



Implemented by



UNIVERSITAS
GADJAH MADA



Study on Countering Abusive Business and Data Practices in Social Commerce in Indonesia





Authors



Dewa Ayu Diah Angendari
Faiz Rahman
Treviliana Eka Putri
Ruth Tarullyna Simanjuntak
Rizka Khairunissa Herdiani
Gabriela Eliana

Reviewer



Dr. Poppy Sulistyaning Winanti

Designer



Muhammad Fanani Arifzqi

Disclaimer

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.



Implemented by





Content

ii	Content
iv	Table
01	Executive Summary
05	Introduction
10	Analysis of Social Media Platform Liability
12	Mapping and Analysis of Indonesian Laws and Regulations
13	• Legal Framework on Consumer Protection
16	• Legal Framework on Trade
20	• Legal Framework on Electronic Information and Transaction (EIT)
26	• Personal Data Protection Bill
29	• Summary of Indonesian Legal Frameworks Analysis
32	Analysis on Social Media Platforms’ Community Guidelines
34	• How Platforms Protect Consumers and Businesses
34	• Comparing the Implementation of Community Guidelines in Social Media vs. E-Commerce Platforms
36	Analysis of Consumer Risks in Social Commerce Transactions in Indonesia
37	Risks and Challenges of Social Commerce Practice in Indonesia
38	• Product Risk
39	• Financial Risk
39	• Privacy Risk
40	Risks in Numbers: Identifying Cases and Complaints
41	The National Consumer Protection Agency (BPKN)
41	The Indonesian Consumers Foundation (YLKI)
42	The Indonesian Directorate General of Consumer Protection and Trade Compliance (PKTN) under the Ministry of Trade
43	Yogyakarta Consumers Foundation (LKY)

45	Mapping the Existing Situation of Social Commerce Environment in Indonesia
45	• Regulatory Framework and Enforcement
47	• Ethical Business and Data Practices in Social Commerce
49	• The Need for Consumer Empowerment
51	Recommendations
55	References



Table

29

Table 1

**Summary of Indonesian Legal Frameworks related to
Abusive Business and Data Practices in Social Commerce**

Executive Summary





Executive Summary

The Covid-19 pandemic has accelerated Indonesia's digital economy in an unprecedented way. According to a survey conducted by Rakuten Insight, more consumers opted for online transactions during the pandemic in comparison to the previous year (Statista, 2022). One of the channels in which online transactions can be conducted is through social commerce. Due to its relatively ease of use, consumers have also shifted to social media platforms to conduct online transactions. On the one hand, social commerce promises financial inclusion by enabling direct transactions between its users with fewer barriers and conditions compared to traditional and e-commerce transactions. On the other hand, there are some underlying risks concerning social commerce practices, such as misleading advertisement and claims, delivery failure, unclear complaint channels and dispute resolution mechanisms, and possible data breach and abuse. These potentially abusive business and data practices need to be addressed immediately.

This research aims to investigate the business and data practices of social commerce in Indonesia. Although when the research is conducted, social commerce is dominated by global platforms such as Meta, Tiktok, and Line, the dynamics of the socio and political context in Indonesia is different compared to other countries. Despite high internet penetration into most regions, the Indonesian digital literacy index varies. There is also relatively limited research on Indonesians' awareness and behaviors towards privacy and personal data. In addition, the country is still lacking regulation in personal data protections which leads to power imbalance between the platforms and its users.

To gain more understanding, this research conducted a literature review, regulation mapping, and interviews to relevant stakeholders ranging from the Indonesian government, CSO, and academics. Unfortunately, researchers are not able to set any interviews with social

media platforms. However, we have conducted thorough research of the publicly available data that social media platforms published in regards to terms and conditions as well as community guidelines.

Further, this research highlights:

Currently, there is yet to be any specific laws and regulations on social commerce. Generally, there are provisions in the Consumer Protection Law, the Trade Law and related Government Regulations as well as EIT Law, and their implementing regulations, that guarantees (1) consumer rights to safety, accurate information and redress, (2) business responsibilities, including e-commerce, and social media platforms and online sellers, and (3) online transactions. The upcoming RUU PDP shall also regulate data privacy and sharing, but this is yet to take place. While Kemendag, BPKN and BPSK are in charge of matters related to consumer protection and dispute settlement, social media moderation is under the purview of Kominfo. For the time being, the agencies can only request that consumers opt for safer platforms when transacting online to ensure their safety. Together with Facebook and Instagram, Kemendag and Kominfo have established a coordination mechanism to take down fraudulent social media accounts, but this relies heavily on reports from users and, thus, more proactive efforts may be needed.

Social media platforms for the time being have also developed community guidelines for its users, which applies to both sellers and consumers on its platforms specifically related to product advertisement and scams. However, there is yet to be an established mechanism to obtain compensation in case a transaction goes wrong. From the explanation above, risks that consumers face in social commerce involve those related to the quality of the product, potential financial loss in case of scams, and privacy risks.

Considering the gaps in the regulatory framework and existing practices, the following are some recommendations in countering abusive practices in social commerce:

- Policymakers/regulators shall strengthen inter-agency coordination to more proactively mitigate potential scams, financial loss and privacy issues. A co-regulatory mechanism together with businesses can be adopted as a benchmark for redress mechanisms and create a data privacy baseline. In relation to the latter, ratification of RUU PDP shall be prioritized. Requirements and procedures for licensing, if any, shall be streamlined.
- Businesses, from social media platforms to sellers, share the same responsibility to uphold consumer rights and ensure data privacy. Community guidelines shall be made more concise and easier to understand, and continuous education for its users should be provided.
- Efforts to increase digital literacy and empower consumers shall continue. Consumer associations and other CSOs can cooperate with either government agencies or businesses to educate consumers with approaches that are more targeted (e.g. based on the needs and methods that are appropriate to the consumer's demographics).





Introduction



Introduction

The term 'social commerce' has been subject to ongoing research within the area of digital platforms such as social media. Social commerce is understood as the tools that facilitate various commercial activities through social media or any third-party Social Network Sites in consumers' online shopping processes or merchants' interactions with their customers (Handarkho, 2021; Lin et al., 2017). Essentially, social media acts as a medium for users to contribute and expand their social networks to exchange information regarding products or services, which eases both the merchants' selling and the customers' purchases (Lam et al., 2016). Social commerce has mostly covered major topics such as innovation, advertisement, organization, and word-of-mouth (WOM). Despite this, it has yet to discuss the risks of social commerce pertaining to data protection and privacy and its business practices.

In recent years, social commerce in Indonesia has become more relevant as social media users are increasing and brings a significant contribution to economic growth (Meilitanova, 2021; Das et al., 2018). Social commerce generated approximately \$3 billion in gross merchandise value and accounted for roughly 40 percent of today's online commerce market in Indonesia. Moreover, the value of social commerce is forecasted to rise to \$55–65 billion by 2022 (Das et al., 2018). However, a recent finding shows that the gross merchandise value (GMV) of social commerce was roughly \$6.1 billion, an increase from previous years, and is expected to reach \$25 million (Nurhayati-Wolff, 2021), a meek forecast in comparison to the former findings. Furthermore, various Indonesian small and medium enterprises (SMEs) started to take advantage of social media platforms to elevate their sales, especially those coming from rural areas with the emergence of the COVID-19 pandemic (Ludwianto, 2021). For instance, offline merchants can swiftly move to online marketplaces using social media compared to other digital platforms.

In this study, we find that within the development of social commerce over the years, experienced and novice merchants turned to social commerce to market their products or services due to three main reasons: (1) ease of setting up; (2) ease of outreach to a wider group of consumers; and (3) opportunity to utilize existing social networks (Paypal, 2019). Social media platforms offer a low barrier to entry for both experienced and novice merchants due to its easy navigation. Compared to traditional e-commerce platforms, which require numerous permits and licenses, signing up to social commerce is easier and needs minimal-to-no requirements. In addition, its usage is also deemed advantageous as the money turnaround is faster than e-commerce, where the payment can take days for the consumer to receive their order (Paxel, 2021).

While e-commerce is still relevant for online shopping, most Indonesian consumers prefer social media to purchase and repurchase goods and services due to their existing relationships with merchants (Pratama et al., 2017; Amelina & Zhu, 2016). As social media is an outlet for personal communication, merchants can easily interact with the consumers using various features such as photos, videos, stories, comment sections, and direct messages. As a result, merchants gained more trustworthiness in the transaction process. Furthermore, if a consumer is satisfied with their purchase, they can further share their opinions on their experiences and recommendations to their social networks (e.g., family and friends) through word of mouth, which makes them act as if they are merchants themselves. However, in response to this finding, Handarkho (2020) noted that those social networks might not greatly influence consumers.

Another factor to consider in the usage of social commerce is the ease of reaching a broader consumer base. In its practice, social commerce can reach its consumers either directly or indirectly. In a direct model, the exchange between consumers and merchants is met without an

⁵See e-commerce data breach cases in Indonesia, e.g.: Tokopedia data breach (Elok Sari, 2020).

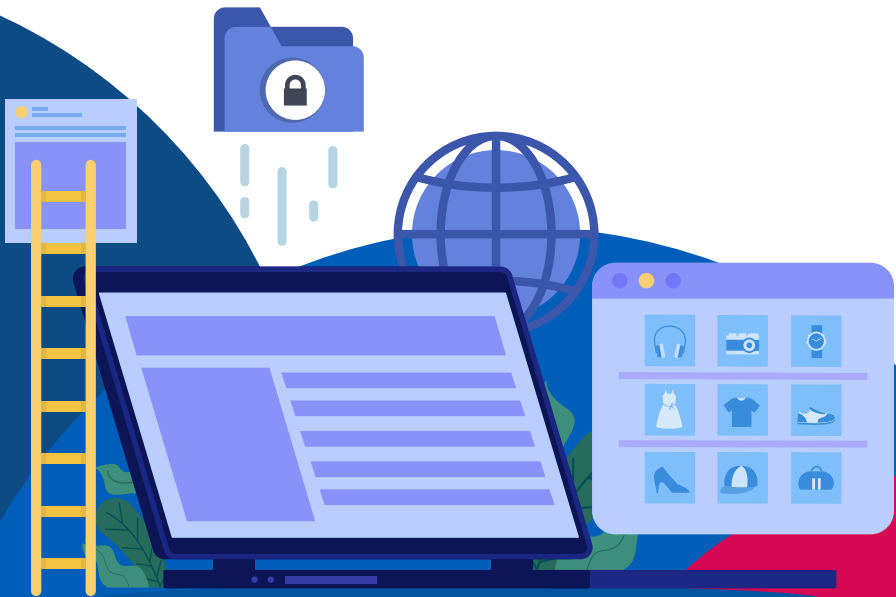
intermediary other than social media. As for the indirect model, it involves an intermediary, such as a reseller community, to bridge the gap between merchants and consumers. When it comes to the latter, merchants can interact with an even wider consumer base as well as more merchants in the online marketplace (SIRCLO, 2020).


