADM is a system that was developed to assist the decision-making process by analysing a large amount of data. The types of data used in ADM are varied from data directly obtained from users, data that are collected by observing users' patterns of behaviours on the platform, and deduced data from other data. After being collected, these large amounts of data will then be processed to make decisions that could range to various contexts. ADM is referred to as automated decision making because the process omits human involvement while solely relies on machines and algorithms. Meanwhile, profiling is an analysis process to identify and classify users into certain categories based on the patterns within collected datasets. ADM and profiling are not mutually exclusive; ADM could be done without conducting profiling and vice versa. However, both are necessary for targeted advertising, particularly in e-commerce and social commerce platforms.

Given the importance of users' data in the practices of ADM, profiling, and targeted advertising, one of the major concerns

regarding ADM is the possible risks to users' privacy and data protection violation. Various studies that have been published have addressed this particular concern. Research conducted by EPRS (2019), to name a few, concluded that the use of ADM may compromise users' privacy. Due to the ADM's mechanism, there is a chance that attackers could illegally retrieve and misuse users' data. Similar conclusions can also be drawn from research conducted by Newell and Marabelli (2015). However, Newell and Marabelli further elaborated that potential risks to users' privacy is the tradeoff between security and convenience that could not be avoided. In order to mitigate the risks, both studies call for the availability of strict regulations that put strong emphasis on protecting users' privacy.

Speaking of the Indonesian context, the concern on privacy and data protection violation has become more prevalent due to the frequent occurrence of data breaches. Throughout 2021 alone, MOCIs handled 43 data breach cases involving various public and private entities (Burhan, 2021). One of the most prolific cases was when Joko Widodo's social security number and Covid-19 vaccination certificate were leaked (Kompas.com, 2022), which shows that there are no data subjects in Indonesia who are invulnerable to data breaches. Several e-commerce platforms also received public backlash after failing to protect users' personal data from being illegally leaked and sold on the dark web.

Although the Indonesian government has appointed the Ministry of Communications and Informatics to conduct further investigations and prevention attempts, the absence of regulatory frameworks specifically tailored to ensure data protection makes the current efforts futile. As discussed in the second section of this report, Indonesia does not have any laws that comprehensively regulate personal data protection. There are several regulations that are often used as references for personal data protection in

Indonesia. However, they are inadequate to guarantee privacy and data protection for individuals who live in Indonesia. For example, under the current regulations, entities who could not comply with the responsibilities to ensure data privacy are not given strict consequences.

Over the past couple of years, Indonesia has made some efforts to improve the existing data protection mechanism. In January 2020, the president of Indonesia signed the Personal Data Protection (PDP) Bill, which has been drafted since 2016. Unfortunately, two years after the signing, the PDP Bill has not been passed yet and is still being finalised by the Indonesian House of Representatives (DPR). If the bill is finally passed, it will introduce some serious changes to Indonesian data protection mechanisms¹. The proposed bill will provide clear definitions of personal data and its types, identify key roles, introduce new data ownership rights, provide new cross-border data transfer regulations, detail data breach notification requirements, and designate data protection officers. More importantly, noncompliance with the new PDP Law will result in stricter sanctions.

Private entities, in this case e-commerce and social commerce platforms, that participated in interviews shared that they are fully supporting the PDP Bill and eager to comply when DPR finally passes the bill. However, some raised a concern that many drastic adjustments must be taken to comply with the new PDP Law. Although it remains unclear when the government will pass the PDP Bill, some platforms have taken some initiatives. For example, some platforms have established DPO or appointed some of their employees for similar roles. Even though there will be a two year transition period², some platforms are pessimistic that the adjusting process may take a much longer time.

¹ Personal Data Protection Bill

² *ibid*

Platforms are also unsure whether their users, especially sellers, will immediately comply with the new data protection mechanism. For instance, there have been doxxing incidents in cases where sellers receive unfavorable ratings or reviews. In this case, not only internal measures shall be taken, but there shall also be efforts to educate sellers on their responsibility to ensure consumer data privacy. Platforms are also unsure whether their users, especially sellers, will immediately comply with the new data protection mechanism. The representative of X E-commerce Platform shared that one of the biggest hurdles in ensuring consumers' data privacy is to make sure that sellers are aware of the concept of data protection. There have been numerous incidents of sellers doxxing consumers who gave them unfavourable ratings and reviews." In regard to that, platform X has changed their mechanism to prevent sellers from using consumers' personal information recklessly. Any publicly posted text contents containing consumers' personal information will be taken down by the system. However, there is a loophole which allows sellers to share consumers' personal information through images.

It has been suggested that the lack of awareness regarding privacy and data protection among platforms' users is because many Indonesians are not savvy in digital literacy. In 2021, Indonesia's digital literacy index was 3.49, which is among the lowest in South East Asia. MOCIs has also pointed out that there is still a lot of homework to do, especially in improving digital literacy on digital safety. Thus, taking a holistic approach is essential to mitigate any potential risks on consumers' privacy and data protection.

B The Risk of Algorithmic Bias and Dark Patterns

Aside from the concern regarding users' privacy and data protection, another concern arises: the practices of ADM, profiling and targeted advertising could enable unhealthy business practices. When it comes to automated systems such as ADM, most people are often thought that the technology is free from bias. In contrast to what many people assume, the use of ADM could cause bias that could manifest and affect users in various ways. As suggested in earlier studies, the bias is even more prevalent in targeted advertising (Lee *et al.*, 2019).

Targeted advertising requires data collection on a specific individual's consumption behaviour to pinpoint users' preferences. By doing so, targeted advertising could place advertisements that are specifically targeted to the target audiences based on their background and consumption behaviour on the application. Thus, algorithmic bias is a cautionary tale of such practices. Research conducted by Sweeney (2013) discovered that when compared to results for online search queries for white names, the ads that were shown for African American names were more likely from a service that renders arrest records. Another research conducted by Carnegie Mellon University (2020) has similar findings, which found evidence of biased ads distributions on Facebook. The bias was based on demographic characteristics, which may discriminate against certain socioeconomic groups. Hence, in the long run, biased ADM practices could worsen the current state of social inequalities.

There is also a concern that the use of algorithms, profiling, and targeted advertising also contributes to the phenomenon of *dark patterns* which has been briefly mentioned in the introduction. Dark patterns could be defined as user interfaces used by certain

platforms or online businesses to influence consumers to make decisions that they would not have otherwise made if fully informed and capable of selective alternatives (Mathur, et al 2021). Within Indonesia context, research conducted by research conducted by Wahyuningtyas (2021) has identified 12 forms of dark patterns used by e-commerce platforms, which includes: hidden cost, disguised ads, misdirection, privacy zukering, and so on. The research also found that most of the respondents were not aware of the use of dark patterns in e-commerce platforms as the majority of consumer complaints reported to the National Consumer Protection Agency (BPKN) related to e-commerce and social commerce were on issues regarding non-delivery, payment failure, or misleading advertisement.

The use of dark patterns in business could be considered a violation to fair business conduct because it is deliberately intended to mislead, deceive, and persuade consumers into making unintended and possibly harmful choices (Karagoel and Robert, 2021). Although some argue that the use of dark patterns could be helpful for consumers, it may benefit businesses more than it does the consumers and could perpetuate power imbalance between businesses and consumers. In the case of hidden cost for example, a pair of shoes were advertised as Rp 500.000/pair, but when a consumer purchased the product they had to pay an extra Rp 50.000 for 'administrative fee' and another Rp 1.000 for 'transaction fee'. These unforeseen surcharges added to the purchase are often mandatory and unavoidable, leaving consumers with no other choice.

Chapter IV

Analysis of Regulations related to Algorithmic Decision-Making, Profiling, and Targeted Advertising: State and Platforms Policies

➔ Mapping and Analysis of Indonesia's Laws and Regulations

The first section will map and assess three different legal frameworks related to Algorithmic Decision-Making (ADM), profiling, and targeted advertising: Consumer Protection, Trade, and Electronic Information and Transaction (EIT). In addition, the Personal Data Protection (PDP) Bill will also be analyzed to provide a better understanding of whether Indonesia's expected data protection legal framework is sufficient to protect the consumer's rights to data privacy that are prone to be violated through the advertising policies of digital platforms and online businesses. Each sub-section will cover the key terminologies and responsibilities of relevant actors and stakeholders. This sub-section will also provide an analysis of legal loopholes of the legal frameworks related to the discussed issue—to what extent the laws and regulations could protect consumers from potential risks of ADM, profiling, and targeted advertising.

