International Journal of Business, Law, and Education
Publisher: IJBLE Scientific Publications Community Inc.
Volume 6, Number 2, 2025
https://ijble.com/index.php/journal/index

Legal Response To Consumer Protection Risks In the Information Technology Era

Zahra Dwi Arianti[1], Rina Arum Prastyanti[2]
Duta Bangsa University Surakarta, Indonesia
zahradaa364@gmail.com[1], rina_arum@udb.ac.id[2]

ABSTRACT
In the rapidly evolving digital era, consumers are increasingly exposed to a variety of new threats that were previously unimaginable, ranging from the misuse of personal data to the opaque manipulation of digital behavior through algorithms and persuasive design. These phenomena signal a profound shift in the consumer landscape, where legal certainty and traditional enforcement mechanisms may no longer suffice. This article critically analyzes whether current consumer protection laws, especially within the Indonesian context, are adequately equipped to address the contemporary risks posed by information technology. By employing a normative juridical approach and enriched with comparative legal analysis, the study draws upon key philosophical foundations from thinkers such as Satjipto Rahardjo, Gustav Radbruch, Aristotle, John Rawls, Ulrich Beck, and Nonet & Selznick. These theoretical perspectives are used to frame a vision of a more responsive, just, and forward-looking legal system. Through comparisons with regulatory frameworks in the European Union, the United States (notably California), Singapore, and Malaysia, this paper proposes that Indonesia's legal architecture must evolve not merely to react but to anticipate and shape digital transformations in ways that ensure fairness, transparency, and inclusivity. Such a legal model must be both normatively grounded and practically agile to protect consumers in an increasingly borderless and algorithm-driven marketplace.

Keywords:
Digital Consumer Protection, Legal Responsiveness, Algorithmic Risk, Comparative Law, Normative Theory

INTRODUCTION

The acceleration of digital transformation has fundamentally restructured the way consumers engage with markets, services, and information. From e-commerce and mobile banking platforms to telehealth services and social media, digital technology has permeated almost every aspect of daily life. This digital integration offers a wide range of opportunities, but it also generates complex legal and ethical dilemmas, especially regarding consumer protection. Modern digital consumers face risks that are often invisible, systemic, and difficult to fix using conventional legal frameworks.

These emerging risks include but are not limited to the commodification of personal data, the proliferation of misleading digital interfaces (commonly referred to as "dark patterns"), the operation of opaque and potentially biased algorithms, and jurisdictional ambiguities that hinder law enforcement when digital services cross national borders. Often, consumers find themselves passively approving the collection of data and algorithmic profiling without a clear understanding of the consequences, an asymmetry that reflects a more profound structural imbalance in power and information. This raises a critical question: Is the existing legal system responsive enough to the disruptive effects of digital innovation? Or are they reactive and fragmented, unable to keep up with rapid technological change? Can the law still serve its basic purpose, that is, to provide justice, certainty, and usability in a digital age defined by algorithmic complexity and opacity? This article argues that the legal

system must evolve beyond reactive enforcement to embrace a proactive and anticipatory role. Based on a legal philosophy that emphasizes justice, responsiveness, and the needs of vulnerable individuals, this article seeks to reconstruct a legal paradigm that is more aligned with the digital economy. At the heart of this investigation are some influential thinkers:

Satjipto Rahardjo, who advocates for law as an instrument of social engineering that must prioritize the protection of marginalized groups; Gustav Radbruch, whose triadic conception of law emphasizes the importance of legal certainty, justice, and utility in equal measure; Aristotle and John Rawls, who stress that laws must be grounded in fairness and equality; Ulrich Beck, who highlights that modern risks are increasingly man-made and demand institutional reflexivity; and Nonet & Selznick, who envision the evolution of law from a repressive institution to a responsive and morally grounded system.