However, social commerce also poses challenges that can risk both consumers and merchants relating to consumers' data, return and refund process, and information quality of the products. For instance, with the case of personal data breaches in e-commerce, concerns over consumers' data protection are becoming more prevalent in Indonesia. Moreover, most public social networks such as Facebook also suffer from security problems and social engineering attacks, leading to the misuse of consumers' data (selling consumers' information) and merchant/consumer fraud (Turban et al., 2010).

In the case of product return and purchase, social media's role in the issue between consumers and merchants is relatively vague. While built-in payment features are already implemented (e.g. WeChat) or currently being developed (e.g. WhatsApp) (SIRCLO, 2020), policies and mechanisms on the return and refund process have yet to be acknowledged by most social media platforms (Ahmad & Laroche, 2017). This gap within the jurisdictions of these platforms should be regarded since most consumers are concerned about the merchant's refusal to replace or refund a product or service.

Furthermore, product risk on the information quality of the marketed products and services is another challenge that needs to be addressed. It is the key feature of social commerce in providing up-to-date, accurate, and comprehensive information on products or services, such as purchase experience, product or service recommendations, rating and review, and incomplete purchase history (Meilitanova, 2021; Beyari & Abrareshi, 2016). However, consumers still face challenges such as scams perpetrated by social platforms (Riefa, 201), an ongoing issue relating to social commerce.

Departing from this, studies on social commerce have grown rapidly over the years as digital platforms such as social media are becoming increasingly integral for activities such as online shopping. Despite this, research on this topic, particularly within an Indonesia context, has yet to cover issues relating to the risks of social commerce usage. Thus, this paper focuses on mapping existing regulations of social commerce in Indonesia and the roles of stakeholders in countering abusive business and data practices in its usage.





Analysis of Social Media Platform Liability



➔ Analysis of Social Media Platform Liability

This chapter consists of two sections. The first section will map and examine three legal frameworks relevant to the issue of abusive business and data practices in social commerce: the Consumer Protection, Trade, and Electronic Information and Transaction (EIT). Additionally, the Personal Data Protection Bill (PDP Bill) will also be analyzed to provide a broader picture of Indonesia's politics of law in personal data governance, especially to protect citizens' data from abusive business and data practices. The second section will present an analysis of social media platforms' community guidelines in moderating transactions on their platform.



Mapping and Analysis of Indonesian Laws and Regulations

In the commercial context, abusive business practices may refer to the misrepresentation of goods, misleading or false advertising, or even fraud.² On the other hand, abusive data practices refer to internet fraud, phishing, privacy, and security-related issues, i.e., data misuse, data breaches, unauthorized data access, illegal data modification by third parties, issues related to data owners' lack of control over the processing of data (Marriot, Williams, & Dwivedi, 2017), and cybersecurity breaches which may result in fraud and theft (Deloitte, 2015).

The discussion of both abusive business and data practices correlates to the protection of consumers within the e-commerce context as the electronic means of trade, hence invoking three different legal frameworks on, *inter alia*, consumer protection, trade, as well as electronic and information transactions (EIT). It is notable also to analyze Indonesian regulations concerning personal data protection, as the issue of abusive data practices is highly connected to consumers' data protection. However, as Indonesia currently lacks an established framework governing personal data protection, we can examine the Personal Data Protection Bill, which has been discussed and is being finalized.

²See international practices referring to abusive or unfair business practices, e.g.: United Kingdom Department for Business, Energy & Industrial Strategy. (2018). Misleading and Aggressive Commercial Practices: New Private Rights for Consumers Guidance on the Consumer Protection (Amendment) Regulations 2014; The Law Commission and The Scottish Law Commission. (2012). Consumer Redress for Misleading and Aggressive Practices. The Stationery Office Limited; Commonwealth of Australia. (2016). Avoiding unfair business practices: A guide for businesses and legal practitioners [Australia Consumer Law Guide]. <https://consumer.gov.au/sites/consumer/files/2016/05/0553FT_ACL-guides_UnfairPractices_web.pdf>.

➔ Legal Framework on Consumer Protection

Countering abusive business and data practices in social commerce is an act to protect consumers; therefore, Law No. 8 of 1999 on Consumer Protection (CP Law) applies, which was promulgated to balance consumers' and businesses' interests. Aimed at empowering consumers and providing accessible information, the Law asserts that consumers have the right to safety, the right to be informed, the right to guidance and education, and the right to obtain compensation in transactions. Although not primarily aimed at social commerce, the law establishes the rights and obligations of trading parties, including social commerce.

Under the CP Law, to ensure consumer protection, businesses³ are required to act in good faith, provide accurate information, guarantee the quality of goods and services, as well as provide compensation for goods and services that are not in accordance with the agreement, or if consumers suffer losses from the use of goods and service. On the other hand, consumers' responsibilities revolve around maintaining good faith in transactions, as outlined in Article 5 of the Law.

In tackling abusive business practices in social commerce, the CP Law may address issues regarding the selling of counterfeit products. Article 8, for example, prohibits businesses from producing and selling goods that do not fulfill the existing standards under applicable laws and are not in accordance with the conditions in its description. Article 9 further offers grounds to resolve issues on the incorrect information provision, where businesses are prohibited from conducting false advertising. In addition, information on the price, utility, and condition of goods cannot be altered. Hence, the preceding articles may address the selling of counterfeit products, especially when counterfeit products are advertised as authentic products. Violations of the previous obligations may entail criminal sanctions, such as fine or imprisonment, and additional criminal sanctions.⁴

³Businesses refer to individuals or legal and non-legal business entities established and domiciled or conducting business activities within the Indonesian jurisdiction.

⁴Article 62 of Law No. 8 of 1999 on Consumer Protection.

If businesses fail to compensate consumers who face losses caused by the consumption of goods sold, administrative sanctions may be given.⁵

The CP Law stipulates that the government (or regulators) is responsible for fostering and overseeing the implementation of consumer protection regulations.⁶ Such responsibilities adhere to the OECD's Recommendation on Consumer Protection in E-Commerce.⁷ The Law also provide the establishment of the National Consumer Protection Agency (BKPN) and the Consumer Dispute Settlement Agency (BPSK), as well as the government's recognition of (formally registered) Consumer Associations (LPKSM). Essentially, the BKPN is tasked to foster consumer protection efforts by disseminating consumer protection information, providing recommendations to the government in constructing consumer protection laws, and accepting complaints from citizens, consumer associations, and businesses.

The CP Law provides the role of the government in overseeing the implementation of consumer protection and recognizes the establishment of institutions to oversee consumer protection. However, the Law does not regulate how governments can be held accountable for failure to oversee consumer protection implementation. Another issue that the CP Law does not address is the obligation of social media – the third party in social commerce transactions – to protect consumers in such transactions, even though these consumers are also the consumers of social media platforms.

The problem of applying consumer protection frameworks to business models blurs the boundaries between consumers and businesses like social commerce that exist internationally (OECD, 2016; Riefa, 2020). Numerous countries have addressed how the consumer protection

⁵Article 60 of Law No. 8 of 1999 on Consumer Protection.

⁶See Article 29 of Law No. 8 of 1999 on Consumer Protection. The government is responsible to exert efforts to support the proliferation of healthy relationships between Businesses and consumers, the development of non-governmental consumer protection institutions, and the improvement of human resources in the fields of research and development activities.

⁷The OECD's Recommendation which upholds that governments must increase business and consumers' awareness of applicable consumer protection regulations, is in line with the CP Law's stipulation on the responsibility of governments to foster the implementation of consumer protection.

framework must include the responsibilities of social media platforms (ELSAM, 2021). However, the European Union is still proposing regulations that address the liability of social media platforms (PwC, 2021). Generally, there are three models of liability for social media platforms acting as intermediaries, *inter alia*, the strict liability model, safe harbour model, and broad immunity model (Article 19, 2013; Ahsinin, 2017). First, as implemented in China and Thailand, the strict liability model, directly renders intermediaries liable for contents posted by third parties; hence, social media platforms can be held liable for failure to control trade infringements that they are aware of (Article 19, 2013, Riefa, 2016; Riefa, 2020).

In contrast, the safe harbour model has been adopted by the US and the UK, which grants intermediaries immunity with the condition that they comply with specific requirements stipulated under the laws (Article 19, 2013; Riefa, 2016; Riefa, 2020); requirements may include the direct removal of access to illegal information on social media platforms. Perhaps it is notable to mention that the US shields intermediaries from liabilities to prevent the possibility of overly burdening third parties, which may hamper the development of intermediary services (Riefa, 2016). Similarly, Australia provides digital platform liability recommendations (Flew & Wilding, 2020; Australian Competition & Consumer Commission, 2021), and formally recognizes liability exemptions for information providers and advertisers through the Australian Consumer Law (Commonwealth of Australia, 2016). Conversely, the broad immunity model exempts intermediaries from the requirement of monitoring their content; hence, they have broad immunity from liability to content published by third parties (Article 19, 2013).

To conclude, the CP Law has provided grounds to understand the rights and obligations of consumers and businesses involved in trade activities. Still, it does not specifically regulate the rights and obligations of social media platforms as the third party or intermediary within social commerce. Despite having regulated concerns regarding the abusive business practices that may happen within trade activities, the Law does not regulate matters pertaining to protecting consumers from abusive data practices.

→ Legal Framework on Trade

As social commerce refers to the act of trade via social media, abusive business and data practice in social commerce is governed by the Legal Framework on Trade. Despite the term 'social commerce' not specifically employed in Law No. 7 of 2014 on Trade (Trade Law) and Government Regulation No. 80 of 2019 on Trade through Electronic Systems (GR 80/2019), the regulations coined the term e-commerce as transactions carried out through electronic devices and procedures;⁸ it may, therefore, be concluded that social commerce falls within the definition of e-commerce (Huang & Benyoucef, 2013). According to the laws mentioned above, parties involved in trading in an E-Commerce setting must ensure the fulfillment of the principles of good faith, cautiousness, transparency, trust, accountability, balance, and fairness.

GR 80/2019 recognizes several parties involved in e-commerce and social commerce. Under Article 1(6) of the regulation, businesses through Electronic Systems include individuals or companies in the form of a legal or non-legal entity conducting trade activities. As social commerce involves individuals and companies that are not in charge of the operation of social media platforms, the regulation provides under Article 1(10) that merchants include businesses operating via social media platforms provided by other companies, e.g. Instagram and Facebook. The Law also recognizes businesses providing electronic communication facilities utilized for trade transactions as Electronic Systems Trade Operators (PPMSE) and intermediary services operators which provide electronic communication facilities in the form of search engines, hosting, and caching, as regulated under Articles 1(11) and 1(12), respectively. The former addresses the role of social media platforms as the medium in which transactions occur, starting from the sale and ending with the purchase of goods, whilst the latter addresses the role of social media platforms as a bridge between consumers and merchants.

⁸Article 1(2) of Government Regulation No. 80 of 2019 on Trade through the Electronic System (GR 80/2019).

