International Proceeding
Universitas Tulungagung
2025

DIGITAL CONSUMER PROTECTION FROM THE PERSPECTIVE OF CONSUMER PROTECTION LAW

Satrio Pamungkas Wicaksono[1], Desti Fitriana[2], Mukhammad Alvin[3], Nurkarimah Nasuha Amalia[4], Muh. Zulkifli Muhdar[5]

[1,2,3,4]Universitas Tulungagung, Indonesia
[5]Universitas Muslim Indonesia Indonesia
nurkarimah198@gmail.com

Abstract

The development of digital technology has expanded the scope of transactions in society through e-commerce, digital financial services, and online applications. These changes have not only provided convenience, but also given rise to new forms of vulnerability such as misuse of personal data, cyber fraud, and information imbalance between businesses and consumers (OECD, 2021[1]; UNCTAD, 2020[2]). This study examines how Indonesia's legal framework, including the UUPK, ITE Law, and PDP Law, responds to these phenomena using a normative legal research approach (Marzuki, 2017[3]). The findings show that although the basis for protection is available, its effectiveness is still limited by low digital literacy, regulatory disharmony, and weak supervision and law enforcement (BPKN RI, 2021)[4]. This study emphasises the need for harmonisation of regulations, increased digital education for consumers, and optimisation of electronic dispute resolution mechanisms.

Keywords: *Consumer Protection Law, ITE Law, E-commerce, Personal Data Protection Law, Consumer Protection,*

BACKGROUND

Advances in digital technology have significantly changed people's consumption patterns. Economic activities have now shifted to the digital space, which offers speed and efficiency but also brings new risks such as data leaks, behavioural manipulation through algorithms, and online fraud (World Economic Forum, 2020[5]; Acquisti., 2015[6]).

Science, 347(6221), 509–514

Advances in digital technology have drastically changed the way people shop and increased economic efficiency. However, this also raises dilemmas related to pressing global risks. From a higher policy perspective, the main challenge that arises is how to ensure that digital transformation continues to provide economic benefits while effectively addressing inherent risks such as information leaks, behavioural manipulation through algorithms, and virtual fraud. For the World Economic Forum, this issue is more than just a technical or business issue, but a challenge in global governance that requires a strong and ethical framework

to protect data, maintain consumer trust, and prevent technology from causing instability or in justice in social and economic aspects. (World Economic Forum, 2020).

Changes in digital consumptiofocus on the fundamental conflict between the development of digital economic innovation and the reduction of individual privacy. Acquisti, a leading expert in privacy and digital economics, asserts that there is a significant hidden cost to the efficiency and speed of online transactions: consumers' personal data. From this perspective, the crucial issue is not only how to prevent data leaks, but also how to address the privacy paradox,where consumers often express the importance of privacy but are actually willing to sacrifice it for convenience or digital discounts. The core problem is that the topic of privacy and data has become the basis for behavioural manipulation through algorithms and fraud provisions, turning economic transactions into a space where personal information is used as a valuable commodity. Therefore, the main challenge is to design policies and technologies that can reform incentives in the digital economy so that companies no longer benefit exclusively from large data collection and privacy violations, in order to create a truly sustainable digital ecosystem that respects individual rights. The main risks include the threat of data leaks that affect consumer privacy and financial security; behavioural manipulation through intelligent algorithms, where digital systems use behavioural data to influence purchasing decisions in subtle ways and ; and an increase in online fraud cases that exploit the ease of digital transactions for criminal purposes. Thus, the digital age requires society to find a balance between taking advantage of digital conveniences and maintaining vigilance against security threats and ethical issues inherent in modern platforms. (Acquisti, 2015).

From a consumer protection law perspective, these developments require regulations that not only protect consumer interests in products and services,
but also their digital privacy, transaction security, and information transparency (Nasution, 2018[7] ; Howells & Wilhelmsson, 2017[8]).

Advances in digital technology require us to adapt and implement comprehensive consumer protection laws throughout the country.For academics in Indonesia, the main concern is how local regulations, such as the Consumer Protection Law, need to be expanded and strengthened to remain relevant in the context of online transactions that increasingly dominate the local market. From the perspective of the legal system in Indonesia, it can provide legal certainty and adequate access to consumer protection amid the dominance of the digital market, especially with regard to issues of digital privacy, transaction security, and clarity of information, so that consumer rights in the local market remain guaranteed and effectively protected. Thus, the main challenge lies in how to bridge the gap between existing consumer protection principles and the various complexities and new risks presented by e-commerce, to ensure legal certainty and procedural justice for consumers in Indonesia. (Nasution, 2018)

Inefficiencies in the EU consumer protection legal framework face challenges arising from the increasingly expansive digital world. The essence is that technological risks, such as potential privacy breaches and algorithmic manipulation tactics, are global in nature, but EU consumer protection laws remain too fragmented and focused on a national approach. This leads to a lack of consistency in protection in the integrated digital market. The current regulatory model cannot guarantee adequate consumer protection in a digital market that crosses national borders, and radical reform is needed in the harmonisation of consumer protection laws to address issues such as information asymmetry and deceptive practices such as dark patterns. The proposed total harmonisation and review of the EU consumer legal

framework is an important step that requires Member States to surrender their regulatory autonomy in favour of uniform, high EU standards. This is intended to create fair competition across the region, ensure data security and privacy, and address issues related to algorithm transparency and harmful digital business practices, so that consumer protection can be effective and unified across the regional digital space. (Howells & Wilhelmsson, 2017).