This normative perspective is used not only as a theoretical abstraction but as a tool to diagnose the shortcomings of existing consumer protection frameworks and to formulate a roadmap to meaningful reform. In particular, Indonesia's legal framework, anchored in Law No. 8 of 1999 and the ITE Law, will be assessed based on international best practices, including the European Union's GDPR and Digital Services Act, California's Consumer Privacy Act, and the data protection laws of Singapore and Malaysia. With the existence of the Consumer Protection Law, it is hoped that business actors will be more motivated to increase their competitiveness by paying attention to the interests of consumers. Consumer protection laws are crucial for sellers as business actors, as they can prevent sellers from engaging in activities prohibited by law and also protect buyers from potential losses. If sellers understand the consumer protection law, they will not violate it and sell goods according to the established rules. Through this multidimensional analysis, this article seeks to identify concrete legal strategies that are not only technologically relevant but also socially just and democratically accountable.

METHOD

This study uses a normative juridical methodology, combining philosophical-legal investigation with comparative legal analysis. The normative aspect enables an evaluation of whether the law, as it stands, fulfills its intended protective function, particularly in light of the principles of justice, legal certainty, and societal utility. A comparative analysis was used to examine how other jurisdictions, notably the European Union, California (US), Singapore, and Malaysia, have handled digital consumer protection. These regions were selected based on their pioneering or evolving approach to regulating data privacy, algorithmic accountability, and platform responsibility. The legal instruments under review include: Indonesia's Law No. 8 of 1999 on Consumer Protection, Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), General Data Protection Regulation (GDPR) and Digital Services Act (EU), California Consumer Privacy Act (CCPA), Personal Data Protection Acts (Singapore and Malaysia).

By integrating normative theories with comparative practice, this study aims to propose reform pathways that are both philosophically grounded and practically viable.

RESULTS AND DISCUSSION

1. Risks of the Digital Environment

Digital platforms, while offering convenience and efficiency, expose users to risks such as data insecurity, where personal and sensitive information is susceptible to theft, leakage, and misuse. Manipulative design: "Dark patterns" guide consumers toward choices that may not be in their best interest. Algorithmic discrimination: Automated decisions can reflect or amplify societal biases.Inequality in digital literacy: Not all consumers possess the Knowledge or tools to protect themselves. Moreover, Transnational complexity: Enforcement is difficult when service providers operate across jurisdictions.

Ulrich Beck's theory of the "Risk Society" is particularly instructive in this context. He emphasizes that modern risks are primarily man-made and structurally embedded, necessitating a legal response that is proactive, rather than reactive.

2. From Legal Formalism to Legal Responsiveness

Drawing from Satjipto Rahardjo's view of law as a tool for social transformation, it becomes evident that rigid, formalistic laws are ill-equipped to address rapidly evolving threats. Legal frameworks must be adaptive, prioritizing substantive justice over procedural rigidity.

Proposed reforms include: more rigorous and user-friendly consent protocols, mandated algorithmic transparency and accountability, accessible complaint and dispute resolution systems, and Public education on digital rights and consumer literacy. Nonet and Selznick's responsive law model further supports this approach by advocating for legal systems that evolve with stakeholder input and social needs.

3. Demystifying the Law for the Public

Gustav Radbruch's triad of values legal certainty, justice, and purposiveness provides a benchmark for evaluating laws in the digital context. Unfortunately, many legal instruments today are overly technical, vague, or inaccessible.

Reforms should aim to: Simplify legal language to improve understanding; Clarify jurisdiction in cross-border digital disputes; Ensure wider dissemination of legal rights in vernacular languages; Equip legal practitioners with digital competency.

4. Embedding Justice in the Digital Domain

From Aristotle's distributive justice to Rawls' theory of fairness, legal structures must aim to counteract systemic inequalities. In digital ecosystems, this means addressing:

a. Unbalanced contracts: "Take-it-or-leave-it" agreements disadvantage users
b. Bias in AI: Without oversight, algorithms can reinforce discriminatory outcomes
c. Behavioral manipulation: Platforms exploit cognitive vulnerabilities for profit
d. Lack of redress: Victims of digital harm often face insurmountable barriers to justice

Recommended strategies include: Independent audits of digital systems; Fairness impact assessments before deployment of algorithms; and State-funded legal aid for digital consumer claims.

5. Building Adaptive Legal Infrastructure

Responsive law requires institutional mechanisms that facilitate learning and change. This includes: Iterative law-making: Updating laws through fast-track parliamentary reviews or executive regulations; Regulatory sandboxes: Controlled

environments to pilot legal approaches for emerging technologies; Participatory regulation: Platforms for citizens, academics, and tech experts to co-create policies; Cross-sectoral governance: Coordination between government, industry, and civil society;These mechanisms ensure that legal instruments are both legitimate and effective in navigating technological complexity.