To address the issue of abusive business practices, the Legal Framework on Trade obligates businesses to provide clear and honest information to consumers⁹ and act according to applicable consumer protection frameworks.¹⁰ Under the framework, offers in e-commerce platforms must, at the very least, provide information regarding the identity and legality of businesses, specification and requirements of goods, conformity and propriety of goods, price and method of payment, method of delivery of goods, risks and conditions, and limitation of liability in the case where risks occur.¹¹ As such, consumers will be protected against abusive business practices such as misleading advertisements. Failure to comply with such obligations may result in administrative sanctions ranging from a written warning, the inclusion of the business in the priority list of supervision, blacklisting, and business license revocation.¹²

GR 80/2019 also provides the baseline to tackle abusive data practices in the context of e-commerce, as governed by Articles 58 and 59 on personal data protection (PDP). Essentially, businesses are obligated to retain personal data according to applicable PDP standards or current business customs, and fulfill data protection principles, i.e. lawfulness, purpose limitation, data minimization, accuracy, storage limitation, and confidentiality.¹³ These principles are recognized internationally.¹⁴ The regulation grants data owners the right to request businesses to remove their personal data if they cease utilizing services provided by e-commerce platforms. However, in social commerce, ensuring the erasure of the owner's personal data may be more challenging.

In addressing the issue of holding social media platforms accountable, Article 17 of GR 80/2019 has provided that PPMSEs and intermediary services are responsible for the following obligations:

⁹See Article 65 of Law No. 7 of 2014 on Trade and Article 13 of GR 80/2019, which obligates information to be provided accurately and honestly.

¹⁰Article 26 of GR 80/2019.

¹¹See Article 65 of Law No. 7 of 2014 on Trade and Articles 13 and 39 of GR 80/2019.

¹²See Article 65(6) of Law No. 7 of 2014 on Trade and Article 80 GR 80/2019.

¹³See Article 59(2) of GR 80/2019, which lays out personal data standards.

¹⁴See for example, Chapter 2 of the European Union's General Data Protection Regulation and Paragraph 6 of the ASEAN Framework on Personal Data Protection.

- To oversee merchants' compliance with Indonesian regulations. PPMSEs, including social media platforms, are prohibited from accepting merchants who do not fulfill prevailing regulations. Failure to comply with this obligation may entail the imposition of administrative sanctions provided by Article 80. In theory, this provision may hold PPMSEs or social media platforms liable for failing to oversee the merchants it allows to operate on its platform. Regardless, not all sellers in social commerce are registered as merchants.
- To eliminate illegal information. GR 80/2019 highlights the importance of information accuracy by providing that PPMSEs and intermediary services can be held liable for legal consequences arising from the existence of illegal information in e-commerce unless they immediately remove such information.¹⁵ Intermediaries are exempted from the clause if they only host, cache, or are functioning as a search engine, and are a mere conduit. The status of mere conduit has been invoked in the European Committee's E-Commerce Directive, where it refers to platforms that do not (a) initiate information transmission, (b) select the transmission receiver, nor (c) select or modify information in the transmission (European Parliament and European Council, 2000). Although this provision adds the responsibility of PPMSEs or social media platforms to ensure the elimination of illegal information, the regulation fails to clarify what constitutes illegal information. If illegal information refers to the Legal Framework on Electronic Information and Transaction, it is any information that causes disturbance to the public order and society,¹⁶ which is vague in pinpointing what constitutes illegal information.

¹⁵ See Article 22(1) of GR 80/2019.

¹⁶ Article 9(4) Minister of Communication and Informatics Regulation No. 5 of 2020 on Electronic System Provider in Private Sector (MCI Regulation 5/2020).

● To ensure the compliance of advertisements to prevailing regulations. As regulated by Article 33 of GR 80/2019, PPMSEs must ensure that electronic advertisements comply with prevailing laws regulating broadcasting, fair business competition principles, PDP, and consumer protection. Thus, advertisements must not include misrepresentation nor false information, which are some of the integral elements of abusive business practices.

Such responsibilities reflect the role of PPMSEs in ensuring that merchants within its platform are acting in accordance with the applicable Indonesian regulations and are not committing actions that may be considered abusive business practices. While it may be less complex to oversee accounts that have registered themselves as merchants in social commerce, PPMSEs may find it harder to oversee accounts that do not register themselves as merchants.

The implementation of the Legal Framework on Trade is overseen by the government, where Article 93 of the Trade Law states that the government is responsible for enacting trade regulations, national standards, and procedures, prescribing trade licensing systems, and creating a conducive business environment. Similarly, Article 76 of GR 80/2019 specifies that the Ministry must guide and oversee matters pertaining to e-commerce. Despite the previous obligations, there are no provisions that addresses the obligation of the government to provide transparency in overseeing E-Commerce activities or enact sufficient laws to protect the society.



→ Legal Framework on Electronic Information and Transaction (EIT)

Law No. 11 of 2008 jo. Law No. 19 of 2016 on Electronic Information and Transactions (EIT Law) is notoriously known to govern activities in cyberspace, including e-commerce, and has been explicitly mentioned in the General Elucidation of the EIT Law.¹⁷ Although the Legal Framework on EIT does not expressly mention the term 'social commerce', previously elaborated definitions and analyses of laws infer that social commerce is essentially part of e-commerce (see also Huang & Benyoucef, 2013). Consequently, the implementation of social commerce must adhere to the Legal Framework on EIT. From the framework's perspective, all electronic media used in commerce activities (including marketplace and social media) are considered Electronic Systems (ES).¹⁸ Thus, Electronic System Operators (PSE) should comply with all obligations stipulated in the Legal Framework on EIT. The EIT Law specifies various actors that constitute PSE, including State Institutions, Business Entities, and society.¹⁹

In this context, marketplace and social media platforms constitute a Business Entity (*Badan Usaha*), which is essentially part of the private sector PSE.²⁰ It is further emphasized in Minister of Communication and Informatics Regulation No. 5 of 2020 on Electronic System Provider in Private Sector (MCI Regulation 5/2020), which was explicitly intended to regulate social media platforms (Rodriguez, 2021; Human Rights Watch, 2021). Considering the importance of social media platforms in social

¹⁷The General Elucidation states that broader issues on the impact of technological development emerge in the private sphere, as electronic transactions for trade activities in ES (electronic commerce) 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 (EIT)

¹⁸The 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(5) of Law No. 11 of 2008 on EIT. The MCI Regulation 5/2020 also defines specific Private Sector PSE, which is User Generated Content (UGC) Private Sector PSE. See Article 1(7) of MCI 5/2020.

¹⁹See Article 1(6) of Law No. 11 of 2008 on EIT. 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(35) of GR 71/2019). In the society category, it also covers institutions formed by society (e.g., civil society organizations, consumers association) (See e.g., Article 41 of Law No. 11 of 2008 on EIT).

²⁰Business Entity is defined as a sole proprietorship or partnership of both legal entity and non-legal entity. See Article 1(22) Law No. 11 of 2008 on EIT.

media platforms in social commerce to facilitate interactions amongst sellers and consumers (see, e.g. Algharabat & Rana, 2020), how platforms, as private sector PSE, operate the ES is crucial in minimizing abusive business and data practices in social commerce.

The Legal Framework on EIT contains at least three key provisions for countering abusive business and data practices:

● Provisions regarding PSE's obligations

In general, PSE is obliged to ensure the proper operation, reliability, and security of ES.²¹ Moreover, PSEs must comply with the minimum requirements, including: retention period; protection of availability, entirety, authenticity, confidentiality, and accessibility of electronic information; understandable procedures and guidelines; and a sustainable mechanism to maintain and update the clarity, and accountability of the procedures and guidelines.²² These requirements can serve as both preventive measures and grounds to hold PSEs accountable, for example, in the event of a data breach.²³

However, as social commerce can be conducted directly²⁴ through social media platforms or indirectly through third parties²⁵ (SIRCLO and Ravenry, 2020), in most cases, the burden to prevent abusive business and data practices falls on users instead of the PSE. It can be distinguished by the types of electronic transactions in the private sector, which include Business-to-Business (B2B), Business-to-Consumer (B2C), and

²¹See e.g., Article 15 of Law No. 11 of 2008 on EIT; Article 3 of GR 71/2019; and Article 9 and Article 10 of MCI Regulation 5/2020.

²²See e.g., Article 16 of Law No. 11 of 2008 on EIT; Article 4 of GR 71/2019; and Articles 9 and 10 of MCI Regulation 5/2020.

²³Non-compliance with the general obligations and minimum requirements in operating ES is grounds for the administrative sanction imposed by the Government to PSE (See, e.g., Article 100 of GR 71/2019).

²⁴For instance, through built-in messaging or comment features of social media platforms.

²⁵For instance, interaction through resellers that bridges transactions between sellers and customers.

Consumer-to-Consumer (C2C)/Person-to-Person (P2P).²⁶ Hence, social media platforms have the role of educating consumers, such as providing understandable community guidelines or related information to their users when utilizing the platform.

Moreover, GR 71/2019 stipulates that businesses (e.g., the seller) in social commerce must inform consumers about products offered, and advertisements with valid and complete information.²⁷ The obligation for PSE to provide reporting mechanisms and complaints settlement services that the public can access²⁸ is essential for oversight over abusive business and data practices on their platforms, especially those conducted by users. Additionally, based on the Legal Framework on EIT, the State (cq. the Government) only acts as the supervisor for the implementation of EIT.²⁹

Provisions related to PDP.

Although similar to the general obligations above, the PDP-related provisions are mainly directed at PSEs as the organizations processing personal data,³⁰ which in this case are social media platforms. The EIT Law emphasizes the importance of users' consent in the data processing. In data protection law, consent is the pivotal means of collecting and processing personal data (e.g. OECD, 2013; Trakman, Walters, & Zeller, 2020). Without consent, access or utilization of personal data is deemed unlawful. In line with this idea, the EIT Law states that

²⁶See Article 41 paragraph (3) of GR 71/2019. These types of interactions can be applied in social commerce, as sellers and buyers are essentially social media users.

²⁷See Article 48 of GR 71/2019.

²⁸See e.g. Article 10 of MCI Regulation 5/2020

²⁹See Article 40 of Law No. 19 of 2016 on Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (Amendment of EIT Law).

³⁰However, we are aware that there is also the possibility of misuse of personal data by users.

data processing should be based on the consent of data subjects unless otherwise specified by laws and regulations.³¹

The EIT Law only governs the need for consent in data processing. Hence, GR 71/2019 provides more detailed provisions on data protection,³² where PSEs must enact PDP principles, i.e. lawfulness, purpose limitation, data minimization, accuracy, the guarantee of data subject's rights, and completeness,³³ which are similar to PDP principles in the EU GDPR. Aside from the data subject's consent in processing personal data, at least one of the following legal grounds must be fulfilled: contractual obligation; legal obligation; vital interest; legitimate interest; public interest; and/or other interests.³⁵ Furthermore, MCI Regulation 5/2020 requires private sector PSEs to protect personal data, especially those processed by private sector PSEs.³⁶

Moreover, privacy policies, which refer to a notice disclosing how social media platforms process users' data, are vital in ensuring compliance with PDP-related provisions stipulated in laws and regulations. Privacy policies are also critical in addressing users' concerns about risks such as the misuse of personal data. As most privacy policies are perceived as lengthy and difficult to understand, it might be difficult for social media platforms to ensure that the privacy policy is readable and easily understandable (Chua et al., 2017). Nevertheless, adherence to the PDP principles above is essential to at least ensure that users' data is not misused.