Although the UUPK is the main instrument for consumer protection, changes in the digital landscape show that some of its provisions are not yet able to accommodate modern transaction models (Widyaningrum, 2020)[9] .

The primary instruments for consumer protection, such as existing laws and regulations, have many gaps and are still not fully capable
covering the complexity of modern transaction models in the digital age. These tools, which are generally designed for physical markets and direct interactions, are often unable to address issues in e-commerce, such as data misuse, weak cyber security, and a lack of accountability from platform providers operating across countries.

Therefore, the author is interested in raising the research question of how legal protection related to consumer personal data is addressed in the context of the Personal Data Protection Act and the Consumer Protection Act in the digital realm.

LITERATURE REVIEW

The Concept of Consumer Protection

In classical literature, consumer protection is defined as an effort to provide legal certainty for consumers (Nasution, 2018). Modern theories have expanded this scope to include the right to privacy, data security, and access to honest information (Ramsay, 2015[10] ;Howells, 2019[11]). Regarding digital consumers, according to x with the article title. while the framework for digital consumer protection in Indonesia.

In the classical view presented by Nasution (2018), consumer protection is essentially an effort to provide legal certainty to consumers. The emphasis on legal certainty makes the study of consumer protection a normative legal study that focuses on regulations, regulated rights, and formal conflict resolution methods. Research based on this definition will focus on analysing relevant regulations and laws to assess the extent to which these norms guarantee the implementation of consumer rights (such as the right to accurate information or the right to make choices). The questions that arise tend to be evaluative and related to procedures, particularly the effectiveness of the consumer complaint process in Law No. 8 of 1999 in providing legal certainty.

It is important to examine whether an emphasis on 'legal certainty' alone is sufficient. Although legal certainty plays an important role in maintaining transaction consistency, criticism of the classical definition suggests that this approach is often formalistic and tends to neglect substantive justice, especially for consumers who are in a weak or powerless position. Therefore, the results of critical research should show that current consumer protection needs to go beyond regulatory certainty and also include protection that responds to market power imbalances, as well as ensuring that existing legal certainty is actually implemented as fair and real protection for consumers in the field.

Contemporary theories onConsumer Protection, as expressed by Ramsay in 2015, have greatly expanded the understanding of protection, no longer focusing solely on the legal certainty of transactions, but now encompassing the basic rights of consumers in the digital and

information world.

It is important to examine whether an emphasis on 'legal certainty' alone is sufficient. Although legal certainty plays an important role in maintaining transaction consistency, criticism of the classical definition suggests that this approach is often formalistic and tends to ignore substantive justice, especially for consumers who are in a weak or powerless position. Therefore, the results of critical research should show that current consumer protection needs to go beyond regulatory certainty and also include protection that responds to market power imbalances, as well as ensuring that existing legal certainty is actually implemented as fair and real protection for consumers in the field. Contemporary theories on Consumer Protection, as expressed by Ramsay in 2015, have greatly expanded the understanding of protection, no longer focusing solely on the legal certainty of transactions, but now encompassing the basic rights of consumers in the digital and information world.

Research following this perspective will focus on examining regulations and practices related to privacy rights, data security, and access to reliable information in the technological age. The questions raised in this research are evaluative and future-oriented, whereby existing laws need to efficiently protect consumers' data privacy rights from misuse on digital platforms, as well as evaluating whether the current regulatory system is adequate to protect consumer data from evolving cyber threats. The results of the study are critically expected to show that consumer protection has shifted from merely physical goods or traditional services to human rights issues in the digital realm. Criticism is directed at the inability of old regulations, which emphasise caveat emptor or legal certainty, to deal with issues of information imbalance and market dominance in the data economy. Therefore, the solution must be proactive and visionary legal proposals, such as the need for active regulation in governing the collection and use of personal data, as well as requiring algorithm transparency to ensure fairness and honesty of information.

The concept of consumer protection in classical literature, as defined, centres on efforts to provide legal certainty for consumers. This definition arises from an awareness of the position of consumers, who are naturally weaker or have an unbalanced bargaining position compared to business actors. In the classical context, this legal certainty means the existence of a clear set of legal rules that can protect consumer rights, especially in sales transactions. This protection includes a guarantee that the goods or services received are as agreed and free from defects, as well as protection against the application of unfair terms by business actors.