➔ Legal Framework on Consumer Protection

Law No. 8 of 1999 on Consumer Protection (Consumer Protection Law) essentially regulates prevalent aspects of consumer protection. The main objective of this Law is to empower consumers, ensure high quality of goods and services in the market, and emphasize the businesses' responsibilities (See ASEAN Committee on Consumer Protection, 2022). To stimulate sales and/or simply introduce their products or services, advertisement certainly plays an important part, as technology evolves, social media platforms commonly use ADM, profiling, and targeted advertising techniques.

Essentially, Consumer Protection Law did not explicitly mention ADM, profiling, and targeted advertising—considering that this Law

only governs consumer protection in general. Pertained to the risks of online advertising practice, OECD identified numerous potential issues as follows: false and deceptive claims; deceptively formatted advertisements, which make it difficult for consumers to identify some advertisements as such threats from 'malvertising'; as well as data privacy and security issues related to increased data collection. (See OECD, 2019). Furthermore, it is also necessary to point out the relevant actors relevant to the implementation of ADM, profiling, and targeted advertising as governed in general under Consumer Protection Law.

First, consumers.³ Essentially, this Law did not explicitly mention the protection of consumers' rights from the risks of ADM, profiling, and targeted advertising in social commerce and e-commerce space—considering this Law only governs consumer protection in general. However, certain provisions implied consumer safeguards related to those issues. According to this Law, the rights of the consumers that are relevant to advertising techniques revolve around how the consumers should obtain accurate, clear, and honest information on the condition and warranty of the goods and/or services, as outlined in Article 4 of the Law, which falls on the business responsibility.

Most provisions revolving around consumer rights are still relevant in the e-commerce and social commerce context, as the wording is neutral and did not specifically mention the means of consumer activities—either through online or offline media. However, it is worth noting that this Law did not specifically mention the consumer's rights related to data collection through advertising techniques such as ADM, profiling, and targeted advertising. Therefore, the application of these provisions will highly depend on the implementers.

³ Consumer is defined as 'each individual user goods and/or services available in society, for the benefit of themselves, family members, other people, and other living creatures and which are not for trading' See Article 1 Number 2 of Law No. 8 of 1999 on Consumer Protection.

Second, business.⁴ According to Article 17(1), businesses in the advertising sector are prohibited from producing advertisements that: deceive the consumers on the quality, quantity, ingredients, use, and prices of the goods and/or services; deceive the guarantee on certain goods and/or services; provide incorrect, wrong or inaccurate information on the goods and/or services; do not provide information on the risks of using the goods and/or services; exploit the incident and/or someone without the permission from the authorized officials or the approval of the person concerned; violate the ethics and/or legal provisions on advertising.

Furthermore, Article 20 stipulated that businesses in the advertising sector are responsible for the advertisement they produce, and all of the consequences caused by the advertisement. The term 'businesses in the advertising sector' needs to be highlighted. This provision can only be applied to businesses that provide advertising services. Whilst, the provisions regarding businesses that practiced advertising has been addressed through Article 9, 10, 11, 12, 13, 14, 15, and 16 of this Law. Those provisions mainly imposed the businesses' prohibition on advertising or providing incorrect, deceiving, and misleading statements about their products and/or services.

Furthermore, Article 20 stipulated that businesses in the advertising sector are responsible for the advertisement they produce, and all of the consequences caused by the advertisement. The term 'businesses in the advertising sector' needs to be highlighted. This provision can only be applied to businesses that provide advertising services. Whilst, the provisions regarding businesses that practiced advertising has been addressed through Article 9, 10, 11, 12, 13, 14, 15, and 16 of this Law. Those provisions mainly

⁴Business is defined as 'an individual person or a company, in the form of a legal or non-legal entity established and domiciled or engaged in activities within the legal territory of the Republic of Indonesia, conducting various kinds of business activities in the economic sector through contracts, both individually and collectively' See Article 1 Number 3 of Law No. 8 of 1999 on Consumer Protection.

imposed the businesses' prohibition on advertising or providing incorrect, deceiving, and misleading statements about their products and/or services.

ADM, profiling, and targeted advertising have yet to be regulated under this Law. Relevant provision regarding the risks of ADM, profiling, and targeted advertising techniques can be found in Article 15, which stipulates that businesses are prohibited from offering goods and/or services by using force or any other methods that can cause either physical harm or psychological annoyance to the consumers. However, this Law did not specifically mention how to measure when the advertising is considered annoying for the consumers.

Furthermore, this Law also did not specifically mention the obligations of social media platforms as third parties and intermediaries. The absence of clear and comprehensive provisions that address social media platforms' obligation regarding advertisement practices depicts that there still exist loopholes in our consumer protection legal framework.

Third, government. According to Article 29(1) of this Law, the Government is responsible for developing the implementation of consumer protection which guarantees the rights of the consumers and businesses, and the implementation of the obligations of the consumers and businesses. The implementation shall be carried out by the Minister and/or the technically related ministers.⁵ Through this Law, the Government is also appointed as a rightful entity to supervise the implementation of consumer protection and application of the legal provisions.⁶

⁵ Article 29(2) of Law No. 8 of 1999 on Consumer Protection.

⁶ Article 30(1) of Law No. 8 of 1999 on Consumer Protection.

Fourth, Registered Consumer Associations.⁷ As mentioned in Article 30(1), besides the Government, the Registered Consumer Associations could carry out the supervision to implement the consumer protection and application of the legal provisions. **Fifth,** the National Consumer Protection Agency.⁸ Article 33 stipulates that the National Consumer Protection Agency's role is to provide suggestions and considerations to the Government to develop consumer protection in Indonesia. **Sixth,** the Consumer Dispute Settlement Agency.⁹ The duties and authorities of the consumer dispute settlement agency can be found in Article 52. To outline, the consumer dispute settlement agency is assigned mainly to handle and settle consumer disputes through mediation, arbitration, or conciliation.

Nevertheless, online businesses and electronic services providers have yet to be regulated explicitly under this Law. This Law has also yet clearly regulated the obligation of the electronic system of social media as a third party in social commerce transactions—to protect consumers from data privacy breaches and/or false, misleading, deceptive, and inappropriate advertisements. Conclusively, this Law did not explicitly mention the protection of consumers' rights from the risks of ADM, profiling, and targeted advertising in the social and electronic commerce space—considering this Law only governs consumer protection in general.

➔ Legal Framework on Trade

In 2014, the Government of the Republic of Indonesia promulgated Law No. 7 of 2014 on Trade (Trade Law) as the baseline legal policy concerning trade-related issues, including those

⁷ Refers to Lembaga Perlindungan Konsumen Swadaya Masyarakat (LPKSM), which is defined as 'a non-government foundation registered and recognized by the Government engaging in consumer protection activities' See Article 1 Number 9 of Law No. 8 of 1999 on Consumer Protection.

⁸ The National Consumer Protection Agency is defined as 'an agency established to help develop consumers' protection' See Article 1 Number 12 of Law No. 8 of 1999 on Consumer Protection.

⁹ The Consumer Dispute Settlement Agency is defined as 'an agency responsible for handling and settling the disputes between entrepreneurs and consumers'. See Article 1 Number 11 of Law No. 8 of 1999 on Consumer Protection.

conducted through electronic systems. Despite having regulated concerns regarding data breaches issues that potentially happen within trade activity, especially through electronic systems, Trade Law is yet to address the use of ADM, profiling or targeted advertising.

On electronic system transactions, the Government has enacted Government Regulation No. 80 of 2019 on E-Commerce (GR 80/2019). However, the term 'social commerce' and 'ADM, profiling, and targeted advertising' cannot be found under this Regulation. Concerning advertising, GR 80/2019 has defined online advertising as the information for the commercial need of products and/or services through electronic communications that are displayed and disseminated to certain parties, either paid or unpaid.

The specific provisions regarding electronic advertisement have also been covered in certain articles. **First**, Article 32 emphasizes the businesses' rights to promote their products and/or services through electronic advertisements. **Second**, Article 33 points out that the advertising can be done through an electronic system provider as a third party; Article 34 highlights the substance or materials of the electronic advertisement shall not violate the consumers' rights and/or fair business practices. **Third**, Article 35 stipulates every party involved in producing, facilitating, and/or disseminating the electronic advertisement shall ensure the substance and materials of the electronic advertisement are not violating the existing laws and shall be responsible for each substance or materials contained in the electronic advertisements.