³¹ See Article 26(1) of Law No. 19 of 2016 on Amendment of EIT Law.

³² Indonesia also has Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection on Electronic System. Considering the substantial similarities, it is preferable to refer to GR 71/2019 in PDP in addressing main issues in PDP, such as definition and principles on data processing.

³³ Article 14(1) of GR 71/2019.

³⁴ Data processing principles in EU GDPR covers lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability (See Article 5 EU GDPR).

³⁵ See Articles 14(3) and 14(4) of GR 71/2019.

³⁶ See e.g., Articles 3(3)(c), 22(2)(d), 30(3)(c), and 40(3)(c) of MCI 5/2020.

Provisions related to sanctions.

According to EIT Law, GR 71/2019, and MCI Regulation 5/2020, PSEs can be imposed by administrative sanctions for non-compliance with obligations stipulated in the previously discussed regulations. The administrative sanctions range from a written warning, administrative fines, temporary suspension, access blocking, and/or removal from PSE registration.³⁷ Moreover, individuals can also face criminal sanctions if they spread false and misleading information that results in consumers' loss or if they intentionally and unrightfully alter, add, reduce, transmit, destroy, remove, transfer, or hide electronic information and electronic documents which belongs to other persons or public property.³⁸

In the context of PDP-related provisions' infringements, prevailing mechanisms set out in GR 71/2019, and MCI Regulation 5/2020 are administrative sanctions. However, there is no guidance on the number of administrative fines imposed in cases of PDP infringements by PSE; it is contingent upon the Ministry of Communication and Informatics, which is the institution that imposes administrative fines according to GR 71/2019 and MCI Regulation 5/2020. Apart from administrative sanctions, the EIT Law also provides another mechanism specifically aimed at infringements of consent in data processing, which is through a civil lawsuit.³⁹ Thus, individuals (users) can file a lawsuit against PSE under this ground.

Based on the explanation above, several Articles can be used as legal bases for the implementation of social commerce, such

³⁷ Article 100 of GR 71/2019. Specific administrative sanctions in the context of private sector PSE can be seen in MCI Regulation 5/2020. The types of administrative sanctions are mostly the same as GR 71/2019, however, MCI Regulation 5/2020 specifies the types of administrative sanctions based on the violations (See e.g., Articles 7(2), 7(3), 8(2), 15(10), 16(11), and 45(4) of MCI 5/2020).

³⁸ See Articles 28(1) and 32 of Law No. 11 of 2008 on EIT.

³⁹ See Article 26(2) of Law No. 19 of 2016 on Amendment Amendment of EIT Law.

as regarding the seller's obligation to provide valid and complete information regarding the products offered, availability of facilities and services and settlement of complaints. Moreover, it is also worth noting that the Legal Framework on EIT focuses on regulating the utilization of technology and content moderation in general rather than the substantial social commerce-related issues. Therefore, apart from the Legal Framework on EIT, addressing substantial social commerce issues should also refer to the Legal Framework on Consumer Protection and Trade, as explained in the previous section.

Furthermore, the formulation of criminal and administrative sanctions depicts a top-down relationship between the State and social media platforms. Hence, applicable laws and regulations in the Legal Framework on EIT reflect an imbalanced relationship between the Government as regulators and PSEs, especially private sector PSEs. Thus, the society (e.g. CSO, consumers association, and academic institutions) has a vital role in overseeing regulators to ensure that they do not abuse their power in supervising private sector PSEs, which could potentially infringe on consumers' rights in electronic transaction activities.



→ Personal Data Protection Bill

As the usage of social commerce obligates consumers to disclose their data, consumers are prone to abusive data practices which may take place during the collection or the processing of data that has been collected or supplied (OECD, 2010). Hence, it is crucial for the government to regulate PDP standards to ensure that social media platforms and businesses do not conduct abusive data practices. However, Indonesia does not have a comprehensive Law regulating PDP, as these regulations are scattered in numerous regulations such as the EIT Law, GR 71/2019, MCI Regulation 5/2020, and MCI Regulation 2/2016. Acknowledging the necessity to address data protection issues and to support e-commerce activities (Agustini, 2020), the Indonesian Personal Data Protection Bill (PDP Bill) has been discussed and is being finalized.

Several parties mentioned in the PDP Bill include data controllers, data processors, data owners, and data protection officers (PwC, 2020), which are terminologies that have also been employed in the EU GDPR. According to the PDP Bill, data controllers are responsible for: ensuring the security and confidentiality of data⁴⁰; informing sufficient information to data owners in obtaining consent; ensuring the fulfillment of the principle of purpose limitation⁴²; and ensuring the fulfillment of data subjects' rights.⁴³ Predominantly, these rights are also recognized in numerous data protection frameworks. On the other hand, the PDP Bill provides that data processors are obligated to conduct data processing upon being appointed by data controllers, consequently obliging them to adhere to the instructions of data controllers.⁴⁴

⁴⁰ See Articles 27, 29 and 30 of the PDP Bill, where data controllers must ensure the protection of personal data from illegal access and illegal data processing.

⁴¹ See Article 24 of the PDP Bill, data controllers are obligated to inform data owners of the legality and purpose of data processing, relevance of data subject to data processing, retention period, period of data processing, and data owners' rights.

⁴² See Article 36 of the PDP Bill.

⁴³ See Articles 26, 31, 32, 34, 35, 37, and 38 of the PDP Bill which reflects data subjects' rights.

⁴⁴ See Article 43 of the PDP Bill and the Article's elucidation, data controllers may appoint data processors. Data processors violating data controllers' instructions no longer becomes data processors but data controllers.

Generally, the PDP Bill provides PDP protection towards data subjects, where data subjects' rights are granted to data owners. Among others, the following are rights regulated within the PDP Bill: the right to information; the right to rectification; the right of access; the right to withdraw consent; the right to object; the right to restrict processing; and the right to compensation in the case of PDP violation.⁴⁵ These rights align with some of the existing data protection frameworks, *inter alia*, the EU GDPR, the ASEAN PDP Framework, the Singapore Personal Data Protection Act 2012, and existing consumer protection frameworks such as the California Consumer Privacy Act 2018 (OECD, 2020).

Aside from the rights of data subjects and the obligations of data controllers above, Article 18 mandates that data processing must be conducted under the explicit content of data subjects. However, other legal grounds may justify the act of data processing without the explicit consent of data subjects, spanning from the performance of contracts, legal obligations, vital interests, public interests, and legitimate interests.⁴⁶ Furthermore, the bill regulates that data subjects may revoke its consent. Once again, these legal grounds align with the legal grounds recognized by the EU and UK GDPR, where similar provisions have been incorporated in respective frameworks. It is notable to understand that this is a shift from the Legal Framework on EIT, where consent is not an alternative legal ground that is treated similarly to other legal grounds justifying data processing.

Despite the PDP Bill requiring explicit consent to be obtained prior to data processing, no provision has been enacted to address the issue of data profiling or mining nor the usage of cookies. The PDP Bill has only incorporated the terms 'profiling' and 'automatic' once in Article 10, where the article allows data subjects to appeal to decisions taken by data processors if such processing is automated based on data profiling. As such

⁴⁵ See Articles 4-13 of the PDP Bill, which highlights the rights of data subjects.

⁴⁶ See Article 18(2) of the PDP Bill, consent is not necessary if other legal grounds can be fulfilled.

the bill has not specifically addressed the issue on automated decision-making (ADM) including profiling and cookies, which remains a critical privacy concern that may constitute abusive business practice (Pandit & Lewis, 2018). In contrast to the GDPR, the regulation explicitly obliges data controllers to provide data subjects information regarding the existence of ADM including profiling, the logic involved, and the consequences of such processing to data subjects.⁴⁷ Accordingly, the PDP Bill can be further developed to accommodate the need to address the issue of ADM including data profiling.

Under the PDP Bill, similar to the previous frameworks, the government is responsible for overseeing PDP implementation.⁴⁸ The government may also impose administrative and criminal sanctions on the violation of the PDP Bill.⁴⁹ Yet, the Bill does not provide any sanctions that can be imposed on the government for failing to fulfill its obligations.

Thus far, the rights of data subjects, the obligations of data controllers and processors, and the recognition of consent and alternative legal grounds provide more legal certainty, which is beneficial in combating abusive data practices during the collection and processing of data. There are several concerns to be considered. **First**, whether issues on consent in data processing will increase with the shift from consent as a requirement to consent as an alternative legal ground. **Second**, legal certainty on ADM including consent to ADM to prevent abusive data practices. **Finally**, whether the oversight of PDP compliance can be conducted effectively despite how blurry social commerce is, especially with the possibility that Businesses are not registered as merchants in social commerce.

⁴⁷See Articles 13(2)(f) and 22 of the GDPR, a specific article regulates matters pertaining to automated individual decision-making including profiling, and ADM must be informed to data subjects.

⁴⁸See Chapter XII on the Role of the Government and Society.

⁴⁹See Chapter VII on Administrative Sanctions and Chapter XIII on Criminal Provisions.

➔ Summary of Indonesian Legal Frameworks Analysis

Based on the analysis of relevant legal frameworks related to abusive business and data practices in social commerce, it can be concluded that, in general, many scattered laws and regulations analyzed have many provisions that can be applied in countering abusive business and data practices. In regards to countering abusive business practices, emphasis has been given to the protection of consumers. Specifically for the prevention of abusive data practices, some of the legal frameworks have incorporated personal data protection principles that must be adhered by social media platforms. In tackling both abusive business and data practices, the legal frameworks above have regulated sanctions that can be given to parties committing such abusive practices as well as the obligation of the government to oversee matters pertaining to social commerce; this depicts a top-down relationship between the government and social media platforms. A summary of the analysis is provided in the following table.