The basic essence of consumer protection from a legal perspective is to achieve a balance between the rights and obligations of consumers and businesses. The main focus is on the basic rights of consumers, such as the right to comfort, security, and safety in consuming goods/services; the right to choose; the right to accurate, clear, and honest information; and the right to have their complaints heard. The legal basis for consumer protection,such as Law No. 8 of 1999[12] in Indonesia, explicitly states this objective, namely to uphold the dignity of consumers and create a healthy business competition climate by ensuring legal certainty. This protection is also preventive (preventing losses) and curative (overcoming losses)

Resolving consumer protection issues requires a multidimensional approach involving increased consumer awareness and strict law enforcement. The main solutions include:

1. Improving Consumer Education and Independence: Consumers need to be encouraged to recognise and understand their rights so that they can protect themselves independently, including being careful in choosing goods/services and understanding

the contents of agreements.

2. Strict Law Enforcement: The government and law enforcement agencies must closely monitor and impose severe sanctions on businesses that violate their obligations in order to ensure legal certainty.
3. Efficient Dispute Resolution: Provide fast, simple, and inexpensive dispute resolution channels, such as through the Consumer Dispute Resolution Agency (BPSK). Disputes can be resolved through non-litigation channels (outside of court) such as mediation, conciliation, or arbitration, or through litigation channels (general court).

The approach to problem solving, whether through direct negotiation, BPSK, or the courts, must always adhere to the principles of legal certainty and justice so that the rights of aggrieved consumers (e.g., compensation in the form of refunds or replacement goods) can be properly restored. (Nasution, 2018).

Contemporary theories on consumer protection, which have been critically analysed, indicate a significant expansion in the scope of protection. Now, the focus is no longer only on the physical safety of products, but has shifted towards the security and sovereignty of consumer information in the digital economy ecosystem. The essence of this change lies in the shift in the type of risk: from traditional merchandise defects to extreme information asymmetry and personal data exploitation. Therefore, protection of privacy rights, data security, and access to transparent and accurate information have become fundamental components of consumer rights. This phenomenon arises because in digital transactions, consumers indirectly "pay" with their data, thereby increasing their vulnerability to surveillance, profiling, and potential market manipulation.

Critically, the main problem lies in the existing regulatory gap and the enormous disparity in power. The question becomes: how can the legal system effectively guarantee the principle of "consumer control" over their personal data, when the business model of digital platforms is built on the monetisation of that data, which often obtains "consent" through non-negotiable standard clauses? The solution to this issue, from a critical perspective, requires an approach that goes beyond the limitations.

conventional contractual framework. This involves the application of a legal framework based on human rights (e.g., Personal Data Protection Law), which promotes full accountability for data controllers. In addition, deterrent administrative sanctions (based on total global turnover, not just compensation for individual losses) are required, as well as the strengthening of independent supervisory agencies with adequate technical capacity. The aim is to ensure that promises of security and information integrity are not merely ethical commitments, but enforceable legal obligations. (Ramsay, 2015; Howells, 2019).

Digital Consumers

Digital consumers interact through electronic platforms, making them dependent on systems that they cannot fully control. This dependence leads to high information asymmetry and opens the door to manipulative designs based on dark patterns (Shiffman, 2020[13]; Narayanan, 2016).

The central issue for Digital Consumers is that interactions are conducted entirely through digital platforms, creating significant dependence on systems that consumers cannot fully control. In this case, there is extreme information asymmetry, where platforms have a comprehensive understanding of consumers' behaviour, preferences, and psychological vulnerabilities, while consumers only receive the information provided, which is often

incomplete. This dependence creates opportunities for the application of manipulative designs, known as dark patterns, which are user interface strategies cunningly designed to encourage consumers to make decisions that are more profitable for the company but detrimental to themselves (e.g., making the subscription cancellation process difficult or forcing consent to data use). The main question in this issue is: how can consumer protection laws effectively identify and regulate dark patterns as unfair or deceptive business practices, given the ever-changing, difficult-to-measure, and sometimes hidden nature of dark patterns in technical design? Furthermore, how can we ensure that responsibility is shifted to platform designers (business actors) rather than blaming consumer negligence? The solution to this problem is not simply to increase transparency, but requires firm legal intervention, such as requiring platforms to adopt "ethical design principles" and directly prohibiting certain types of dark patterns that have been proven to exploit consumer cognitive biases. This solution requires regulatory bodies to have the technical expertise to proactively audit and test interface designs, as well as impose heavy sanctions (e.g., fines based on percentage of turnover) to effectively reduce the economic incentives for businesses to employ such manipulative tactics. (Shiffman, 2020; Narayanan, 2016[14]).

Indonesia's Legal Framework

Digital consumer protection is regulated through several regulations. The Consumer Protection Law (UUPK) provides the general framework, the Electronic Information and Transactions Law (UU ITE) governs the validity of electronic transactions, while the Personal Data Protection Law (UU PDP) strengthens

Personal data protection. In certain sectors, the OJK and BI have also issued regulations to ensure the security of digital transactions (OJK, 2020)[15].