Provisions contained in the Trade Law may, to some extent, fulfill the legal certainty of consumers' rights while encountering unfair advertising practices. However, it is worth noting that there still exists a loophole under GR 80/2019. As mentioned before, this regulation has not explicitly mentioned the term 'ADM, profiling, and

targeted advertising’ and its substantial implications. Hence, there is still room for improvement to maximize consumers’ data protection against data misuse and exploitation by the businesses, platforms, and/or advertisers.

Other than GR 80/2019, the new implementing regulation under this GR has been issued, namely, Minister of Trade Regulation No. 50 of 2020 on Provisions of Business Licensing, Advertising, Guidance, and Supervision of Businesses Trading Trade through Electronic Systems (MoT Regulation 50/2020). This regulation emphasizes that electronic advertisement must comply with the Indonesian advertising code of ethics and the relevant laws and regulations. The electronic advertisement is also obliged to comply as follows: it does not deceive, include false claims; false, incorrect, or inaccurate information; should be contained with risks associated with the use of advertised goods and/or services; it does not exploit any incident and/or person without authorization; it should provide with an exit function to close and skip the advertisement.

Conclusively, the existing laws and regulations are still not explicitly mentioned regarding the utilization of consumers’ data in forming advertising strategies (ADM, profiling, and targeted advertising). The existing laws and regulations are still focusing on how the displayed advertisement should conform with the actual conditions of goods and/or services—it should not contain false, misleading, deceptive information, etc. Considering the potential negative implications of the utilization of ADM, profiling, and targeted advertising, the existing legal framework on trade can also be improved to cover the mitigation of such consequences.

➔ Legal Framework on Electronic Information and Transaction

Unlike previously discussed legal frameworks, Law No. 11 of 2008 jo. Law No. 19 of 2016 on Electronic Information and Transaction (EIT Law) is not specifically intended to regulate commercial activities. However, electronic commerce is one of the main concerns of the EIT Law, which can be seen in the General Elucidation of the EIT Law.¹⁰ Conversely, this Law is regarded as the main Law for regulating activities on social media platforms. Furthermore, from EIT Law's perspective, e-commerce and social media are Electronic System (ES).¹¹ Consequently, Electronic System Operators (PSE) must comply with the EIT Law and its implementing regulations in implementing their ES.

The EIT Law identifies various actors that constitute PSE, including the State Institutions, Business Entities, and society in general.¹² In this regard, marketplace and social media platforms are part of the "Business Entity" category and specifically categorized as Private Sector PSE in the Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transaction (GR 71/2019) and Minister of Communication and Informatics Regulation No. 5 of 2020 on Electronic System Provider in Private Sector (MCI Regulation 5/2020).¹³

From the legal framework of EIT, concern regarding the risks for consumers from the utilization of ADM, profiling, and targeted

¹⁰ It is stated that broader issues on the impact of technological development that emerge in the private sphere, as electronic transactions for trade activities in ES (electronic systems) have become a part of national and international trade. See Paragraph 6 of General Elucidation of Law No. 11 of 2008 on Electronic Information and Transaction.

¹¹ The Electronic System is defined as 'a set of electronic devices and procedures that serve to prepare, collect, process, analyse, store, display, announce, send, and/or disseminate Electronic Information. See Article 1 Number 5 of Law No. 11 of 2008 on Electronic Information and Transactions. The MCI Regulation 5/2020 also defines specific Private Sector PSE, which is User Generated Content (UGC) Private Sector PSE. See Article 1 Number 7 of Minister of Communication and Informatics Regulation No. 5 of 2020 on Electronic System Provider in Private Sector.

¹² See Article 1 Number 6 of Law No. 11 of 2008 on Electronic Information and Transactions. State Institutions in Government Regulation No. 71 of 2019 on Implementation of Electronic System and Transactions (GR 71/2019) covers legislative, executive, judiciary, regional-level institutions, and other institutions established based on laws and regulations (See Article 1 Number 35 of Government Regulation No. 71 of 2019 on Implementation of Electronic System and Transactions). In the society category, it also covers institutions formed by society (e.g., civil society organizations, consumer associations) (See e.g., Article 41 of Law No. 11 of 2008 on Electronic Information and Transactions).

¹³ Business Entity is defined as a sole proprietorship or partnership of both legal entity and non-legal entity. See Article 1 Number 22 Law No. 11 of 2008 on Electronic Information and Transactions.

advertising from EIT Law and its implementing regulations are substantially similar to other legal frameworks discussed above, which is raised from the use of consumers' data. Essentially, the operation of ADM, profiling, and targeted advertising highly depend on how platforms utilize their users' data. In ADM, the use of personal data will influence users' decision-making ability. It goes the same with profiling and targeted advertising, as the users' (personal) data will be used to define who the user is and what they want (See, e.g., Schlee, 2013; Matzer & Mann, 2019).

In this regard, the central (and the only one) point of personal data-related regulation in the EIT Law is related to the data subject's consent in personal data processing by PSE. The EIT Law states that the use of any personal data of an individual must be made with the consent of the individual concerned.¹⁴ In general, consent has a central role in data protection. Apart from the interest in informational privacy, consent is also related to the interest in fair processing and fair use of personal data, and confidentiality of information (Brownsword, 2009). Therefore, under the EIT Law, unless otherwise provided by laws and regulations, the use of personal data without consent will be regarded as unlawful.

However, EIT Law did not further specify what constitutes 'valid legal consent.' It is further explained in the Elucidation of Article 14(3) of GR 71/2019 as explicit consent and not conveyed in secret or based on errancy, negligence, or coercion. Moreover, if the data subject withdraws the consent, the personal data should be erased.¹⁵ It is essential to guarantee that in the future, users will not be provided with any information based on their previous activities in e-commerce and social media platforms, which was provided based on the utilization of ADM, profiling, and targeted advertising technologies.¹⁶

¹⁴ See Article 26 of Law No. 19 of 2016 on the Amendment of Law No. 11 of 2008 on Electronic Information and Transactions.

¹⁵ See Article 16(1) letter b Government Regulation No. 71 of 2019 on Implementation of Electronic System and Transactions.

¹⁶ For instance, e-commerce or social media users want to delete their accounts and thus delete their personal data stored on

Furthermore, other legal grounds for personal data processing can be found in GR 71/2019,¹⁷ such as based on contract, legal obligations, vital interests of the data subject, public interests, and legitimate interests.¹⁸ This is similar to the legal grounds stipulated in the EU General Data Protection Regulation (EU GDPR).¹⁹ Another similar take of personal data regulations in GR 71/2019 to EU GDPR is regarding data processing principles. Based on GR 71/2019, PSE has an obligation to implement personal data protection principles, including data minimization, purpose limitation, protection of data subject's rights, accuracy, etc.²⁰ Furthermore, GR 71/2019 also obliges the PSE to provide information regarding the guarantee of privacy and/or personal data protection, which is generally informed in the privacy policy. A reasonable privacy policy/notice can further enhance platforms' transparency (See, e.g., Kerry and Chin, 2020), as it essentially provides how they process users' data.

According to legal framework of EIT, all personal data-related provisions above can be used both by the Government (as the regulator) or society in general (as the users) to hold the platforms accountable. Based on these grounds, the Government, through the Ministry of Communications and Informatics, can impose administrative sanctions on PSE in the form of a written warning, administrative fines, temporary suspension, access blocking, and/or removal from PSE registration.²¹ As for users, they can file a civil lawsuit against PSE on the basis of a violation of the consent for the

the platforms. In the future, if they access e-commerce and social media (without login to the platforms or by using a new account), they will have more general information provided rather than specific information targeted to them based on their behaviour in the platforms.

¹⁷ Indonesia also has Ministry of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection on Electronic System (MCI Regulation 20/2016). However, considering 'updated' provisions fundamental personal data protection, such as definition and principles of data processing, it is preferable to refer to GR 71/2019.

¹⁸ See Article 14(4) Government Regulation No. 71 of 2019 on Implementation of Electronic System and Transactions.

¹⁹ See Article 6(1) EU General Data Protection Regulation.

²⁰ Data processing principles in EU GDPR are lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability (See Article 5 EU General Data Protection Regulation).

²¹ Article 100 of Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions. Specific for private sector PSE, it further specifies in MCI Regulation 5/2020, based on the violations (See e.g., Article 7 (2) and (3), Article 8(2), Article 15(10), Article 16(11), and Article 45(4) Minister of Communication and Informatics Regulation No. 5 of 2020 on Electronic System Provider in Private Sector).

consent for the damages incurred as stipulated in the ITE Law.²² However, there are no further regulations regarding the procedural Law on civil lawsuits based on the infringement of consent.