Table 1. Summary of Indonesian Legal Frameworks related to Abusive Business and Data Practices in Social Commerce

	Issues Covered	Issues Not Covered
Legal Framework on Consumer Protection	<ul style="list-style-type: none"> ● Consumer protection ● Obligations and rights of businesses and consumers ● Prohibition of incorrect information provision ● Prohibition of the selling of counterfeit products ● Criminal and administrative sanctions ● Government's role in oversight 	<ul style="list-style-type: none"> ● Transparency in government's role in oversight ● Obligations of social media as third parties or intermediaries ● Prohibition of abusive data practices ● Consumer protection in the event of abusive data practices

	Issues Covered	Issues Not Covered
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 ● Prohibition of incorrect information provision and false advertising ● Prohibition of the selling of counterfeit products ● Prohibition of abusive data practices through PDP principles ● Criminal and administrative sanctions ● Government's role in oversight 	<ul style="list-style-type: none"> ● Transparency in government's role in oversight ● Elucidation of "illegal information" that should be eradicated by intermediaries
Legal Framework on EIT	<ul style="list-style-type: none"> ● E-Commerce ● Obligations and rights of PSEs and business entities ● Prohibition of incorrect information provision ● 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 	<ul style="list-style-type: none"> ● Transparency in government's role in oversight

	Issues Covered	Issues Not Covered
Legal Framework on EIT	<ul style="list-style-type: none"> ● Content moderation ● Criminal and administrative sanctions and the possibility of the civil lawsuit ● Government's role in oversight 	<ul style="list-style-type: none"> ● Transparency in government's role in oversight
Personal Data Protection Bill	<ul style="list-style-type: none"> ● Obligations and rights of data controllers, data processors, 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 ● Government's role in oversight 	<ul style="list-style-type: none"> ● Transparency in government's role in oversight ● Data subject's consent to automated decision-making and data profiling

Source: Processed by Author, 2022.





Analysis on Social Media Platforms' Community Guidelines

In the era where social media became a daily diet for most people, trade practices are now shifting into the virtual world. Brands no longer built their giant store in most cities and handed out physical flyers to show their presence. Instead, brands are spending most of their marketing budgets in the form of online advertisement, most importantly through social media. The credibility of the brands now depends highly on their online presence because it has the potential to manufacture trust among potential customers. The one with top celebrities to back it has the most followers, and engaging content usually wins the race.

The ease of doing trade using social media not only simplifies the business process for sellers. It also gives convenience to buyers to buy their needs from their phones. But sadly, this also creates an opportunity for a new method of scam, fraud, or other abuse, especially among users who lack digital literacy.

Unlike the marketplace or e-commerce, trade within social media platform, especially Facebook, Instagram, or Line, is a direct transaction from consumer to seller and not guaranteed by a third party. As a result,

everyone can easily sell a product and make fake or overpromising to lure potential buyers, which might not reflect the actual condition of the product or service they are selling.

One of the most common scamming practices is "Black Market Phone" in which sellers post a smartphone with below-average prices.⁵⁰ Consumers who are not careful will quickly become fascinated into this marketing, transfer the fund to the seller without hesitation, and fall into the trap. Unfortunately, the phone they paid for never came, and the scammer got away with it. This phony method might look "too good to be true", but many people still fell for it in reality.

Another example of abusive activity on the social media marketplace is overpromising claims and misleading advertising. The most common practices are beauty products or medicines that claim that their product is recommended by doctors and even used by celebrities. Consumers who lack factual information regarding their products and their condition are prone to fall for the over-simplistic information provided by the sellers. Therefore, cases of side effects and other product malfunction-related issues have surged drastically. Sadly, the consumer can not get any repercussions from the seller. In fact, they are also at risk if posting their bad impression with the product through social media.⁵¹

The platform actually has some community guidelines that prevent such things from happening again. However, the implementation is insufficient, and some loopholes make it easy for the seller to continue their fraudulent activity.

⁵⁰Hendri, Seni. (2022, January 9). Awasi! Penipu Incar Pengguna Facebook, Modus Promosi HP Murah, Sejumlah Warga Aceh Timur Jadi Korban. Aceh Tribun News. < <https://aceh.tribunnews.com/2022/01/09/awasi-penipu-incar-pengguna-facebook-modus-promosi-hp-murah-sejumlah-warga-aceh-timur-jadi-korban>>

⁵¹Hidayat, Ferry. (2021, October 23). Konsumen Terancam Penjara Usai Perawatan di Klinik Kecantikan L'Viors Surabaya, SAFENet Bilang ini. Warta Ekonomi. < <https://wartaekonomi.co.id/read369334/konsumen-terancam-penjara-usai-perawatan-di-klinik-kecantikan-lvior-surabaya-safenet-bilang-ini>>

→ How Platforms Protect Consumers and Businesses

Regarding fraudulent businesses running freely on social media, the platform itself has already put community guidelines as protection for buyers and sellers. Nevertheless, there's still a lack of control on the implementation and loopholes on the policy that makes the fraud and abuse practices still going.

The current community guideline are lengthy and not easily understandable for the consumers as well as the sellers. It simply covers clauses regarding violence, abuse, and criminal activity. While the implementation simply exists for user agreement/consent without explicit undertaking. Current guidelines lack the strict provision of transaction protection and verification process, making it for repeatable fraudulent activities. Moreover, the creative marketing campaign often impairs the user/consumers' judgment due to their level of digital literacy. The consumer needs to understand the importance of user credibility, which can be found from the seller's history or customer impression of their product.

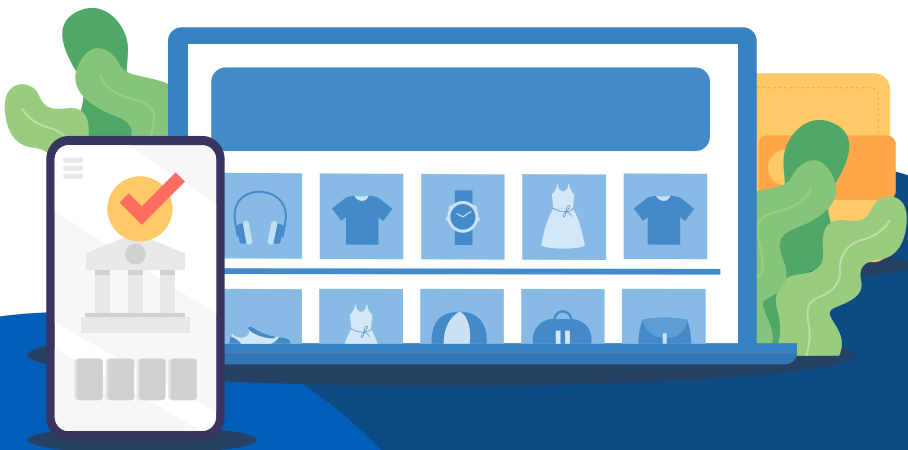
→ Comparing the Implementation of Community Guidelines in Social Media vs E-Commerce Platforms

The emergence of e-commerce and marketplace platforms with sophisticated user experience has driven a higher trading activity between business to consumer and consumer to consumer. What differentiates these platforms from social media is that marketplace and e-commerce platforms have a strict verification process involving phone numbers, national ID, and bank book verification. In addition, trade activities involving these platforms also utilize an escrow account to hold the buyer's money during the transaction process. On the other hand, the seller will receive the funds after the transaction is completed to fulfill both parties and get a fair trading experience.

Many of the mentioned platforms lack these processes and may look into Carousell community guidelines. Carousell is (mainly) a consumer-to-consumer marketplace platform similar to the social media platforms marketplace. The difference between Carousell and others is that the platform offers a rating system and testimonials for every buyer and seller. That way, users are already informed of the fact and previous history of the sellers or buyers. Carousell also involves phone number verification and a strict ban policy for any fraud activities. That way, people can only have 1 Carousell ID for their phone number.

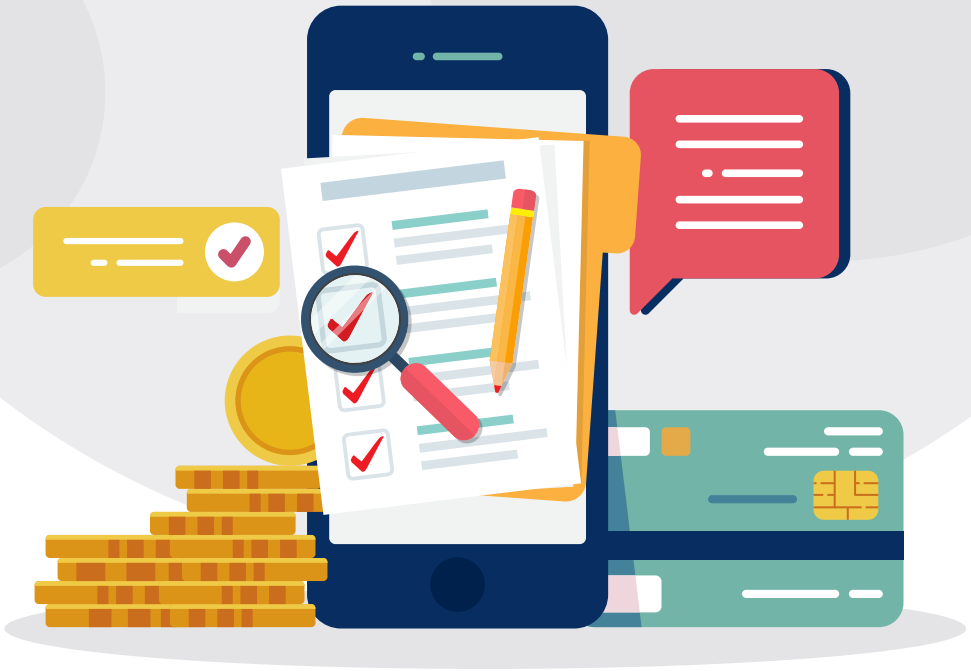
The testimonial features, ratings, and single phone number policy on Carousell make it hard for "new scammer" to lure any potential buyers. The community guidelines also make people who have good testimonials think twice to make any fraudulent activities since they are bound to the rating system and would risk losing the good reputation that they've built.

The policy and the moderation system from Carousell, perhaps, is the thing that needed to be implemented in the social media platform trade transaction, be it in the marketplace (for business) or personal account.





Analysis of Consumer Risks in Social Commerce Transactions in Indonesia



→ Analysis of Consumer Risks in Social Commerce Transactions in Indonesia

Risks and Challenges of Social Commerce Practice in Indonesia

In the attempt of mapping out risk in the utilization of social commerce, this section would highlight at least three types of risks deriving from the work of Farivar, Turel, and Yuan (2017), which are:

→ Product Risk

1. Products and or goods received by buyers are different with the description of the product that is stated in the site. This can encompass several aspects, which are: quality loss, quantity loss, and actual fraud.

- Quality loss occurs when products received by buyers are of lower quality from what have been advertised. An example of a quality loss is when a product is advertised as being an original one, but consumers receive a knockoff product. The case of knockoff shoes that are sold through Instagram and claimed to be of original ones have occurred frequently (Iskandar, 2020). In such a situation, sellers can also ignore customers' complaints or simply block unsatisfied customers' accounts from posting their dissatisfaction in the account.
- Quantity loss occurs when consumers receive less products or incomplete products from what have been advertised.
- Fraud occurs when consumers receive an entirely different product from what has been advertised by the seller. An example of fraudulent acts occurred in Yogyakarta in 2021 where a consumer only received a mobile phone case instead of a mobile phone from a transaction that she did through e-commerce (Indozone, 2021).