The legal framework in Indonesia to protect consumers in the digital world is diverse and integrated, not relying solely on a single law. The content and explanation focus on three main pillars: the Consumer Protection Law (UUPK), which serves as a general legal basis and regulates basic rights and obligations; the Electronic Information and Transactions Law (UU ITE), which guarantees the legality and legal certainty of digital transactions; and most recently, the Personal Data Protection Law (UU PDP), which specifically strengthens consumers' privacy rights and control over their data. In addition, technical regulations from institutions such as the Financial Services Authority and Bank Indonesia (BI) complement this protection, especially in the digital financial services sector. The issues that need to be critically highlighted are: how to ensure coordination and harmonisation between various cross-sector regulations (UUPK, UU ITE, UU PDP, and OJK/BI regulations) to avoid overlap or even legal loopholes in facing new challenges for digital consumers (such as dark patterns or deepfakes), as well as how to ensure effective law enforcement when jurisdiction and supervisory authority are spread across various institutions. The solution must critically include the creation of an Omnibus Law for Digital Consumer Protection or at least the formation of a Coordination Supervisory Agency with a cross-sector mandate, ensuring a single standard for fair commercial practices (especially for data and platform design), and increasing the independence and technical capacity of supervisory agencies such as BPSK or the PDP Authority so that they can quickly respond to violations and impose sanctions that are preventive and have a deterrent effect, not just compensation. (OJK, 2020)[15] .

The main essence of consumer protection in the legal context discussed in this study confirms that the Indonesian government has made progress in formulating regulations and

laws to protect personal data, although there are still challenges in their implementation. From a normative point of view, this study shows that privacy policies play a crucial role in regulating interactions between digital platforms and users, as well as explaining provisions related to data collection, processing, and protection. The high level of clarity and transparency in privacy policies recognised by respondents indicates that normative standards are beginning to be adhered to by the platforms concerned.

In addition, the discussion also highlights ethical responsibilities, stating that the protection of children in the digital realm is a shared responsibility between parents, the government, and companies. This study emphasises the importance of fair privacy practices by companies and government policies in ensuring equal online privacy protection. This is a normative disclosure of expectations regarding desired ethical and social standards.

Furthermore, the conclusion section offers recommendations based on norms addressed to stakeholders. These recommendations include the need to improve clarity and transparency in privacy policies and to build and maintain trust through good communication and data security. This has implications for the establishment of expected standards of behaviour for policymakers and platform developers to create a safe and privacy-conscious digital environment in Indonesia .

Similarly, previous research has outlined the role of the OJK as a regulator and supervisor in a normative context. As a regulator, the OJK has issued regulations such as POJK No. 77/POJK. 01/2016 concerning Information Technology-Based Money Lending Services and POJK No. 18/POJK. 07/2018 concerning Consumer Complaints in the Financial Services Sector. As a supervisor, the OJK provides legal protection to lenders in two forms: preventive protection (through education, transparent information, fair treatment, and supervision of the list of legal platforms) and repressive protection (after default, namely by assisting the collection process through mediators, restructuring, and complaint management). Disputes caused by default in loan agreements made in the form of electronic documents can be resolved through two mechanisms: litigation (in court) or non-litigation (out of court). This dispute resolution mechanism is regulated in POJK No. 18/POJK. 07/2018, starting with the submission of a complaint to the company (either verbally or in writing), then, if a resolution is not reached, the complaint can be submitted to the OJK through the Consumer Protection Portal Application (APPK), and finally to an Alternative Dispute Resolution Institution (LAPS) such as Arbitration, Mediation, or Adjudication.

Previous Studies

Previous research indicates that e-commerce oversight remains weak (Widyaningrum, 2020), while regulatory disharmony hinders the effectiveness of consumer protection (Astuti, 2021)[16].

Regarding regulatory inconsistencies that hinder the effectiveness of consumer protection, the content and explanation show that although the legal system in Indonesia is quite complex (UUPK, UU ITE, UU PDP), implementation and coordination in the field remain major challenges. Limitations in e-commerce supervision are caused by the lack of supervisory capacity, both in terms of personnel and technical skills, to directly monitor millions of transactions and products on digital platforms, making it easy for violations such as counterfeit goods or misleading information to occur. Disharmony in regulations arises when sectoral regulations (such as those issued by the Ministry of Trade, OJK, and Kominfo) conflict or are not in line with each other, making it difficult for business actors to comply with the

rules and, more importantly, making it difficult for consumers to find a clear dispute resolution channel. The main question in this problem formulation is: how to
harmonise and integrate supervisory authority among various state institutions so that they can respond quickly to the complexity of the digital market, while eliminating opportunities for business actors to "hide" behind uncoordinated regulations. Critically, resolving this issue requires changes in the institutional structure of supervision, namely by establishing an Integrated Digital Consumer Protection Agency with a single mandate and cross-sectoral executive powers to oversee e-commerce. In addition, this solution needs to be supported by investment in artificial intelligence (AI)-based surveillance technology to handle the scale of transactions, as well as definitive standardisation (Regulatory Harmonisation) through Government Regulations that bind all relevant institutions, in order to create a single legal certainty for consumers and business actors. (Widyaningrum, 2020, Astuti, 2021).