Nevertheless, no regulations in the EIT legal framework explicitly govern the utilization of ADM, profiling, and targeted advertising and its potential risks. The only means to mitigate the potential risks of ADM, profiling, and targeted advertising in the legal framework of EIT is through the enforcement of personal data-related provisions, considering users' data is 'fuel' to make ADM, profiling, and targeted advertising work. Without personal data, these technologies will never be capable of producing the intended outputs, such as personalized information or goods.

Specific regulations addressing the utilization of ADM, profiling, and targeted advertising are also necessary, considering the potential risks such as producing misleading information, discriminatory and biased information, and decisions for their users (MacCarthy, 2019).²³ However, there is also a challenge in formulating and enforcing the regulations, as most of the risks from using ADM, profiling, and targeted advertising are primarily indirect risks. It means that the damages that occur will not instantly happen when the machine works but gradually through many information collected and processed by the machine.

➔ **Personal Data Protection Bill**

To date, there is yet to be a standalone Data Protection Law in Indonesia. The personal data protection regulation is currently scattered in more than 32 different laws and regulations (See Aprilianti, 2020; Riyadi, G., A., 2021), which results in legal loopholes for consumer protection violations (Soemarwi, V. W. & Susanto, W., 2021). As mentioned by OECD in the report mentioned above, one of

²² See Article 26(2) of Law No. 19 of 2016 on Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.

²³ In this context, discriminatory and biased decisions refer to what the platform shows (either product or information) to the users in their social media or e-commerce platform.

the most significant issues in the e-commerce and social commerce practices, is regarding privacy and data protection, considering the rapid increase of data collection. Therefore, a legal basis for data protection is essential to provide legal guarantee for consumers' data protection in the e-commerce and social commerce practices.

The center of attention of this PDP Bill is electronic information (Data Guidance, 2021). There are relevant actors regulated that are relevant to the discussion on ADM, profiling, and targeted advertising. **First**, the personal data controller.²⁴ The PDP Bill stated that personal data controllers are obliged to ensure the accuracy, completeness, consistency, and security of personal data being processed.²⁵ **Second**, the personal data processor.²⁶ The Personal Data Processor is responsible for any data processing activities appointed by the personal data controller. The personal data processor must conduct the data processing activities instructed by the personal data controller.²⁷

Third, personal data owner.²⁸ This Bill stated some of the personal data owner rights as follows: the right to request information; the right to request access to and/or a copy of personal data correction errors and inaccuracies from the Personal Data Controller; the right to request termination of personal data processing and/or deletion and/or destruction of personal data, as well as revocation of the processing consent submitted; The right to request whether or not to process personal data through a pseudonym mechanism for specific purposes; and The right to sue and receive compensation over personal data violations in accordance with the Law.

²⁴ The Personal Data Controller under the Personal Data Protection Bill include individuals, public sector institutions, and (private) organizations/institutions. See Article 23(1) of Personal Data Protection Bill.

²⁵ Article 27(1) of Personal Data Protection Bill.

²⁶ Personal data processor defined as 'individuals, public entities, and organization/institution that processes personal data on behalf of personal data controller' Article 1 Number 4 jo. Article 23 of Personal Data Protection Bill.

²⁷ Article 43 (1) of Personal Data Protection Bill.

²⁸ Personal data owner defined as 'individual as a data subject that owns personal data attached to themselves' Article 1 Number 5 of Personal Data Protection Bill.

Fourth, personal data protection officer. PDP Bill obliges that both data controllers and data processors must appoint a Data Protection Officer (DPO)²⁹ if they process personal data to provide public services; their main activities require regular and systematic monitoring of personal data on a large scale; and their principal activity consists of processing specific data³⁰, including criminal data, on a large scale. **Fifth**, the Government. Through the Ministry of Communication and Informatics, the Government could impose administrative sanctions that further will be elucidated through Government Regulation.³¹

This Bill explicitly states that regarding data processing, it is required to obtain explicit consent as stated in Article 18 (1) and its elucidation and contained in Article 20. Interestingly, the Bill stated that Personal Data Owner has the right to object to decision-making actions that are only based on the automatic processing of a person's profile (profiling). However, there is no further explanation or regulation concerning the utilization of automated processing of user data.

Hence, it is worth noting that this Bill regulated data privacy and security in general, including the activity conducted in social media and did not differentiate or specify the utilization of data for advertising purposes. Unfortunately, although this PDP Bill has the provisions that may be able to protect consumers from data privacy violations, this initiative may still be lacking as it has yet to regulate the utilization of *cookies*.³² In practice, both social media and e-commerce platforms have mentioned the utilization of cookies under their terms and condition, which will be elaborated on in the

²⁹ Article 45(2) of Personal Data Protection Bill.

³⁰ Specific data defined as 'personal data that requires special protection, and consists of data relating to health data and information biometric data, genetic data, life or sexual orientation, political orientation, criminal record, child data, personal financial data, and/or any other data in accordance with the prevailing laws and regulations'. Article 3(3) of Personal Data Protection Bill.

³¹ Article 50 (2), (3), (4) of Personal Data Protection Bill.

³² Text files used to collect the data and information from users and can be used for marketing them in advertisements network as well as third party websites with the help of JavaScript and flash technologies (Jegatheesan, S, 2013).

next section. On the contrary, Indonesian Advertising Ethics has explicitly stipulated that data collected through the cookies mechanism should be informed to the users, and the user consent regarding the cookies' utilization is required.³³

➔ Summary of the Laws and Regulations Analysis

The analysis above illustrates that Indonesia has no specific laws and regulations governing the utilization of ADM, profiling, and targeted advertising and its potential risk of data breach and data abuse. However, there are many provisions scattered in various laws and regulations relevant to ADM, profiling, and targeted advertising, such as regulations on consumer protection, obligations of PSE, and personal data protection. Furthermore, the analysis of various legal frameworks shows that the only means to minimize the potential risks of ADM, profiling, and targeted advertising is through enforcement of personal data-related provisions, considering data is the 'fuel' of the machine that makes those technologies work. The summary of the analysis can be seen in the following table.

Table 1. Summary of Laws and Regulations Related to Algorithmic Decision-Making, Profiling, and Targeted Advertising in Indonesia

	Issues Covered	Issues Not Covered
Legal Framework on Consumer Protection	<ul style="list-style-type: none"> • Consumer protection • Obligations of businesses in the advertising sector • Prohibition in advertising regarding incorrect, deceiving, and misleading statements about the advertised products and/or services • Business prohibition from offering goods and/or services by using force or any methods which cause either physical or psychological annoyance to the consumers 	<ul style="list-style-type: none"> • Obligations of social media as third parties • Consumers' legal protection against ADM, profiling, and targeted advertising • Consumers' legal protection against data privacy breaches caused by advertising practice

³³ See Number 4.6.9 of Indonesian Advertising Ethics (2020).

	Issues Covered	Issues Not Covered
Legal Framework on Consumer Protection	<ul style="list-style-type: none"> The role of the Government, Registered Consumer Association, National Consumer Protection Agency, and Consumer Dispute Settlement Agency 	
Legal Framework on Trade	<ul style="list-style-type: none"> E-Commerce Consumer protection Obligations and rights of businesses, merchants, PPMSEs, and intermediaries, including social media as third parties or intermediaries involved in producing, facilitating, and/or disseminating the electronic advertisement Prohibition of incorrect information provision and false advertising Government's role in oversight 	<ul style="list-style-type: none"> Consumers' legal protection against data privacy breaches caused by advertising practice
Legal Framework on Trade	<ul style="list-style-type: none"> E-Commerce Obligations and rights of ESOs and business entities (marketplace and social media platforms) Obligations related to the use of personal data of an individual Prohibition of abusive data practices through PDP principles Requirement of consent and the fulfillment of at least one of the legal grounds for data processing Criminal and administrative sanctions, and the possibility of a civil lawsuit 	<ul style="list-style-type: none"> Further explanation of what constitutes 'valid legal consent' in utilizing consumers' personal data The utilization of ADM, profiling, and targeted advertising
Personal Data Protection Bill	<ul style="list-style-type: none"> Obligations and rights of data controllers, data processors, and data owners Recognition of data protection officers Prohibition of abusive data practices through PDP principles Requirement of consent or the fulfillment of at least one of the legal grounds for data processing Data owner's rights related to profiling Government's role in oversight 	<ul style="list-style-type: none"> The utilization of ADM and targeted advertising The utilization of 'cookies' in advertising

Source: Processed by Author, 2022.