2. Distribution of foods and drugs that are illegal, already expired, or do not yet have distribution permits. This case has been very rampant especially during the COVID-19 pandemic where ordering food through e-commerce and social commerce have become more common, especially since the government applied the emergency public activity restrictions (*Pemberlakuan Pembatasan Kegiatan Masyarakat-PPKM*). In 2020, The Food and Drug Monitoring Agency (BPOM) reported that in the period of

1 January 2020 to 30 April 2020 only, the government have taken down at least 700 websites and seller accounts that sells food that are either illegal, expired, or do not yet have distribution permit (*Tanpa Izin Edar-TIE*) (Sulistiyawati, 2020).

→ Financial Risk

Financial risk is defined as the loss of financial assets or money. This occurs when consumers do not receive anything despite having paid for the products or goods (loss of money). There was a viral case of an actress, Fairuz Rafiq in June 2021, where she bought a preloved luxury bag on Instagram and had her account blocked after she transferred the money to the seller. She was unable to contact the seller after the transaction had occurred (Hadiansyah, 2021). Realizing that she has been scammed by the seller, Fairuz stated that she has reported the case to the related authorities—the police. However, to date, there has not been any sufficient information on how this incident is being resolved by related stakeholders. This case drew good attention from the public, due to the significance of a relatively knowledgeable public figure that is still caught in this situation. Consumers that have less knowledge as well and are less affluent may suffer greater loss if such situations occurred to them. Such motives—preloved goods, fake testimonies, and fake followers—have often caused consumers and/or would-be consumers to be more prone against these fraudulent activities. Unfortunately, to date, there has not been any detailed data on the number of cases of financial risks in social commerce in Indonesia.

→ Privacy Risk

Deriving from Sun, Fang, and Hwang (2019), privacy breach is considered as a major problem in the development of social commerce. This is especially related to the collection of user interaction and activities

online that are utilized by social commerce to produce personalized advertisements and offers. Despite being promoted as a helpful feature in maximizing user's personal experience by offering goods and advertisements that suit users' likes and interactions, it is also helpful to identify several drawbacks and risks that potentially might arise. Fourberg et.al. (2021) have mapped out several potential privacy risks in the digital advertising, which encompasses several raising concerns such as:

- Potentials of data being shared across third parties without consent and knowledge from data owners has raised privacy concerns
- Location based and/or interest-based advertising targeting may also limiting customers' choices
- *Dark pattern elements*- exploitation of consumers' behavioral biases that might lead them into behaving in a specific way that is contrary to their own preferences

Risks in Numbers: Identifying Cases and Complaints

In Indonesia, reports on consumer complaints are not yet centralized. We gathered data and interviewed three national stakeholders (The National Consumer Protection Agency–BPKN, The Indonesian Consumers Foundation–YLKI, and The Indonesian Directorate General of Consumer Protection and Trade Compliance) and one stakeholder at the provincial level (Yogyakarta Consumers Foundation–LKY) to understand the different types of risks and challenges that consumers have and may face in the utilization of social commerce.

The National Consumer Protection Agency (BPKN)

Indonesia National Consumer Protection Agency (BPKN) was first established under Law No. 8 Year 1999 on Consumer Protection. BPKN members encompasses several key actors in consumer protection, that are: academics, governments, experts, and the Consumer Associations (LPKSM). In 2021, BPKN stated that they have received 3256 consumer complaints; mostly coming from the housing, financial services and e-commerce sector.

The Indonesian Consumers Foundation (YLKI)

Established in 1973, YLKI is a non-government and non-profit organization with the objectives to increase consumer awareness on their rights and responsibilities. Once consumers have a better understanding and knowledge on their rights and responsibilities, it is expected that they will be able to protect themselves (against fraudulent acts, etc) and also their environment.

In 2021, most complaints received by YLKI concerned transactions in e-commerce, namely for cases of non-delivery, redress, goods received not as advertised/described, and account breaches. No specific data on social commerce was collected, but YLKI mentioned that there are also some reports of data misuse



The Indonesian Directorate General of Consumer Protection and Trade Compliance (PKTN) under the Ministry of Trade

The Director General of Consumer Protection and Trade Compliance stated that in 2021, the office recorded 9,393 consumer complaints. This number has multiplied by 10 times in comparison to the previous year which only recorded 931 customer complaints. This situation might be influenced by the current pandemic situation where people are doing more online transactions than the previous years. In response to this situation, Kemendag is in the position to encourage the public to use an already established e-commerce (marketplace) instead of social commerce to ensure its safety and security, supported with the availability of a complaint mechanism that is integrated within the platform. In response to incoming complaints and reports from consumers, PKTN is also actively helping in resolving the issue, especially if the seller has been legally registered as a business entity and also has an offline shop. Things will become more complicated if there is not enough information on the offline shop, as the case will be better handled by the police.

In 2021, the Ministry of Trade's Directorate General of Consumer Protection and Trade Compliance has received a total of 8949 E-Commerce-related reports, where these reports may include transactions that occur within the social commerce context; there are no parameters differentiating social or E-Commerce reports.⁵² Furthermore, these reports are only reports which fall under the field of the Legal Framework of Consumer Protection, hence other reports that do not fall under the purview of Consumer Protection can be reported to other agencies such as other ministries or the police.⁵³

⁵²Interview with Directorate General of Consumer Protection and Trade Compliance, Ministry of Trade of the Republic of Indonesia.

⁵³Interview with Directorate General of Consumer Protection and Trade Compliance, Ministry of Trade of the Republic of Indonesia. See also Donny B.U. and Indriyatno Banyumurti, *Keamanan Siber untuk E-Commerce* (Ministry of Communication and Informatics and ICT Watch, 2018).

Yogyakarta Consumers Foundation (LKY)

LKY was first established in 1978 as YLKI Yogyakarta, a part of YLKI and represented Yogyakarta at the national level. Nonetheless, due to several circumstances, YLKI Yogyakarta disengaged themselves with YLKI and established its own organization—now named LKY. Significant changes that can be highlighted from this transformation: (1) LKY is independent of YLKI, and (2) LKY is no longer part of a foundation, but is now serving as CSO (Civil Society Organization).

In 2021, LKY only received 4 complaints regarding e-commerce and social commerce that were submitted with concerns such as non-delivery, goods not as advertised or incomplete. LKY is not aware about the total number of consumer complaints in Yogyakarta regarding e-commerce and social commerce since complaints are usually filed to the regional ombudsman, BPSK, or other LPKSM. It is worth noting that despite the relatively low number of complaints, this does not mean that the actual cases are low, too. Consumers often do not report complaints when the number of losses is relatively little.

Drawing from the data that has been collected from various sources and agencies, we have noted several key takeaways in the case of consumers reporting that is related to social commerce risks:

There has not been any centralized mechanism in which consumers can report their complaints. We noted that there are different agencies across government bodies and also civil society organizations that address similar issues on consumer risks. Hence, the need for collaboration and communication across institutions and organizations.

Joint initiatives across agencies and institutions needed not only for addressing the issue, but also for research and development—which may be reflected in the collection of data, cases, and reports.

There has not been any specified information on risks that are associated with social commerce. Reports and complaints on social commerce currently fall under the online transaction umbrella, which also encompasses transactions that occurred in the e-commerce sector as well. Nonetheless, agencies and organizations reported that there is a rise in consumers' complaints and reports regarding online transactions, especially in times of the pandemic.

There is a tendency of under-reporting in several cases of scams and fraud. LKY and YLKI agree that when the number of losses is perceived to be relatively small, consumers tend to not report the case. However, this might result in the continuation of the cases, where at the end, the collective losses will continue to add up and get bigger in the future.





Mapping the Existing Situation of Social Commerce Environment in Indonesia

➔ Regulatory Framework and Enforcement

Currently, there are no regulations governing solely social commerce, as social commerce is regulated under the Legal Framework on Consumer Protection, Legal Framework on Trade, and the Legal Framework on EIT. Therefore, social commerce issues are frequently merged with E-Commerce issues. Accordingly, social commerce cases do not fall only under one agency's jurisdiction, as it is highly contingent upon whether such cases can fall under the Legal Framework on Consumer Protection.

On the other hand, though current regulations require ESTOs to oversee E-Commerce and social commerce merchants,⁵⁴ there has been no practice where ESTOs or social media platforms have been held liable for failure to oversee unlicensed merchants.⁵⁵ Furthermore, it becomes challenging for social media platforms to oversee unlicensed merchants, as the difference between personal accounts and accounts selling goods can be blurry (Riefa, 2020; OECD, 2016).

⁵⁴Government Regulation No. 80 of 2019 on Trade through the Electronic System.

⁵⁵Interview with Center for Indonesian Policy Studies.

In regards to data protection, despite the PDP Bill - which requires companies to hire Data Protection Officers - not being enacted yet, several companies have started opening Data Protection Offices and hiring Data Protection Officers. Accordingly, businesses have started to become aware of the possibilities of abusive data practices, and are committed to preventing data leaks from occurring. This practice indicates the importance of the enactment of the PDP Bill, as good practices of data protection must be formalized in regulations.

For the foregoing concerns, current frameworks regulating social commerce needs to accommodate the vast development of social media dynamics. In particular, governments must be able to not only regulate, but also oversee the current practice of social commerce. One of the ways that can be done by the government in more effectively ensuring the streamlining of laws regarding social commerce and overseeing current social commerce practices includes to cooperate with ministries and governmental agencies involved in the fields of social commerce, i.e., the Ministry of Trade, the Ministry of Communications and Informatics, and BKPN.

Furthermore, it is worthy to note that despite the inexistence of a regulation on social commerce, a new regulation does not necessarily have to be established if amendments and harmonizations can sufficiently fulfill the needs to accommodate the developments of social commerce. In harmonizing the existing laws and regulations, regulators may opt to vertical or horizontal harmonization. The former refers to the harmonization of laws and regulations within different hierarchies (e.g.: the harmonization of governmental regulations with laws), while the latter refers to the harmonization of laws and regulations within the same hierarchies (e.g.: the harmonization of governmental regulations with governmental regulations) (Budoyo, 2014).

⁵⁶Interview with tech company.

⁵⁷Interview with tech company.

⁵⁸Interview with GIZ Independent Consultant*

➔ Ethical Business and Data Practices in Social Commerce

Social commerce possesses different ethical challenges with the offline business environment. First, despite the fact that this research agrees that social commerce provides room for economic participation and inclusion for the wider public, it should position itself as more than just an economic agent. Svensson & Wood (2008) argues that it should aim to be a broader agent of change. It refers to the expectation that organization should also put the social well-being of the society as its interest.

Second, the offline ethical paradigms are largely challenged by the presence of social commerce. In an offline environment, consumers identity is generally anonymous and consumers can usually trade their personal information with certain benefits from the organization (Caudill & Murphy, 2000). In social commerce, it is nearly impossible for consumers to maintain their anonymity. Once consumers are connected to the platforms, they immediately share their information, which will later become accessible to the platforms. Unfortunately, not all social commerce users are aware about the type of data they provide, when the data is being extracted, and for whom the data is transferred or used. It means “social commerce platforms collect consumers’ information in a way that consumers can neither avoid nor detect” (Ashworth & Free, 2006).