RESEARCH METHOD

This study uses a normative legal research model with a legislative and conceptual approach. This method is commonly used to assess the suitability of a legal rule with its theory and social context (Marzuki, 2017; Soekanto & Mamudji, 2018[17]). The analysis is based on primary legal materials in the form of laws and secondary legal materials such as journals, books, and reports from international institutions (Hutchinson & Duncan, 2012).
The method applied in this study is Normative Law, which focuses on the analysis of laws contained in documents, with two main approaches: the legislative approach and the conceptual approach. This study aims to conduct an in-depth analysis of the structure and content of relevant regulations (such as laws, government regulations, and related regulations) to identify their effectiveness, consistency, and possible overlapping norms. The questions formulated are evaluative and prescriptive in nature, aiming to find legal answers regarding the harmony between applicable norms (das sein) and ideal standards or expected legal concepts (das sollen). This method is very important because it not only evaluates the law from an internal perspective, but also assesses the suitability of a norm with its theory and social context; that is, the research must analyse whether the norm is relevant and fair from a philosophical and sociological perspective. Critical resolution is sought through systematic comparison between the results of analysis of legislation and the legal theories or principles studied through a conceptual approach. If normative gaps, inconsistencies, or incompatibilities between rules and the demands of social justice are found, the research results must provide constructive normative recommendations in the form of proposals for new interpretations, revisions, or the creation of regulations that are more effective and accountable in terms of doctrine, so as to produce legal reforms based on strong legal arguments. (Marzuki, 2017).

The research method applied was normative law, focusing on written law. In this study, the aim was to conduct an in-depth literature study using a legislative approach to systematically analyse all relevant regulations, as well as a conceptual approach to examine the doctrines, principles, and legal theories that form the ideal basis. The research question in this study needs to be prescriptive-evaluative, asking the extent to which the applicable legal norms are compatible or consistent with the ideal legal concepts or principles that should exist. This method is very important because it is often used to assess the extent to which a law is compatible with its theory and social context, with an emphasis that research should not only

focus on the text of the article, but also consider the philosophical and sociological aspects of the rule. Critical resolution is achieved when researchers successfully identify gaps or inconsistencies between applicable norms and the theory or social context used as a reference, and provide solid normative recommendations, including proposals for new legal interpretations, regulatory changes, or legal reforms that are more doctrinally appropriate, effective, and in line with the social dynamics of society. (Soekanto and Mamudji 2018).

This problem formulation will be descriptive and evaluative in nature, seeking to answer how the implementation or content of the law in question aligns with the legal concepts presented by experts (from journals or books) or international standards (through institutional reports), emphasising the importance of secondary sources to support and critique primary sources. A critical resolution is achieved when the research not only describes the content of the law, but also makes legal discoveries by utilising arguments from secondary sources (doctrine) to assess whether the norms in the law are sufficient, consistent, and relevant to current legal theory and relevant international standards, so as to provide suggestions for better legal interpretation or change. (Hutchinson and Duncan, 2012).

RESULTS AND DISCUSSION

Principles of Consumer Protection in Digital Transactions

In the digital ecosystem, the principles of security and safety are increasingly crucial because platforms manage large volumes of consumer data (Tene & Polonetsky, 2012)[19].

How security and consumer protection aspects are becoming increasingly important in the digital world, given that service providers manage vast amounts of consumer data. Findings on how effective and how the principles of data security and online transactions established by regulations (such as the ITE Law or Personal Data Protection Regulations) are implemented. Existing regulations aim to Balancing the risks arising from the large volume and complexity of consumer data managed by digital platforms by applying the principle of data protection by design, which is already integrated into the operations of e-commerce platforms. Therefore, an in-depth analysis can be achieved if the discussion not only explains the existence of regulations, but also highlights the protection gap between technological risks (e.g., data breaches or misuse of information) and how quickly the legal system responds. Referring to the thoughts of Tene and Polonetsky (2012), the emphasis will be directed at how there must be a shift from merely formal compliance to the application of stricter principles of accountability and data transparency by platforms. This emphasises that consumer protection in the digital world needs to produce mechanisms that ensure information security as a basic right, not just a procedural obligation for business actors.Inequality in bargaining power also arises because consumers cannot negotiate terms of service, so the principle of balance is often not achieved (Howells, 2019). The use of designs that make it difficult for consumers to understand certain choices deepens information uncertainty (Narayanan, 2016).