The existing laws and regulations are still focusing on the substances of the displayed advertisement—for instance, whether the advertisement has already in accordance with the actual conditions of goods and/or services; or whether the advertisement contains any misleading, inappropriate, and/or lawful information. It is also crucial to immediately harmonize the national laws and regulations related to online advertising and its potential risks to the consumers' data, including its way to handle the issues.

At the international and regional level, the EU has already governed online advertising under the proposed Digital Services Act. In January 2022, European Parliament passed amendments to the draft of Digital Services Act with some noteworthy changes, including the targeted advertising, profiling, and ADM provisions. The agreed document related to targeted advertising and profiling under the Digital Services Act are as follows:

- Online platforms should ensure that recipients (consumers) of the service can refuse or withdraw their consent for targeted advertising purposes;
- Online platforms should also not use personal data for commercial purposes related to direct marketing, profiling, and behaviourally targeted advertising of minors;
- Refusing consent in processing personal data for the purposes of advertising should not result in access to the functionalities of the platform being disabled;
- Targeting individuals based on special categories of data which allow for targeting vulnerable groups should not be permitted; and
- Requires digital services to offer "options based on tracking-free advertising.

Furthermore, this draft also explicitly mentioned algorithmic systems used by digital platforms. The provisions related to algorithmic systems under this Act are as follows:

- Requires online platforms to disclose to users whether their services use algorithm-based decision-making systems and how this affects the way information is displayed to the users; and
- Requires online platforms to clearly present the parameters for such recommender systems in a comprehensive manner to ensure that the users understand how information is prioritized for them.

As reflected with the overseas regulation, there is still room to improve our digital service legal framework, especially on ADM, profiling, and targeted advertising and its potential risk to consumers' data privacy and protection rights.

➔ **Mapping and Analysis: Algorithms for Advertising and Rules of the Game in Digital Platforms**

This section consists of 4 (four) sub-section that cover advertisement-related policies in both social commerce and e-commerce platform. The sub-sections are as follows: Instagram, Facebook, Bukalapak, and Shopee. Each sub-section will analyze and discuss whether the existing policies and/or terms and conditions are sufficient to protect consumers against the potential risks of ADM, profiling, and targeted advertising.

➔ Instagram

Firstly, it is crucial to understand how Instagram works in displaying suggested posts, reels, story, and account for the user, including posts for which businesses can promote their products and/or services. In terms of what the users can view in their feed, Instagram utilizes an algorithm that further will rank the posts based on what users 'care the most' in their Instagram feeds. The different kind of algorithms is tailored specifically to each feed, explore, and reel. For example, regarding the displayed stories and feeds, Instagram ranked them based on the information signals about each post, according to these order (Mosseri, A., 2021): Information about a post (how popular, how long is the content, location attached, etc.); Information about the person who posted (how many times other users have interacted with that person); Your activity (how many posts you've liked); Your history of interacting with someone (how interested you are in seeing posts from a particular person).

Instagram also mentions what informations they collect and for what purpose. The following are the information Instagram collects and uses: information and contents that the user posted (e.g., metadata, photo location, the date a file was created, account profile); networks and connections (e.g., people, accounts, hashtags that connected to the users); app usage (e.g., types of content that the user view or engage, features being used, actions, and people that the user mostly interact or engage); information about transactions while purchasing Instagram products; information about the user that is provided by other users; device information (e.g., device attributes, device operations, identifiers, device signals, data from device settings, cookie data); and information about the user that is provided by partners such as advertisers, app developers, and publishers (e.g., information about the user's device, websites that the user visit, purchases, advertisement that the user sees, etc).

Through the data privacy policy, Instagram uses users' information to provide, personalize and improve its products, including providing data for advertisements and other sponsored content.³⁴ In their data policy, Instagram has also emphasized that they provide advertisers with reports about the kinds of people seeing their advertisements and how their advertisement is performing. Still, they will not share information that personally identifies users unless they give Instagram permission. However, under their terms and conditions, Instagram did not specifically regulate advertisement under separate policies.

Pertaining to the utilization of cookies in the advertisement, Instagram has also mentioned that under their Cookies Policy that through cookies, Instagram and their advertising partners may use such technologies to deliver advertising that is relevant to the users' interests.³⁵ However, this policy did not specifically and explicitly address what kind of information (e.g., IP address, email address, etc.) they obtained through cookies technology. This policy only mentions that these technologies can be used to remember that the users' device has visited a site or service and may also be able to track the devices browsing activity on the other sites or services other than Instagram. That information is being used and shared with other organizations outside Instagram, including the advertiser, to deliver the advertisement and measure the effectiveness of an advertising campaign.

➔ **Facebook**

It is common knowledge that many social media platforms, including Facebook, have developed their own personalized feature. It means that each user's feed will be highly personalized based on users' behaviors on social media platforms. Facebook has been changing its approach to the news feed's algorithm, from

³⁴ See Instagram's Data Policy here: <https://help.instagram.com/155833707900388>

³⁵ See Instagram's Cookies Policy here: https://help.instagram.com/1896641480634370/?helpref=hc_fnav

reverse-chronological order to the 'interaction-driven' mechanism (Oremus, Alcantara, Merrill, & Galocha, 2021).³⁶ To enable such a personalized mechanism, the machine should be fed with users' data, indicating the use of ADM for profiling and targeted advertising. Therefore, it is also essential to investigate the scope of users' data processed, how they are being used, and Facebook's response to potential risks. In general, users' information collected can be categorized into three categories.³⁷

First, data from things users' do and provide, including (a) information and content users' provide, which can include the content's metadata (e.g., location of a photo), (b) networks and connections (e.g., people, account, hashtag, groups, and pages users' connected to and how they interact with them); (c) usage (e.g., how users' use Facebook, types of content users' view or engage, etc.); transactions made on Facebook (e.g., when users' make a purchase in a game or make a donation); (d) things other do and information they provide about users' (e.g. when people share or comment a photo about someone). Second, data regarding the device include attributes, operations, identify, signals, device setting, network and connections, and cookie data. Third, information from partners (e.g., when Facebook's users use third-party apps using Facebook API).

Facebook's Data Policy states that Facebook stores data until it is no longer necessary or until the user's account is deleted. Therefore, if a user deletes their account, Facebook will also delete the things they have posted, and the user will not be able to recover that information later. It is vital to ensure that Facebook will not process any data about the user that has deleted their account. Furthermore, for verification purposes, the government-issued ID submitted will be deleted 30 days after the review unless otherwise stated. These

³⁶ It means the algorithm prioritizes posts from friends and family, as well as viral memes and divisive content.

³⁷ See Facebook's Data Policy here: <https://m.facebook.com/privacy/explanation/>

policies show that Facebook tries to comply with data retention and data minimization principles in processing users' data.

Moreover, Facebook also has a separate advertising policy that advertisers should follow to be reviewed. It specifically addresses the issue of "targeting", in which advertisers must not use targeting options to discriminate against, harass, provoke, or disparage users or engage in predatory advertising practices.³⁸ For advertising, Facebook has also stated in their Data Policy that they do not share information that personally identifies a user unless the user gives Facebook permission. It can be challenging for users to ensure that they do not provide unnecessary permission to process personal data, considering how consent works on social media platforms.

➔ **Bukalapak**

Founded in 2010, Bukalapak is considered one of Indonesia's leading e-commerce platforms. According to Databoks, as of three quarters of 2021, the number of Bukalapak's monthly visitors amounted to approximately 30,1 million (Databoks, 2021). Since last year, Bukalapak has ranked third in e-commerce with the most monthly site visitors after Shopee and Tokopedia (Surur, F., 2021). Judging from its enormous impact on the e-commerce field, it is important to further discuss the platform's policy to protect their consumers' rights, especially regarding data abuse and harmful advertising techniques.

Bukalapak has a specific section in their terms of service regarding user data. The first clause stipulates that Bukalapak has the authority to collect, use, access, store, and/or process users' data. The second clause concerning Bukalapak's authority to use users' collected data to improve the application's quality is detailed in its privacy policy. Lastly, Bukalapak has the authority to disclose

³⁸ See Facebook's Advertising Policies here: <https://www.facebook.com/policies/ads/>

users' data for legal process/government institutions requests.³⁹ Under Bukalapak's privacy policy, it details that the information collected from the users includes 1) Information on Bukalapak accounts; 2) User behavior in Bukalapak (e.g., users' preferences and interests); and 3) Information from the third party. The data can be given to a third party, which can be used to develop the application, database management, analysis, service improvement, and promotion and advertising.⁴⁰ Another section of Bukalapak's privacy policy also mentioned that Bukalapak has the authority to collect, use and disclose users' data for promotion and advertisement purposes.