6. Global Legal Models: Insights for Indonesia

While direct transplantation of foreign laws is inappropriate, selective adoption of international best practices can enhance domestic regulation: European Union: Emphasizes user control, data portability, and platform responsibility under the GDPR and DSA; California: CCPA offers actionable rights like opting out of data sales and knowing what data is collected; Singapore & Malaysia: Provide robust regulatory frameworks with clear data authority roles and public engagement; Indonesia could adapt elements such as independent oversight bodies, stronger sanctions for non-compliance, and mandatory privacy-by-design in technology development.

Discussion

This research highlights how the rapid advancements in the digital environment, despite offering numerous benefits, concurrently introduce significant risks for consumers. Data insecurity, manipulative platform design, algorithmic discrimination, digital literacy inequality, and transnational complexity emerge as serious threats. These findings align with Ulrich Beck's "Risk Society" theory, which emphasizes that these modern risks are largely man-made and structurally embedded. Therefore, the legal response must be proactive rather than merely reactive. An emphasis on substantive justice and legal adaptability is crucial to addressing these evolving challenges, consistent with Satjipto Rahardjo's view of law as a tool for social transformation.

To address these identified challenges, this study proposes a paradigm shift from rigid legal formalism towards a more responsive legal approach. This entails advocating for more rigorous and user-friendly consent protocols, mandated algorithmic transparency and accountability, accessible complaint and dispute resolution systems, and public education on digital rights. The responsive law model championed by Nonet and Selznick further supports this approach, stressing the necessity of legal systems that evolve with stakeholder input and societal needs. Furthermore, simplifying legal language, clarifying jurisdiction in cross-border digital disputes, and ensuring wider dissemination of legal rights in vernacular languages are essential to make the law comprehensible and accessible to the broader public, aligning with Gustav Radbruch's triad of legal certainty, justice, and purposiveness.

Moreover, the research underscores the critical importance of embedding justice within the digital domain by directly confronting systemic inequalities such as unbalanced contracts, bias in AI, behavioral manipulation, and the lack of effective redress for victims of digital harm. Recommended strategies include independent audits of digital systems, fairness impact assessments prior to algorithm deployment, and state-funded legal aid for digital consumer claims. Ultimately, building an adaptive legal infrastructure through iterative law-making, regulatory sandboxes, participatory regulation, and cross-sectoral governance will ensure that legal instruments remain both legitimate and effective in navigating technological complexity. Selective adaptation of global legal models, such as the EU's GDPR,

California's CCPA, and the robust regulatory frameworks in Singapore and Malaysia, can also offer valuable insights for strengthening domestic regulation in Indonesia.

CONCLUSION

The transformation of society through information technology has not only redefined economic and social relations but has also challenged the capacity of existing legal frameworks to offer meaningful protection to consumers. As digital platforms become increasingly integral to commerce, communication, and daily life, the risks consumers face ranging from data misuse to algorithmic discrimination require a legal response that is agile, anticipatory, and grounded in principles of justice.

Traditional legal models, which are largely reactive and territorially bound, are proving inadequate in addressing the complexities of cross-border digital harms. These models often fail to account for the speed, scale, and opacity of technological change. As such, merely amending existing regulations within old paradigms will not suffice. What is needed is a structural reorientation of consumer protection law one that is deeply aligned with the nature of digital risks and the realities of the globalized internet ecosystem.