Traditional consumer protection laws must be revised and updated in order to effectively protect consumer rights amid the challenges of models transactions digital that are volatile, anonymous, and global in nature. The implied solution indicates an urgent need to reform these legal instruments. This change is not merely about adding new articles, but also requires a change in the regulatory approach that emphasises new legal subjects (such as digital platforms and influencers), new objects of protection (such as personal data and algorithms), and the establishment of enforcement mechanisms that are adaptive and proactive

in the cyber world. This requires specialisation in digital regulation to create protection that is appropriate to the needs of the ever-changing digital landscape (Widyaningrum, 2020).

Evaluation of the UUPK in the Digital Age

The UUPK is still relevant in terms of principles, but it was not designed to address the characteristics of digital businesses. For example, the status of platforms as intermediaries is not regulated in detail, nor are issues of personal data protection (Ardiansyah, 2020; Astuti, 2021).

The relevance of the UUPK amid the rapid development of the digital ecosystem shows that the UUPK is still important in terms of principles (such as the right to information and security), but it was not designed to address the unique characteristics of digital businesses. The normative findings emphasise structural weaknesses in the UUPK, particularly in relation to two main issues: the status of platforms as intermediaries, which is not explained in detail, and the issue of personal data protection, which is not sufficiently accommodated (Ardiansyah, 2020[20] ; Astuti, 2021). The problem raised relates to gaps in regulation, whereby the UUPK needs to be effectively applied to the responsibilities of digital platforms that function as intermediaries. The lack of clear regulations on personal data protection in the UUPK also creates legal uncertainty for digital consumers. Therefore, specific and future-proof legal reforms are needed. The proposed solution is to establish a shared liability framework ( ) for intermediary platforms and strengthen protection through the integration of strict data accountability principles (although there is currently a separate PDP Law, alignment with the UUPK is still very important), so that the protection principles in the UUPK can be fully implemented in digital transaction practices.This has led to uncertainty in determining the responsibility of platforms when disputes arise.

Implementation of the ITE Law and PDP Law

The ITE Law provides a basis for the validity of electronic contracts and the prohibition of digital fraud. However, evidence in the digital realm is often hampered by technical aspects (Susanto, 2020)[21] .

The implementation of the Electronic Information and Transactions Law (EIT Law) and the Personal Data Protection Law (PDP Law) related to the validity of contracts and the prohibition of digital fraud, with an emphasis on technical evidence challenges according to Susanto (2020), is presented in a concise paragraph.

In the section on the application of the ITE Law and PDP Law in this study, it was found that both laws have provided a strong legal basis regarding the validity of electronic contracts and the prohibition of digital fraud. Normative analysis shows that de jure, Indonesia has a solid legal framework for recognising digital transactions as valid evidence and for prohibiting cybercrime. The issues that arise, as raised by Susanto (2020)[21], concern the effectiveness of the evidentiary framework under the ITE Law and PDP Law, where the evidentiary process in a digital context is often hampered by technical factors (such as data chain of custody, the unstable nature of evidence, or the use of encryption), as well as evidentiary criteria in criminal and civil procedural law that are sufficient to address technical challenges in cases related to electronic contracts and digital fraud.

It was found that the obstacles did not stem from the absence of legislation, but rather from technical and structural limitations (e.g., the lack of competence of law enforcement officials and judges in the field of digital forensics, as well as the lack of standard procedures for collecting electronic evidence). Proposed solutions include procedural law reform to adopt

the principle of transparency in more adaptive digital evidence, as well as improving the competence of law enforcement human resources so that they can overcome the technical complexities that are the main obstacles in enforcing contract validity and sanctions against digital fraud.

The PDP Law serves as an instrument that regulates the rights of data subjects, such as the right to access, correct, and delete personal data. This regulation also follows global developments related to privacy protection (Warren & Brandeis, 1890)[22] , although the level of compliance among business actors is still low (OECD, 2020)[23] .

The Personal Data Protection Act (PDP Act) is an important regulation that emerged in response to global trends in privacy protection, which historically was based on the idea of the right to privacy proposed by Warren and Brandeis (1890). This law emphasises a comprehensive analysis of individual rights related to data, such as the right to access, correct and delete personal information, as well as comparing it with applicable international standards. Although the PDP Law has outlined individual rights related to data well, there are still questions as to why the level of compliance among business actors remains low (OECD, 2020) and how this condition affects the effectiveness of protecting these rights. On the one hand, the existing norms (data subject rights) are praised for their comprehensiveness, but on the other hand, they also reveal weaknesses in the implementation and dissemination of regulations. To overcome this problem, it is necessary to improve independent and authoritative oversight mechanisms (such as the establishment of an efficient Supervisory Agency), the imposition of administrative and criminal sanctions that truly have a preventive effect, and the implementation of extensive education programmes so that business actors realise that complying with data regulations is not merely a cost, but part of their responsibility and modern business management, so that data subject rights can be realised in practice and not just in theory.