Bukalapak has "cookies" on its site, of which it can give users' cookies data to a third party, which is also being used for advertising purposes. The cookies have been regulated under the privacy policy. The provisions are similar to Instagram's Cookies Policy. However, Bukalapak has specifically mentioned the examples of information they collect and share through this technology: the location of the data, advertisement identification, and email address used for advertising segmentation. Moreover, Bukalapak has a separate advertising policy to address advertisements on the platform. The advertising policy covers provisions on advertisement placement, prohibited contents, the advertiser obligations, etc.⁴¹

➔ **Shopee**

Similar to other e-commerce platforms, such as Bukalapak above, Shopee can collect, use, disclose, and/or process users' data if they agree to Shopee's privacy policy.⁴² The types of users' data collected include name, billing address, bank account and payment information, information sent by the devices used,

³⁹ See Bukalapak's Terms and Conditions here: <https://www.bukalapak.com/terms>.⁹⁵

⁴⁰ See Bukalapak's Privacy Policy here: <https://www.bukalapak.com/privacy>

⁴¹ See Bukalapak's Advertisement Policy here: <https://www.bukalapak.com/ads-privacy>

⁴² However, like other e-commerce and social media platforms, users have no choice but to agree with the privacy policies to use the platform's services.

government-issued identification, marketing and communications data (preferences in receiving marketing from Shopee and communication preferences), transaction data, and photographs, and all data about the content used by users.⁴³

Moreover, to protect buyers' personal data, Shopee will disguise and/or anonymize buyers' data for any unpaid orders, canceled orders, or completed orders. For completed order, the buyer's personal data will be disguised and/or anonymized for 61 (sixty-one) days after the order is completed. However, it is not clear whether, after 61 days, the users' data will be shown to the seller or not. Shopee also collects cookies data,⁴⁴ which they will link to personal data, including items users' have selected for purchases and which web pages users viewed. Therefore, if Shopee users open a web page, advertisements from Shopee sometimes appear, even though the website is not related to Shopee.

Furthermore, the collected data are also being used by Shopee for marketing and advertising purposes. The privacy policy states that Shopee can send their users marketing information and advertisement through 'various modes of communication'. Although the policy indicated that users could unsubscribe from marketing information, it is not clearly stated what modes of communication they used to share marketing information and advertisement.

Furthermore, the collected data are also being used by Shopee for marketing and advertising purposes. The privacy policy states that Shopee can send their users marketing information and advertisement through 'various modes of communication'. Although the policy indicated that users could unsubscribe from marketing information, it is not clearly stated what modes of communication they used to share marketing information and advertisement.

⁴³ See Shopee Privacy Policy here: <https://shopee.co.id/docs/3612>

⁴⁴ Cookies is an identifier stored on user's device that record how and when the service or platform is used or visited, by how many people, and other activities on the platform.

Moreover, they can also transfer users' personal data to third parties for purposes stated in the Privacy Policy, which include (a) complying with legal process; (b) complying with requests from any governmental or regulatory authority that has jurisdiction over Shopee; (c) enforce Shopee's Terms of Service or this Privacy Policy; (d) respond to any threatening or actual claim against Shopee or any other claim that any Content violates the rights of a third party; (e) respond to user requests for customer service; or (f) protect Shopee's rights, property or personal safety. Although the Privacy Policy stated that Shoppe would strive to ensure that third parties keep users' personal data secure, the clause seems to be very broad, and it does not clearly indicate how they guarantee the protection of users' data processed by third parties.

To conclude, Shopee's Terms of Service and Privacy Policy provide similar substance to previously discussed e-commerce and social media platforms, especially concerning collecting and utilizing users' data. Various clauses in the Terms of Service and Privacy Policy clearly indicates that Shopee uses ADM, profiling, and targeted advertising in their platforms to provide more personalized features, goods offered, as well as other advertisements.

Apart from the explanation above, the Privacy Policy stated that Shopee would delete or anonymize users' personal data reasonably if the purpose of personal data were collected no longer being served, retention is no longer necessary for any legal or business purposes, and no warrant legitimizes the further withdrawal of personal data. However, if users stop using the platform, Shopee may continue to store, use and/or disclose users' personal data in accordance with Shopee's Privacy Policy and legal obligations based on privacy laws. However, it is unclear how long Shopee will keep user deleted account' data. Considering various activities can be conducted using users' personal data as provided in the Privacy Policy, it is crucial to give users certainty on this matter to ensure

that in the future, ex-users will not be disturbed and damaged by the arbitrary use of the stored personal data when they no longer use the services provided.⁴⁵

➔ Summary of Digital Platforms' Community Guidelines, Terms and Conditions, and/or Policies related to User Data Utilization

The analysis above shows that all platforms discussed collect and use their users' data in many forms to develop the services and experiences provided to their users. In essence, both social media and e-commerce platforms already have a variety of rules of the game related to data privacy and advertising. Particular gaps and differences between how the state and platforms regulate and protect the consumer's rights to data protection regarding the advertising techniques should be acknowledged, especially by setting a clear legal basis on advertising techniques and their risks as a standard for social media and e-commerce platforms. The summary of how the selected platforms use their users' data can be seen in the following table.

Table 2. Summary of Selected Platforms' Community Guidelines, Terms and Conditions, and/or Policies related to User Data Utilization

Instagram	Facebook	Bukalapak	Shopee
Social Commerce	Social Commerce	E-Commerce	E-Commerce
<ul style="list-style-type: none"> Data Policy: <ul style="list-style-type: none"> What kinds of information does Instagram collect How does Instagram use the information How is the users' information shared How to manage and delete the users' information 	<ul style="list-style-type: none"> Data Policy: <ul style="list-style-type: none"> What kinds of information does Facebook collect How does Facebook use the information How is the users' information shared How to manage and delete the users' information 	<ul style="list-style-type: none"> Privacy Policy: <ul style="list-style-type: none"> Data Collection and Protection Data use, storage, and processing Data removal Cookies policy Limitation of the Platform Liability 	<ul style="list-style-type: none"> Privacy Policy: <ul style="list-style-type: none"> When will Shopee collect personal data What personal data will Shopee collect Collection of other data Cookies policy How does Shopee use the information that the user provides

⁴⁵ A good example on clause regarding when the platform store and delete users data can be seen in Facebook's Data Policy. It states that Facebook stores data until it is no longer necessary or until the user's account is deleted.

Instagram	Facebook	Bukalapak	Shopee
Social Commerce	Social Commerce	E-Commerce	E-Commerce
<ul style="list-style-type: none"> How does Instagram protect the data How does Instagram operate and transfer the data • Cookies Policy: 	<ul style="list-style-type: none"> How does Instagram protect the data How does Instagram operate and transfer the data • Cookies Policy • Advertising Policy • Prohibited and restricted content • Prohibition to use of targeting options to discriminate, harass, provoke, or disparage users or to engage in predatory advertising practices • Data use restrictions 	<ul style="list-style-type: none"> • Advertising Policy • Prohibited contents • Obligations of the advertiser • Limitation of the Platform Liability 	<ul style="list-style-type: none"> How does Shopee protect and retain consumer's information Information disclosure for third parties Information collected by third parties How to withdraw consent, request access to, or correct the information provided to Shopee • Cookies Policy • Advertising Policy • Prohibited content • Responsibilities of consumers • Responsibilities and rights of Shopee • Confidential information to third parties • Limitation of Shopee Liability





Chapter V



Conclusions and Recommendations



A Conclusion

The use of algorithm technology is inevitable in the age of e-commerce. Indeed, this study is primarily evoked by the appearance of social commerce phenomenon in Indonesia. However, we find that the two trading platforms, e-commerce and social commerce use similar technologies, such as machine learning, artificial intelligence, data minings, as well as data analytics. These automations support the ecosystem of Algorithmic Decision Making (ADM), which is also called - simultaneously, with Algorithmic Decision System (ADS). E-commerce and social commerce are using this technology to provide service to their users, both sellers and buyers. Hence, the use of personal data is criticized as most users do not comprehend how their data are being collected, stored, as well as processed. Furthermore, the use of ADM may also lead to the emergence of "dark patterns", which are tricks where user interfaces used by certain platforms or online businesses influence consumers to make decisions that they would not have otherwise made if fully informed and capable of selective alternatives. This may undermine the right of consumers to transparency and honest information, as well as their autonomy in making informed decisions.