Although that data can be used to enhance users' experience in using the services, there are power imbalances between the users and the platforms. As Indonesia still lacks personal data protection awareness and regulation, there is only little control from data owners towards the use of their data. Social commerce platforms may use the users’ data as a valuable commodity. Whereas users as the data owner have little ability to opt not to share their personal information and they do not always have the power to monitor or decide how their data is used.

Third, there is also a question on the responsibility of social commerce platforms when fraud occurs. As an intermediary, social commerce bridges the transaction between sellers and consumers. However, they are not liable or responsible if there are any disputes between the sellers and consumers. In another case like data breach, research from Sadia et. al (2013) argues that despite the lurking risks, data breach relatively has little long-term effect on consumers' perception towards companies. This desensitization occurs due to the numerous accidents involving data breach.

The Indonesian e-commerce association (idEA), highlights that consumers in social commerce rely mostly on trust. There is no guarantee for consumers to be able to exercise their rights to complain or demand compensation if anything goes wrong. Consumers also have little power to opt for safe(r) ways of transactions. Thus, social media platforms need to step up their data privacy and protection measures.

In addition, as business models expand due to digitalization, consumers need to also interact with more parties when making transactions online (for instance sellers, platforms as intermediaries, logistics). Thus, Indonesian Consumer Foundation (YLKI) deemed that all these relevant parties should share the same responsibility for consumer protection.

Fourth, social media companies like Meta collect and share users data across its application. This sharing data practices leads to questions over users' consent and the tendencies towards monopolistic business models. YLKI also noted a similar trend. There is a trend where e-marketplaces are growing to have their own logistics where in some cases, they no longer provide options which service consumers would like to use which may lead to anti-competitive behavior.

→ The Need for Consumer Empowerment

As users and data owners, consumers have a critical role in ensuring their safety towards the digital world. Due to its nature, it is nearly impossible to stop personal data sharing on the internet. However, consumers can protect themselves by being aware of their situation and taking measures to reduce the risks of excessive data sharing.

All of the informants involved in the interview process agree that digital literacy holds crucial roles in hindering consumers from being exposed to the risk of data abuse on social commerce. Particularly, digital literacy should address consumers' knowledge and control over their data and personal information while transacting via social commerce. Consumers should be made aware and understand the importance and risk of privacy and data transfer in social commerce. In addition, consumers should be able to know, monitor, and decide how their data is being collected, used, and stored by social commerce platforms.

To date, there have been various activities taken by the government, platforms, and civil society organizations (CSO) to anticipate the risks of data practices by social commerce. The Directorate General of Consumer Protection and Trade Compliance, The Ministry of Trade (Kemendag), mentioned that MoT and the Ministry of Communication and Information Technology (Kominfo) are cooperating to take down fraudulent social media accounts. The Ministry can also contact social media platforms for further verification and take-down process. In addition, Kemendag can act as mediator should the consumer and business be unable to reach a settlement towards an unresolved dispute.

Likewise, The Director of Digital Economy of Kominfo also highlights the importance of digital literacy in addition to the personal data protection regulation. Kominfo is aware of the dual power that social commerce possesses. On the one hand, social commerce promotes digital economic inclusion especially during the pandemic when many are

struggling with their economic well-being. On the other hand, business and data practice of social commerce has not been fairly regulated. Thus, (potential) consumers should be educated and empowered to create a safe[®] digital environment.

From the CSO's side, LKY and YLKI claim that both institutions have been actively advocating consumers' rights, including digital transactions on online platforms. For instance, by encouraging Kominfo to push the digital literacy agenda and identify areas where government intervention through regulations is needed. They are also educating consumers by providing quick tips and tricks when shopping online using various communication channels, such as engagement with local radio and local community, ie *Kelompok Konsumen Sadar*.

Globally, there are three pre-emptive measures to better protect consumers' privacy online, such as the Digital Literacy Framework by UNESCO (2018), Privacy Literacy Model (Rotman, 2019), and Extended Model of Online Privacy Literacy (Masur, 2020). The framework from UNESCO highlights protecting personal data and privacy includes understanding in using and sharing personally identifiable information and how it is being used by the platforms. The Privacy Literacy Model added that privacy literacy also includes the understanding towards the responsibilities and risks associated with sharing information online. Whereas, the model from Masur (2020) argues that online privacy literacy should include individual and collective levels of privacy. Thus, to empower consumers in protecting their privacy and data online, it is also important to build collective awareness among stakeholders. In addition, research (Milne, 2015) suggests that a user's demographic background, trust towards the social commerce websites, risks and technology tolerance are determining users' privacy perception. Thus, digital literacy on data and privacy should be tailor made depending on the user's background and state of understanding towards privacy.

Recomendation



➔ Recommendations

This research argues that consumers' protection and empowerment holds a crucial role in ensuring ethical business and data practices in social commerce. In general, both protection and empowerment could be achieved through strengthening regulation on personal data protection and training on digital literacy. Thus, there are calls for a pentahelix collaboration which includes the government, industry and platforms, CSO, academicians and the media to contribute their parts.

The Government: There are at least four main institutions that play critical roles in ensuring consumer protection in social commerce, namely Kemendag (Ministry of Trade and Commerce), Kominfo (Ministry of Communication and Informatics), Kemenkop (Ministry of Cooperatives and Small and Medium Enterprise) and Bank Indonesia (Indonesia Central Bank). The legal analysis from the previous sub-chapter highlights there are uncovered issues which are intertwined across ministries and agencies, such as the prohibition of abusive data sharing through the ratification of personal data protections regulation. Thus, there are needs for coordination and collaboration amongst institutions. In addition, each of the

institutions can also play their roles. IdEA suggested that Kemenkop could facilitate MSMEs to hold something similar to a business permit for standardization purposes but with simplified procedures; e.g. a permit to sell household products (PIRT) by BPOM.

It is also important to highlight that the online business model develops rapidly. Therefore, the governments may also need to create regular dialogues with other stakeholders to build similar levels of knowledge and concerns towards the issues. It is also recommended to establish a co-regulatory mechanism in collaboration with social media platforms to ensure consumer rights (safety, privacy, redress) are upheld in social commerce. The government is also encouraged to work closely with the social media platforms and CSO to craft and run tailor made digital literacy programs, emphasizing on the users' knowledge and control over privacy and personal data.

Industry/Platforms: as facilitators of online transactions and the main point of contact from users, social media platforms are also expected to actively protect and educate its users while shopping online. The education can take place inside or outside the platforms. Inside the platforms, social media companies could consider establishing guidelines or terms of use that are easier to understand and easier reporting mechanism. These guidelines may help users to understand what and how their data is collected and used by the platforms. In addition, the guidelines can also be beneficial for users to learn behaviors that may indicate fraud or scams. Whereas reporting mechanisms will encourage users to notify platforms and other users' about the potential fraud and scam.

Moreover, platforms are also encouraged to make use of the technology to better protect the consumers. There is a need to ensure the safety of the systems and network to avoid online scams.

CSO: with the close proximity with the members of communities, CSO has the strength to educate individuals about the importance of privacy and personal data while being online. Aside from mass training through various communication channels, CSO could also include training for the leader of the communities and specially designed programs for vulnerable consumers, such as women in rural areas, the elderly and people with disabilities. Furthermore, CSO can also speak their voice and push the regulators to issue relevant regulations, such as personal data protection regulations.

Academics: as the digital world evolves at the speed of light, it is also crucial to conduct research and provide data as a basis for the regulation-making process by the government. Academicians could shift their focus of research towards the ethics of data practices and consumers' privacy, disseminate the finding as a basis for regulators to create decisions and formulate materials for digital literacy training.

The media: the media has the scale and credibility to broaden the impact and outreach of public awareness towards the importance of privacy and personal data protection. As more people become more aware of the underlying risks, there are more chances to change their behavior while being online. At the same time, the media could also act as a watchdog to monitor issues and regulations on this issue.



References





References

- Agustini, Pratiwi, 'Percepatan RUU PDP Dukung E-commerce saat Pandemi', Ministry of Communication and Informatics of the Republic of Indonesia, <<https://aptika.kominfo.go.id/2020/06/percepatan-ruu-pdp-dukung-e-commerce-saat-pandemi/>>
- Ahmad, S.N.; Laroche, M., 2017. Analyzing electronic word of mouth: A social commerce construct. *International Journal of Information Management*, 37(3), 202–213.
- Ahsinin, A. (2017). Tanggung Jawab Perantara dalam Tata Kelola Konten Internet [Policy brief]. ELSAM. <<https://elsam.or.id/wp-content/uploads/2019/10/Policy-Brief-4-Tanggung-Jawab-Perantara-dalam-Tata-Kelola-Konten-Internet.pdf>>
- Algharabat, Raed S. & Rana, Nripendra P., 'Social Commerce in Emerging Markets and its Impact on Online Community Engagement' *Information Systems Frontiers* 23 (2021).
- Amelina, D. and Zhu, Y.Q., 2016. Investigating effectiveness of source credibility elements on social commerce endorsement: The case of instagram in Indonesia. In *Pacific Asia Conference on Information Systems (PACIS) 2016 Proceedings*. 232.
- Article 19. (2013). Internet Intermediaries: Dilemma of Liability [Policy brief]. <https://www.article19.org/wp-content/uploads/2018/02/Intermediaries_ENGLISH.pdf>
- ASEAN Framework on Personal Data Protection.
- Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of business ethics*, 67(2), 107–123.
- Australian Competition & Consumer Commission (2021). Digital Platform Services Inquiry – March 2022 Report on general online retail marketplaces [Issues paper]. <<https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20March%202022%20report%20-%20Issues%20paper.pdf>>
- Bayari, H., & Abareshi, A. (2016). THE CONCEPTUAL FRAMEWORK OF THE FACTORS INFLUENCING CONSUMER SATISFACTION IN SOCIAL COMMERCE. *The Journal of Developing Areas*, 50(6), 365–376.
- Budke, C., Ferguson, J. (2017). Data Integration and e-Commerce Threats Challenging Providers. *Missouri Medicine*, 114(6), 419–423.
- Budoyo, S. (2014). Konsep Langkah Sistematis Harmonisasi Hukum dalam Pembentukan Peraturan Perundang-Undangan. *Jurnal Ilmiah CIVIS*, IV(2), 607–622.
- Busalim, A.H.; Hussin, A.R., 2016. Understanding social commerce: A systematic literature review and directions for further research. *International Journal of Information Management*, 36(6), 1075–1088.
- B.U., Donny, & Banyumurti, Indiyatno (Eds), *Keamanan Siber untuk E-Commerce* (Ministry of Communication and Informatics and ICT Watch, 2018). Available at: <https://spada.uns.ac.id/pluginfile.php/625755/mod_label/intro/_06_keamanan%20siber%20e-commerce%20-%20internet%20sehat%20literasi%20digital-op.pdf>
- Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing*, 19(1), 7–19.
- Commonwealth of Australia. (2016). Avoiding unfair business practiceS: A guide for businesses and legal practitioners [Australia Consumer Law Guide]. <https://consumer.gov.au/sites/consumer/files/2016/05/0553FT_ACL-guides_UnfairPractices_web.pdf>
- Chua, Hui Na; Herbland, Anthony; Wong, Siew Fan; Chang, Younghoon, 'Compliance to personal data protection principles: A study of how organizations frame privacy policy notices', *Telematics and Informatics* 34 (2017).