There are weaknesses in the implementation and dissemination of regulations. To overcome this problem, it is necessary to improve independent and authoritative oversight mechanisms (such as the establishment of an efficient Supervisory Agency), the imposition of administrative and criminal sanctions that truly have a preventive effect, and the implementation of extensive education programmes so that business actors realise that complying with data regulations is not merely a cost, but part of modern business management and responsibility, so that the rights of data subjects can be realised in practice and not merely in theory.

Challenges in Law Enforcement

Some of the main obstacles include limited oversight mechanisms (UNCTAD, 2019)[24] , low digital literacy among the public (Kominfo, 2023), overlapping sectoral regulations (Astuti, 2021), and jurisdictional issues in cross-border transactions (ASEAN Secretariat, 2021).

The main obstacles to the implementation of consumer protection laws in the digital world stem from a number of interrelated issues. These include limitations in oversight by the relevant authorities (UNCTAD, 2019) and low levels of technological literacy among the public, which leads to vulnerability (Kominfo, 2023)[25] .

as well as overlapping sectoral regulations (Astuti, 2021) that create regulatory uncertainty. In addition, there are also complex issues regarding jurisdiction in cross-border

transactions (ASEAN Secretariat, 2021)[26]. To overcome regulatory overlap, it is necessary to synchronise regulations with the aim of strengthening law enforcement efforts in digital consumer protection. Furthermore, it is important for Indonesia to enhance international cooperation to resolve consumer disputes involving foreign jurisdictions, which not only illustrates the existing obstacles but also offers integrated solutions. Proposed solutions include institutional structural reforms to strengthen supervisory agencies (e.g., by imposing more serious sanctions and investigative powers), regulatory adjustments to eliminate regulatory overlap, and increasing digital literacy as a preventive measure in consumer protection. In addition, it is important to strengthen cooperation at the regional and international levels (e.g., through the ASEAN framework) in addressing jurisdictional issues so that law enforcement can be carried out effectively, comprehensively, and capable of protecting consumers without being hindered by geographical or technical boundaries. These conditions demonstrate the need for regulatory harmonisation and strengthening the capacity of supervisory agencies.

CONCLUSION

Indonesia's legal framework has provided a basis for protecting consumers in digital transactions. However, the emergence of new risks necessitates the updating of regulations and the strengthening of institutions that perform supervisory functions (World Bank, 2021).
The series of recommendations include:

1. Updating the UUPK to recognise the existence and responsibilities of digital platforms (Ardiansyah, 2020).

   Although the UUPK can still be applied in principle, its main weakness lies in the lack of clear legal categories for intermediary platforms. Often, these platforms hide behind the label of 'intermediary', which only functions as a link between sellers and buyers, thereby avoiding direct responsibility for losses suffered by consumers, such as counterfeit goods or delivery problems. Ardiansyah (2020) emphasises that there needs to be an update that creates an appropriate and layered liability mechanism, whereby platforms are not only responsible for system security and consumer data (covered by the ITE Law/PDP Law), but also bear partial responsibility for the products or services marketed, especially when the platform is proven to have been negligent in verifying its partners or allowing dishonest practices. In short, the revision of the UUPK must change the legal perspective from traditional B2C (Business-to-Consumer) transactions to a C2C (Consumer-to-Consumer) model facilitated by platforms, in order to create legal certainty and substantial justice by ensuring that consumers have a clear entity that can be held accountable in the digital economy era.
2. Strengthening the enforcement of the Personal Data Protection Law, including establishing a special personal data supervisory agency (OECD, 2020).

   Although the PDP Law has established rights for data subjects, its implementation is weak without a single entity that has authority, is independent, and is equipped with adequate resources. Critics argue that enforcement by existing institutions, which may have certain interests or be under the influence of the executive, can reduce the objectivity and effectiveness of penalties. The establishment of a Personal Data Supervisory Agency as directed by the PDP Law is an important solution because this agency will act as an independent authority with full power to conduct investigations, impose effective administrative sanctions, and provide consistent

explanations of the provisions of the law. Thus, strengthening enforcement should not only focus on the wording of articles, but also on the ability of institutions to ensure the accountability of business actors and to effectively protect the privacy rights of the public in accordance with global data management practices.

3. The application of digital dispute resolution mechanisms, including mediation and electronic arbitration (Syahputra, 2022).

   Online Dispute Resolution (ODR) provides a fast, accessible, and affordable way to resolve digital consumer issues, which are typically low in value but high in volume. However, the criticism is that although this system provides efficiency in the process, the main challenges arise from the aspects of legality, jurisdiction, and enforcement of electronic decisions, especially when the parties are located in different countries. Therefore, this conclusion emphasises the need for formal regulations (such as the ITE Law or BANI/Mediation Regulations) to be strengthened to recognise and ensure the binding legal force of mediation and arbitration processes conducted entirely electronically, so that the efficiency offered by digital systems does not compromise legal certainty and justice for consumers.