Reviewing the current regulatory framework in Indonesia, there has not been any law specifically regulating social commerce. On the other hand, the provisions regulating e-commerce fall under several laws which are Legal Framework on Consumer Protection,

Legal Framework on Trade, Legal Framework on Electronic Information and Transaction, and Data Protection Bill. There have not been any specific rules that regulate the ADM itself. Nonetheless, self-regulatory mechanisms are applied by the platforms to provide consumers sufficient information on how their personal data will be collected, processed, and stored.

Based on the interview we have with academicians and e-commerce platforms, it is not the personal data per se that contributes to the ADM, instead, the behavior of users are the most important. The machine generates preferences and service options based on our clicks on the platforms. Therefore, regulations alone are not enough. Users' digital literacy takes the main part for users to better protect themselves.

B Recommendations

Based on the discussions above, this research argues that various stakeholders can contribute to minimizing the risks for consumers due to ADM, profiling, and targeted advertising implementation. The recommendations are presented below.

➔ Policymakers

● Reformulating the regulation of online advertising

● Defining terms related to online advertising

The existing regulation has yet mentioned the kinds of digital advertising techniques such as ADM, profiling, and targeted advertising that are commonly used by social media and e-commerce platforms in generating their advertisements. It is critical to immediately define along with its potential risks to the rights of data privacy and protection of the consumers under specific regulations on data privacy and/or advertisement.

- Identifying the obligations and rights of social media and e-commerce platforms as third parties or intermediaries related to advertising practice

Unfortunately, the existing regulations and policies have yet explicitly mentioned the obligations and rights of social media and e-commerce platforms in regard to the consumers' data utilization for advertisement purpose. The current regulations and policies have only governed in general—considering that all of the regulations and policies under Consumer Protection, Trade, and EIT did not explicitly mention ADM, profiling, and targeted advertising.

- Regulating the utilization of the consumers' data for ADM, profiling, and targeted advertising

The provisions related to advertising under Consumer Protection, Trade, and Electronic Information and Transaction are still burdening on the substance of the advertisement. For instance, how the displayed online advertisement should conform with the conditions of goods and/or services, false, misleading, inappropriate information contained in the advertisement, and/or unlawful advertisements, while the potential risks related to the consumers' data remain untouched. As discussed, it is important to immediately reformulate certain provisions that specifically regulate these matters. As there is still room for improvement in Indonesia's legal framework pertaining to the advertisement, the government can refer to the newly promulgated legal framework for digital service in Europe, namely Digital Services Act. According to what is already being discussed above, the existing Digital Services Act has

has explicitly regulated ADM, profiling, and targeted advertising under its act.

- Optimizing personal data protection in Indonesia through PDP Bill

- Considering that there is still no comprehensive and specific regulation of data protection, we urge the government to immediately enact the PDP Bill. However, it is worth noting that the current draft can be improved. For instance, the PDP bill has yet to accommodate ADM, targeted advertising, and cookies utilization under any provisions.

- Enhancing cooperation with social media platforms, e-commerce platforms, the national consumer protection agency, and consumer association

- By reflecting on the potential risks pertaining to consumers' data use for advertising purposes, it is important for all stakeholders to recognize the importance of the protection towards consumers' rights to data privacy while advertising. Therefore, it is crucial for each party to immediately establish a strong and firm collaboration by making a joint decree or other legal instruments to ensure the platforms' compliance as well as aligning perceptions between parties. We also recommend for the government, the national consumer protection agency, association, and also platforms to hold a multi-stakeholder discussion and keep maintaining effective communication in handling issues related to the consumers' data.

It has been mentioned that regulations on the technology itself is not adequate. Skills and capacity of the users also determine how

users can protect themselves. This notion is also emphasized by our interviewees, ranging from government, associations, as well as industries. Therefore, some initiatives taken by stakeholders are also focusing on increasing the level of users' digital skills.

➔ **Businesses**

Businesses which implement ADM, profiling, and targeted advertising in their services should be able to ensure consumer privacy, safety and sovereignty. This can be done by allowing users to make personal and customized decisions on what services/add-ons they want to implement while using their services. Self-regulation will allow users to have more control over their decisions on the platforms. Additionally, platforms also carry out several campaigns for both sellers and consumers in order to increase their awareness and skills in protecting their data.

➔ **Consumer associations and other CSOs**

Consumers associations and CSOs have an important role in consumers' awareness and education regarding ADM practices. We have learned from the previous chapters that consumers in Indonesia are not familiar with the practices of ADM, profiling, and targeted advertising. Many of them are also unaware of the potential risks resulting from such practices. Thus, consumer associations and other CSOs' should further educate and raise awareness on ADM practices amongst stakeholders (especially consumers). Educating consumers on how they can better protect themselves in regard to making decisions online should be a priority for consumer associations and concerned CSOs.

Consumer associations and CSOs could start the efforts to educate consumers by conducting a series of training on digital literacy, workshops, and campaigns to familiarize consumers with ADM, profiling, targeted marketing, and the harms that it may cause. These advocacy efforts shall also extend to the other stakeholders,

not limiting the possibility of joint efforts with relevant government agencies and platforms.

It is also important for consumer associations and CSOs to provide consumers with any guidance required to ensure their protection and rights in online transactions. Aside from that, advocating for more comprehensive regulations on the practices of ADM, profiling, and targeted advertising is another necessary step that consumer associations and CSOs should take.

➔ **Consumers**

Consumer protection can only be achieved with a combined effort of key stakeholders, in which consumers are one of them. Hence, consumers have to bear some responsibility. There are several things that consumer could do to partake in consumer protection effort, such as:

- Consumers need to improve their digital literacy by actively seeking information and learning the latest trends related to e-commerce and social commerce practices in Indonesia.
- Consumers also need to be aware of their rights as consumers.
- It is also important for consumers to realize that they are also responsible for the protection of their data. Thus, consumers need to take a more active role in data protection initiatives by practicing the principles of personal data protection in their daily lives.

→ References

- A Mathur, et al., 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites,' (2019), Proc. ACM Hum.-Comput. Interact. 3, CSCW, Vol. November/Article 81, <<http://dx.doi.org/10.1145/3359183>> in Wahyuningtyas, S. (2021)
- Al-Adwan, Ahmad Samed; and Kokash, Husam, 'The Driving Forces of Facebook Social Commerce', Journal of Theoretical and Applied Electronic Commerce Research 14(2) (2019)
- Aprilianti., I., 'Melindungi Masyarakat: Memajukan Hak-Hak Konsumen Digital', CIPS, (2020), <https://c95e5d29-0df6-4d6f-8801-1d6926c32107.usrfiles.com/ugd/c95e5d_c1e1d8e85dfe4552934aff1b830b9c32.pdf>
- ASEAN Committee on Consumer Protection, 'Indonesia's Consumer Protection', <<https://aseanconsumer.org/selectcountry=Indonesia>>
- Brownsword, Roger, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' in Gutwirth, Serge; Pouillet, Yves; De Hert, Paul; de Terwangne, Cecile; Nouwt, Sjaak (eds) Reinventing Data Protection? (Springer, 2009).
- Bukalapak, 'Advertisement Policy', <<https://www.bukalapak.com/ads-privacy>>
- Bukalapak, 'Privacy Policy', <<https://www.bukalapak.com/privacy>>
- Bukalapak, 'Terms and Conditions', <<https://www.bukalapak.com/terms.95>>
- Burhan, F., (2021). Kominfo Tangani 43 Kebocoran Data Tahun Ini, BPJS Kesehatan Belum Artikel ini telah tayang di Katadata.co.id dengan judul "Kominfo Tangani 43 Kebocoran Data Tahun Ini, BPJS Kesehatan Belum".[online] Available at: <[Study on Risks for Consumers Due To Algorithmic Decision-making and Profiling
by E-Commerce and Social Media Platforms in Indonesia](https://katadata.co.id/desyetyowati/digital/61cd8cf0e5173/kominfo-tangani-43-kebocoran-data-tahun-ini-bpjs-kesehatan-belum#:~:text=Kementerian%20Komunikasi%20dan%20Informatika%20(Kominfo,Jenderal%20Aplikasi%20Informatika%20(Aprika).> [Accessed 20 March 2022].</p>
</div>
<div data-bbox=)

Castelluccia, C., & Le Métayer, D. (2019). Understanding algorithmic decision-making: Opportunities and challenges. European Parliament.

Castelluccia, C., & Le Métayer, D. (2019). Understanding algorithmic decision-making: Opportunities and challenges. European Parliament.