- Das, K. et al., 2019. The digital archipelago: How online commerce is driving Indonesia's economic development. McKinsey & Company. Available at: <<https://www.mckinsey.com/featured-insights/asia-pacific/the-digital-archipelago-how-online-commerce-is-driving-indonesias-economic-development>>.
- Deloitte. 2015. Consumer data under attack: The growing threat of cyber crime (The Deloitte Consumer Review). <<https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-nov-2015.pdf>>
- Elokari, E.A., 2020. Tokopedia data breach exposes vulnerability of personal data. The Jakarta Post. Available at: <<https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html>>.
- ELSAM. (2021). Menggagas Model Tanggung Jawab Platform Digital, Tawaran Awal [Video]. YouTube. <<https://www.youtube.com/watch?v=IrdU3jt52fs>>.
- European Commission, 2021. Proposal for a Regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.
- Flew, T., Wilding, D. (2020). The turn to regulation in digital communication: the ACCC's digital platforms inquiry and Australian media policy. *Media, Culture & Society*, 43(1): 48-65. <https://doi.org/10.1177/0163443720926044>.
- Handarkho, Y.D., 2020. The intentions to use Social Commerce from social, technology, and personal trait perspectives: Analysis of direct, indirect, and moderating effects. *Journal of Research in Interactive Marketing*, 14(3), 305–336.
- Handarkho, Y.D., 2021. Social experience vs. social technology in enhancing the intention to use Social Commerce: A case study of Indonesia. *Journal of Enterprise Information Management*, 34(3), 860–883.
- Huang, Z, & Benyoucef, M. 2013. From e-commerce to social commerce: A close look at design features' *Electronic Commerce Research* 12(4).
- Law No. 8 of 1999 on Consumer Protection.
- Law No. 11 of 2008 on Electronic Information and Transactions.
- Law No. 7 of 2014 on Trade.
- Law No. 19 of 2016 on Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.
- Ludwianto, B., 2021. Social Commerce, tren belanja online di media Sosial Yang Cuan Saat pandemi. *Kumparan*. Available at: <<https://kumparan.com/kumparantech/social-commerce-tren-belanja-online-di-media-sosial-yang-cuan-saat-pandemi-1wUPwUbo0Fx/full>>.
- Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions.
- Government Regulation No. 80 of 2019 on Trade through the Electronic System.
- Grant, hazel; and Crowther, Hannah, 'How Effective Are Fines in Enforcing Privacy?' in Wright, David; and Hert, Paul De (Eds.), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer, 2016).
- Madiaga, T. (2020). Reform of the EU liability regime for online intermediaries: Background on the forthcoming digital services act [Research paper]. European Parliamentary Research Service. <[https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA\(2020\)649404_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf)>
- Marriott, H., Williams, M., Dwivedi, Y. (2017). Risk, privacy and security concerns in digital retail. *The Marketing Review*, 17(3), 337-365.
- Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, 8(2), 258-269.
- Milne, G. (2015). *Digital privacy in the marketplace: perspectives on the information exchange*. Business Expert Press.

- Meilatinova, N., 2021. Social Commerce: Factors affecting customer repurchase and word-of-mouth intentions. *International Journal of Information Management*, 57, p.102300.
- Minister of Communication and Informatics Regulation No. 5 of 2020 on Electronic System Provider in Private Sector.
- Nurhayati-Wolff, H., 2021. Social commerce GMV Indonesia 2018-2022. Statista. Available at: <<https://www.statista.com/statistics/1256663/indonesia-social-commerce-gross-merchandise-value/>>.
- Organization for the Economic Co-operation and Development, Consumer Data Rights and Competition - Background note (OECD, 2020). Available at: <[https://one.oecd.org/document/DAF/COMP\(2020\)1/en/pdf](https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf)>
- Organization for the Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013)
- Organization for the Economic Co-operation and Development, The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines [Background Paper] (OECD, 2010). Available at: <<https://www.oecd.org/sti/ieconomy/46968784.pdf>>.
- Organization for the Economic Co-operation and Development, 2016 Ministerial Meeting on the Digital Economy Background Report: Protecting Consumers in Peer Platform Markets, Exploring the Issues [Background Report] (OECD, 2016). Available at: <<https://www.oecd-ilibrary.org/docserver/5jlwvz39m1zw-en.pdf?expires=1647919230&id=id&accname=guest&checksum=34F71CCF3DE0CDE4F9AD82D8EA4CC369>>.
- Human Rights Watch, 'Letter to Minister Plate RE: Amendments to Ministerial Regulation 5 (Mr5), May 17, 2021', Human Rights Watch, <https://www.hrw.org/sites/default/files/media_2021/05/210517%20HRW%20letter%20to%20Minister%20Plate.pdf>.
- Pandit, H.J., Lewis, D., 2018. Ease and Ethics of User Profiling in Black Mirror. In Companion Proceedings of the The Web Conference 2018, WWW '18. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, pp. 1577-1583. <<https://doi.org/10.1145/3184558.3191614>>
- Paola, M., Maria, K., 2018. Profiling with Big Data: Identifying Privacy Implication for Individuals, Groups and Society. In 2018 Mediterranean Conference on Information Systems (MCIS).
- Paypal, 2019. 'Beyond Networking: Social Commerce as a Dive of Digital Payments - Asia Report'. Paypal. Available at: <<https://www.paypalobjects.com/digitalassets/c/website/marketing/global/stories/images/paypal-asia-social-commerce-report.pdf>>.
- Paxel, 2021. Paxel Buy & Send Insights: UKM Lebih Suka Berjualan di Media Sosial. Available at: <<https://paxel.co/id/berita-dan-promo/paxel-buy-and-send-insights-ukm-lebih-suka-berjualan-di-media-sosial>>.
- Pratama, M.O., Meiyanti, R., Noprisson, H., Ramadhan, A. and Hidayanto, A.N., 2017, October. Influencing factors of consumer purchase intention based on social commerce paradigm. In 2017 International Conference on Advanced Computer Science and Information Systems (ICACSIS) (pp. 73-80). IEEE.
- PwC, 2021. 'Indonesia's Progress on Data Protection', PwC Indonesia, <<https://www.pwc.com/id/en/publications/digital/digital-trust-newsflash-2020-02.pdf>>
- PwC, 2021. 'The Digital Services Acts Package and what it entails', PwC Middle East and UK, <<https://www.pwc.com/m1/en/publications/documents/the-digital-services-acts-package.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).

- Riefa, C. (2015). *Consumer protection and Online Auction Platforms: Towards a Safer Legal Framework*. Ashgate: Farnham.
- Riefa, C., 2019. Consumer protection on social media platforms: Tackling the challenges of Social Commerce. *EU Internet Law in the Digital Era*, 321–345.
- Riefa, C. (2020). Consumer Protection on Social Media Platforms: Tackling the Challenges of Social Commerce. In Synodinou, T.E., Jougleux, P., Markou, C., & Prastitou, T. *EU Internet Law in the Digital Era* (321–345). Springer.
- Rodriguez, Katitza, 'Indonesia's Proposed Online Intermediary Regulation May be the Most Repressive Yet', Electronic Frontier Foundation, <<https://www.eff.org/deeplinks/2021/02/indonesias-proposed-online-intermediary-regulation-may-be-most-repressive-yet>>.
- SIRCLO and Ravenry, 'Navigating Indonesia's E-Commerce: COVID-19 Impact and The Rise of Social Commerce' (SIRCLO and Ravenry, 2020). Available at: <<https://files.sirclocdn.xyz/sirclo/files/Navigating-Indonesia-s-E-Commerce-COVID-19-Impact-and-The-Rise-of-Social-Commerce-SIRCLOXRavenry.pdf>>
- Svensson, G., & Wood, G. (2008). A model of business ethics. *Journal of Business Ethics*, 77(3), 303–322.
- The Law Commission and The Scottish Law Commission. (2012). *Consumer Redress for Misleading and Aggressive Practices*. The Stationery Office Limited.
- Trakman, L.; Walters, R.; & Zeller, B., 'Digital Consent and Data Protection Law - Europe and Asia-Pacific Experience,' *Information & Communication Technology Law* 29(2) (2020).
- Turban, E., Bolloju, N.; Liang, T.-P., 2010. Social commerce: an e-commerce perspective. *Proceedings of the 12th International Conference on Electronic Commerce Roadmap for the Future of Electronic Business - ICEC '10*.
- United Kingdom Department for Business, Energy & Industrial Strategy. (2018). *Misleading and Aggressive Commercial Practices: New Private Rights for Consumers Guidance on the Consumer Protection (Amendment) Regulations 2014*.
- Farivar S., Turel, O., & Yuan, Y. A (2017). A trust-risk perspective on social commerce use: an examination of the biasing role of habit", *Internet Research*, Vol. 27 Issue: 3, pp.586–607, <https://doi.org/10.1108/IntR-06-2016-0175>
- Iskandar, (2020). Marak Penipuan Online Shop di Medsos, Hati-Hati Modusnya Makin Canggih. *Liputan 6*. Available at: <https://www.liputan6.com/teknoread/4157301/headline-marak-penipuan-online-shop-di-medsos-hati-hati-modusnya-makin-canggih>
- Indozone.id (2021), Viral Beli iPhone 11 di Shopee, Cewek Ini Terkejut karena yang Datang Barang Ini, Indozone.id, Available at: [Ahttps://www.indozone.id/news/vWsBV8v/viral-beli-iphone-11-di-shopee-cewek-ini-terkejut-karena-yang-datang-barang-ini/read-all](https://www.indozone.id/news/vWsBV8v/viral-beli-iphone-11-di-shopee-cewek-ini-terkejut-karena-yang-datang-barang-ini/read-all)
- Akurat.co, (2021), Baru Menimpa Fairuz A. Rafiq, Ini Cara Menghindari Penipuan Belanja Online di Instagram, Akurat.co, Available at: <https://today.line.me/id/v2/article/pRmrr6>
- Sun, Y., Fang, S., & Hwang, Y., (2019), Investigating Privacy and Information Disclosure Behavior in Social Electronic Commerce, *Sustainability*, 2019, 11, 3311; doi:10.3390/sul1123311
- Fourberg, N., et al. (2021). Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice. European Union: Luxembourg.
- Statista (2022), Impacts of COVID-19 pandemic on the online purchase behavior among consumers in Indonesia as of May 2020, Statista, <https://www.statista.com/statistics/1127876/indonesia-impact-on-online-purchase-behavior-covid-19/>



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](https://www.instagram.com/cfds_ugm)

 [@cfds_ugm](https://twitter.com/cfds_ugm)

 [@cfds_ugm](https://twitter.com/cfds_ugm)

 CfDS UGM