4. Improving digital literacy, particularly regarding data privacy and security (Ministry of Communication and Information Technology, 2023).

   The vulnerability experienced by consumers is often not only the result of weak regulations or negligence on the part of businesses, but also due to consumers' lack of knowledge about how platforms operate, the dangers of phishing, the importance of using strong passwords, and their rights under the PDP Law. The criticism that has arisen is that relying solely on law enforcement (repressive methods) is not effective enough without being supported by a preventive approach through widespread education. Digital literacy skills need to be transformed from mere technical skills into a critical understanding of privacy and data security, enabling consumers to make wise and safe choices in the digital world. Therefore, this conclusion emphasises the need for systematic and sustainable educational programmes involving the government, academia, and the industry sector, so that the public can become "gatekeepers" for their own personal data, thereby significantly reducing the risk of data misuse and online fraud.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behaviour in the digital age. Science, 347(6221), 509–514.

Ardiansyah, M. (2020). Reformulation of consumer protection policies in the digital economy era. Indonesian Legislation Journal, 17(4), 501–514.

ASEAN Secretariat. (2021). ASEAN consumer protection framework in the digital era. Jakarta: ASEAN Secretariat.

Astuti, M. (2021). The effectiveness of consumer protection supervision in digital transactions. Socio-Legal Review, 8(1), 45–60.

National Consumer Protection Agency of the Republic of Indonesia. (2021). Annual report on consumer protection in the digital age. Jakarta: BPKN RI.

Howells, G. (2019). The age of digital consumer law. Journal of Consumer Policy, 42(3), 437–458.
Howells, G., & Wilhelmsson, T. (2017). Consumer law and policy: Text and materials on regulating consumer markets (2nd ed.). Oxford University Press.
Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Legal research.
Deakin Law Review, 17(1), 83–99.
Ministry of Communication and Information Technology. (2023). Indonesia's digital literacy index. Jakarta: Ministry of Communication and Information Technology of the Republic of Indonesia.
Marzuki, P. M. (2017). Legal research (Revised edition). Kencana.
Narayanan, A. (2016). Dark patterns: Past, present, and future. Communications of the ACM, 59(6), 20–24.
Nasution, A. Z. (2018). Consumer protection law: An introduction. Diadit Media. OECD. (2020). Consumer protection enforcement in the digital economy. OECD Publishing. OECD. (2021). Consumer policy and the digital economy. OECD Publishing.
Financial Services Authority. (2020). Consumer protection report for the financial services sector.
Jakarta: OJK.
Ramsay, I. (2015). Consumer law and policy: Text and materials on regulating consumer markets (3rd ed.). Hart Publishing.
Shiffman, L. (2020). Consumer behaviour in the digital age. Pearson.
Soekanto, S., & Mamudji, S. (2018). Normative legal research. RajaGrafindo Persada. Susanto, M. (2020). Validity and evidentiary strength of electronic contracts in ITE law.
Padjadjaran Law Review, 8(1), 120–138.
Syahputra, E. (2022). Resolution of digital consumer disputes: Opportunities and challenges. Jurnal RechtsVinding, 11(2), 233–249.
Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control. Northwestern Journal of Technology and Intellectual Property, 11(1), 239–273.
Law No. 8 of 1999 on Consumer Protection Law Law No. 11 of 2008 on Electronic Information and Transactions
UNCTAD. (2019). Legal framework for consumer protection in e-commerce. United Nations. UNCTAD. (2020). Digital economy report. United Nations.
Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220.
Widyaningrum, A. (2020). Consumer protection in e-commerce transactions: Legal challenges in Indonesia. Journal of Law and Development, 50(2), 356–372.
World Bank. (2021). Regulating the digital economy. Washington D.C.: World Bank Group. World Economic Forum. (2020). Global risks report.
L Judijanto, M Taufik, RS Dewi, S Nur, D Jiao, Rechtsnormen Journal of Law, 2024 - Cited by 1
I Fathni, B Basri, S Zulaika, RS Dewi, Sanskara Hukum Dan HAM, 2023 - Cited by 11

Dewi, R.S., Dwiatmanto, D., & Surjanti, S. (2024). Comparison of Consumer Protection Laws Between Indonesia, the Philippines, and South Korea in Achieving Justice. *SASI*, *30*(2), 169 - 182. DOI: https://doi.org/10.47268/sasi.v30i2.2048. RS Dewi, S Surjanti, W

INFLUENCERS LIABILITY TOWARDS CONSUMERS FOR PRODUCTS PROVEN TO BE OVERCLAIMED. (2024). *INTERNATIONAL SEMINAR*, *6*, 1-8. https://conference.unita.ac.id/index.php/conference/article/view/152 S Syamhadi, MF Adiman, RS Dewi, Journal of Law and Human Rights Wara Sains, 2023 - Cited by 2

L Setianingsih, PE Wulandari, BS Purnomo, RA Rianto, AN Ahyar, RS Dewi, International Seminar, 2023 - Cited by 1