To this end, this article proposes several strategic directions:

a. Realigning Legal Norms with Technological Realities
Legal systems must transcend the inertia of formality and align more closely with the operational logic of digital platforms. Laws should address not only the outcomes of consumer harm but also the architecture of digital systems ensuring accountability in data collection, algorithmic design, and user interface manipulation.

b. Embedding Fairness, Transparency, and Justice into Legal Design
Legal design must prioritize values such as equity, accessibility, and clarity. This entails enforcing standards that mandate fairness in contracts, algorithmic decisions, and data use while ensuring that consumers, regardless of their digital literacy, can understand and invoke their rights effectively.

c. Enabling Continuous Legal Adaptation through Participatory Governance
Laws in the digital age cannot remain static. Regulatory frameworks must incorporate mechanisms for periodic review, public participation, and interdisciplinary dialogue. This includes feedback loops from affected communities, consultation with experts in technology and ethics, and legislative responsiveness to emerging risks.

d. Enhancing International and Cross-Border Cooperation
Because digital transactions routinely cross national borders, consumer protection must evolve toward greater international collaboration. This includes harmonizing data protection standards, facilitating mutual legal assistance, and developing transnational enforcement protocols to prevent regulatory arbitrage and ensure accountability.

e. Promoting a Rights-Based and Inclusive Legal Framework
At the heart of consumer protection should lie a commitment to human dignity and fundamental rights. This means shifting from a purely transactional view of consumer law to one that centers on protecting individual autonomy, privacy, and agency in digital interactions. Inclusive dialogueamong governments, businesses,

civil society, and users must guide the formulation and implementation of such laws.

In closing, consumer protection law must no longer be viewed as a supplementary tool but as a foundational pillar in shaping a fair and trustworthy digital society. Law should not be confined to reacting after harm occurs but must evolve into a dynamic institution capable of diagnosing emerging risks, preempting systemic injustices, and safeguarding the public interest in an increasingly data-driven world.

Reference

Beck, U. (1992). *Risk Society: Towards a New Modernity*. London: SAGE Publications.

California Consumer Privacy Act (CCPA) of 2018, California Civil Code §§ 1798.100 – 1798.199.

Darnia, M. E., dkk. (2023). Strategi Penguatan Hukum Perlindungan Konsumen Dalam Era Digital. *Perkara: Jurnal Ilmu Hukum Dan Politik*, 1(4), 07 November–Desember.

Digital Services Act (Regulation (EU) 2022/2065).

European Commission. (2025). *Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy*. https://ec.europa.eu, diakses 1 April.

Future of Privacy Forum. (2023). *Comparative Analysis of Global Privacy Laws*.

General Data Protection Regulation (EU) 2016/679.

Harahap, A. (2018). Macrozoobenthos diversity as bioindicator of water quality in the Bilah river, Rantauprapat, Medan. *J. Phys.: Conf. Ser.*

Howells, G., & Weatherill, S. (2005). *Consumer Protection Law*. Ashgate Publishing.

Kominfo. *Rancangan Undang-Undang Perlindungan Data Pribadi*. https://www.kominfo.go.id, diakses 1 April 2025.

Koops, B.-J. (2014). The Trouble with European Data Protection Law. *International Data Privacy Law*, 4(4).

Malaysia's Personal Data Protection Act (PDPA) 2010.

Nonet, P., & Selznick, P. (1978). *Law and Society in Transition: Toward Responsive Law*. New York: Harper & Row.

Nugroho, A. (2022). Principle of Balance of Relationship Between Banks and Customers in Mudharabah Agreements. *International Journal of Educational Research & Social Sciences*, 3(2), 645–652.

OECD. (2016). *Consumer Protection in E-commerce: OECD Recommendation*. Paris: OECD Publishing.

Rahardjo, S. (2000). *Ilmu Hukum*. Bandung: Citra Aditya Bakti.

Rahardjo, S. (2009). *Hukum Progresif: Hukum yang Membebaskan*. Jakarta: Kompas.

Radbruch, G. (2006). Statutory Lawlessness and Supra-Statutory Law. *Oxford Journal of Legal Studies*, 26(1).

Rawls, J. (1971). *A Theory of Justice*. Cambridge, MA: Harvard University Press.

Singapore's Personal Data Protection Act (PDPA) 2012.

Sinaga, D. Y. (2022). The Effect of Realistic Mathematics Learning Model and Project-Based Learning Model on Problem Solving Ability and Motivation of Students in Class V Private Elementary School Markus Medan Helvetia.

International Journal of Educational Research & Social Sciences, 3(2), 590–600.

Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), jo. UU No. 19 Tahun 2016.

World Economic Forum. (2021). *Advancing Digital Agency: The Power of Data Intermediaries*.

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 30(1).