Competition & Markets Authority. (2021). Algorithms: How they can reduce competition and harm consumers. GOV.UK. Retrieved 22 February 2022, from <<https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers#contents>>

Databoks, 'Naik Tipis, Kunjungan ke Web Bukalapak pada Kuartal I - 2021', <<https://databoks.katadata.co.id/datapublish/2021/11/25/naik-tipis-kunjungan-ke-web-bukalapak-pada-kuartal-iii-2021>>

Data Guidance, 'Indonesia-Data Protection Overview', <<https://www.dataguidance.com/notes/indonesia-data-protection-overview>>

EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

EU Digital Service Act

Facebook, 'Advertising Policies', <<https://www.facebook.com/policies/ads/>>

Facebook, 'Data Policy', <<https://m.facebook.com/privacy/explanation/>>

Facebook, 'Terms of Service', <<https://www.facebook.com/terms.php>>

Government Regulation No. 71 of 2019 on Implementation of Electronic System and Transactions.

Government Regulation No. 80 of 2019 on E-Commerce.

H Brignull, 'What Are Dark Patterns' (2019) <https://www.darkpatterns.org/> diakses 29 September 2021. in Wahyuningtyas, S. (2021)

H., Hettiarachchi, C. Wickramasinghe and S. Ranathunga, 'The Role of Social Commerce on Consumer Decision: A Theoretical Foundation', *Journal of Business and Technology*, 1(2) (2017).

Instagram, 'Cookies Policy', https://help.instagram.com/1896641480634370/?helpref=hc_fnav

Instagram, 'Data Policy', <https://help.instagram.com/155833707900388>

Interview with Andry Alamsyah, 2022.

Interview with Badan Perlindungan Konsumen Negara, 2022

Interview with Bank Indonesia, 2022

Interview with Center for Indonesian Policy Studies, 2022

Interview with E-Commerce Platform, 2022

Interview with Yayasan Lembaga Konsumen Indonesia, 2022

J Luguri dan LJ Strahilevitz, 'Shining a Light on Dark Patterns', *University of Chicago, Public Law*

Jegatheesan., S., 'Cookies Invading Our Privacy for Marketing, Advertising, and Security Issues' , *International Journal of Scientific and Engineering Research* 4(5) (2013), <https://doi.org/10.48550/arXiv.1305.2306>

Karagoel, I., & Nathan-Roberts, D. (2021, September). Dark Patterns: Social Media, Gaming, and E-Commerce. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 65, No. 1, pp. 752-756). Sage CA: Los Angeles, CA: SAGE Publications.

Kerry, Cameron F.; and Chin, Caitlin, 'Hitting refresh on privacy policies: Recommendations for notice and transparency', *Brookings*, <<https://www.brookings.edu/blog/techtank/2020/01/06/hitting-refresh-on-privacy-policies-recommendations-for-notice-and-transparency/>>

Kingsley, S., Wang, C., Mikhalenko, A., Sinha, P., & Kulkarni, C. (2020). Auditing digital platforms for discrimination in economic opportunity advertising. arXiv preprint arXiv:2008.09656.

KOMPAS.com. (2022). Saat Nomor KTP (NIK) Jokowi Bocor.... [online] Available at: <<https://www.kompas.com/tren/read/2021/09/04/170500165/saat-nomor-ktp-nik-jokowi-bocor?page=all>> [Accessed 20 March 2022].

Law No. 11 of 2008 on Electronic Information and Transactions.

Law No. 19 of 2016 on Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.

Law No. 7 of 2014 on Trade.

Law No. 8 of 1999 on Consumer Protection.

Lee, N. T., Resnick, P., & Barton, G. (2019). Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms. Brookings Institute: Washington, DC, USA.

Lee, Z., 'Indonesia's Tech Pioneer Raises \$1.5 Billion Through IPO to Battle E-Commerce War', *Forbes*, <<https://www.forbes.com/sites/zinnialee/2021/07/22/indonesia-tech-pioneer-raises-15-billion-through-ipo-to-battle-e-commerce-war/?sh=36bcd555169c>>

MacCarthy, Mark, 'Fairness in Algorithmic decision-making', *Brookings*, <<https://www.brookings.edu/research/fairness-in-algorithmic-decision-making/>>

Mann, M. and Matzner, T. (2019) 'Challenging algorithmic profiling: The limits of data protection and anti-discrimination in

responding to emergent discrimination', Big Data & Society. doi: 10.1177/2053951719895805.

Mann, M. and Matzner, T. (2019) 'Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination', Big Data & Society. doi: 10.1177/2053951719895805.

Matzner, Tobias; and Mann, Monique, 'Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination', Big Data and Society 6(2) (2019).

Minister of Communication and Informatics Regulation No. 5 of 2020 on Electronic System Provider in Private Sector.

Minister of Trade Regulation No. 50 of 2020 on Provisions of Business Licensing, Advertising, Guidance, and Supervision of Businesses Trading Trade through Electronic Systems.

Mosseri, A., 'Shedding More Light on How Instagram Works', *Instagram*, <<https://about.instagram.com/blog/announcements/shedding-more-light-on-how-instagram-works>>

Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification'. *The Journal of Strategic Information Systems*, 24(1), 3-14.

Noh, Y (2016) "A study on the effect of digital literacy on information use behavior". *Journal of Librarianship and Information Sciences* 49(1). Doi: <https://doi.org/10.1177/0961000615624527> Oremus, Will; Alcantara, Chris; Merrill, Jeremy B.; and Galocha, Arthur, 'How Facebook shapes your feed', *The Washington Post*, <<https://www.washingtonpost.com/technology/interactive/2021/how-facebook-algorithm-works/>>

Organisation for Economic Co-operation and Development, 'Good Practice Guide on Online Advertising: Protecting Consumers in E - C o m m e r c e ' , <[https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP\(2018\)16/FINAL&docLanguage=En](https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2018)16/FINAL&docLanguage=En)>

Personal Data Protection Bill.

Primawan, B. (2022) Interviewed by Center for Digital Society, Research on Social Media for Online Commerce and Its Impact on Consumers in Indonesia, 23 February.

PWC, 'Indonesia's Progress on Data Protection', <<https://www.pwc.com/id/en/publications/digital/digital-trust-newsflash-2020-02.pdf>>

Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Riyadi., G., A., 'Data Privacy in the Indonesian Personal Data Protection Legislation', CIPS, (2021), <https://c95e5d29-0df6-4d6f-8801-1d6926c32107.usrfiles.com/ugd/c95e5d_d4dad8abc56341b090a727d438957b57.pdf>

Schlee, C. (2013). Targeted advertising technologies in the ICT Space: A use case driven analysis. Springer Science & Business Media.

Schlee, Christian, Targeted Advertising Technologies in the ICT Space: A Use Case Driven Analysis (Springer Vieweg, 2013).

Shopee, 'Privacy Policy', <<https://shopee.co.id/docs/3612>>

Shopee, Terms of Service', <<https://shopee.co.id/docs/3001>>

Soemarwi., V. W., and Susanto, W., 'Digital Technology Information in Indonesia: Data Privacy Protection is a Fundamental Right', Proceedings of the International Conference on Economics, Business, Social, and Humanities, 570 (2021) <https://linter.untar.ac.id/repository/penelitian/buktipenelitian_10214002_3A020921105357.pdf>

Surur, F., 'Top 10 Best Selling E-Commerce 2021 in Indonesia: Tokopedia Becomes the Champion, Shopee Couped, Tren Asia', <<https://www.trenasia.com/top-10-best-selling-e-commerce-2021-in-indonesia-tokopedia-becomes-the-champion-shopee-couped>>

Sweeney, L. (2013). Discrimination in online ad delivery. *Communications of the ACM*, 56(5), 44-54.

Wahyuningtyas, S. (2021) 'Kajian Dark Patterns Dalam Platform E-Commerce di Indonesia',

Working Paper No. 719, University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879, 7 Agustus 2019, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205, accessed on 1 March 2022.






Center for Digital Society

Faculty of Social and Political Sciences
Universitas Gadjah Mada
Room BC 201-202, BC Building 2nd Floor,
Jalan Socio Yustisia 1
Bulaksumur, Yogyakarta, 55281, Indonesia

Phone : (0274) 563362, Ext. 116
Email : cfds.fisipol@ugm.ac.id
Website : cfds.fisipol.ugm.ac.id

 facebook.com/cfdsugm

 [Center for Digital Society \(CfDS\)](#)

 [cfds_ugm](#)

 [@cfds_ugm](#)

 [@cfds_ugm](#)

 [CfDS UGM](#)