ISSN 3139-8839 (Online)

Strengthens Or Complicates? Data Privacy Legislation And Online Consumer Protection In Brazil And India

By *Chetan Abhiraj*

VOLUME I | ISSUE II | ARTICLE V
APRIL 2026

The Legalis IP Quarterly

Abstract

E-commerce platforms have witnessed a dramatic rise worldwide: according to the United Nations Conference on Trade and Development (UNCTAD), the value of global sales reached $26.7 trillion in 2021 alone. Yet, consumer protection laws have not kept up with the paradigm shift from traditional commerce to digital transactions, thus rendering them inadequate in the face of new challenges. Traditionally based on the law of contract and torts, consumer protection laws are proving to be insufficient as personal data have increasingly become an object of trade that cannot be excluded from the analysis. In the wake of the General Data Protection Regulation (GDPR), several jurisdictions have drawn up their own privacy legislation, among which are the Brazilian LGPD and the Indian DPDP Act. But does this spate of legislative activity actually serve to bolster consumer protection, or does it merely raise the bar of requirements? A doctrinal and comparative case-study analysis of the Brazilian LGPD and the Indian DPDP Act is used to examine this issue, on the grounds of their respective differences and similarities. It is concluded that the creation of the LGPD, in synergy with the Brazilian Consumer Protection Code, enables greater clarity in terms of remedies, whereas the Indian DPDP Act, grafted on the Consumer Protection Act, 2019, has resulted in a certain measure of contradictory obligations, and the paper proposes a three-step remedy of harmonisation, expert opinion and review.

Keywords: Data Privacy, Consumer Protection, E-Commerce, LGPD, DPDP Act, Comparative Law, Regulatory Fragmentation

I. Introduction

There has been a rise in e-commerce/digital marketplaces worldwide. While the mode of the transaction switched from physical to digital, the compliance couldn't catch up with the pace. AS per UN Trade and Development (UNCTAD), there were $26.7 trillion global e-commerce sales in the year 2021.[1] This number not only shows the financial implications but also the number of people directly affected, making the legality of the transaction highly relevant. While conventionally this issue has been under consumer protection, which is part of contract/tort-based consumer law, it has become insufficient given the involvement of the digital marketplace. It is now converging with data protection laws because they have themselves become a transaction category, and thus can't be just left out.

The General Data Protection Regulation (GDPR) is the first comprehensive privacy and security law in the world.[2] Post that, various countries drafted legislation, including the LGPD in Brazil[3] and the DPDP Act in India.[4] What GDPR did was to create a Brussels effect. This surge of privacy legislation protects consumers, but it doesn't replace the consumer protection laws. Privacy legislation protects consumers' information, but doesn't fix the commercial gaps.

This paper firstly examines the disadvantages of existing consumer protection laws, and then examines whether various data privacy regulations have strengthened consumer rights or complicated them. This paper equips a doctrinal and comparative case-study methodology, supplemented by empirical literature on financial impact. The paper will analyse the various frameworks around India and Brazil, and their implications. This paper has chosen India due to its large consumer base; secondly, Brazil, because it is a civil law jurisdiction and an emerging economy. These two jurisdictions represent contrasting regulatory postures, where one represents an integrated and the other represents a fragmented response to the same underlying problem.

This paper is limited to online consumers and doesn't cover the non-brick-and-mortar consumer law generally. This paper will cover relevant sections of consumer protection statutes and data privacy statutes and their interaction in each jurisdiction.

II. Global disadvantages in consumer protection laws for online consumers

[1] U.N. Conf. on Trade & Dev., *Estimates of Global E-Commerce 2019 and Preliminary Assessment of COVID-19 Impact on Online Retail 2020*, UNCTAD/PRESS/PR/2021/009 (May 3, 2021), https://unctad.org/press-material/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-retail-sales.
[2] 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, 2016 O.J. (L 119) 1 [hereinafter GDPR].
[3] Lei No. 13.709, de 14 de Agosto de 2018, Lei Geral de Proteção de Dados Pessoais [LGPD] [General Data Protection Law], Diário Oficial da União [D.O.U.] (Braz.) [hereinafter LGPD].
[4] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023) [hereinafter DPDP Act].

Consumer protection for online customers is fundamentally different from that of traditional customers due to a lack of territorial jurisdiction. For example, if X (a consumer) buy a product from an online platform operating in a different country. Unlike the traditional consumer, where the transaction happens in the same country, the regulations and remedies are consistent. A consumer operating cross-border faces inconsistent standards with no single governing framework.

Another issue is a weak international enforcement mechanism. There is no standard global body to solve the online consumer dispute, so an aggrieved consumer has no direct international recourse. While the WTO exists, its primary function is to settle disputes between states, and it doesn't concern individuals or consumers.[5] Another course of action that a consumer could have is Online dispute resolution. The ODR mechanism isn't uniform globally; in a few countries, it can address the concern, but broader adoption lags in countries with weak digital infrastructure. This paper acknowledges that this issue is not a mere legal issue, but access to justice, and since it impacts the consumer relief, this paper has included this point. Consumers also suffer from information asymmetry and a lack of transparency. According to a survey, 70% of users experienced issues with product information, not that they failed to identify them.[6] Also, many consumers don't know about their rights and their remedies. Therefore, even in the presence of a statute, consumer protection underperforms in practice.

Lastly, the personal data used by these platforms, when violated, couldn't be covered by the consumer protection act, since it doesn't fit the legal definition of a good or service under most consumer protection statutes. This becomes a problem, particularly when an app that monetises the data as payment doesn't clearly fall within that statutory definition. This creates a coverage gap: when the economics of the transaction make data the currency of the services, the exchange falls entirely outside the consumer protection statute's scope. These structural disadvantages are what data privacy legislation has attempted, only partially, to address. The following section examines that attempt across jurisdictions.

III. CASE STUDY

A. Brazil

The primary legislation for consumer protection is the CDC (Consumer Protection Code, Law 8,078/1990).[7] CDC included provisions for consumer databases even before any dedicated privacy law. In the context of Brazilian law, legislation always views data protection as an integral part of consumer protection. Additionally, General Data Protection Law (Lei Geral de Proteção de Dados), LGPD (Law 13,709/2018, in force 2020), complements the existing CDC with articles such as article 45, which explicitly routes data breaches back to CDC consumer-

[5] World Econ. Forum, *The Global Governance of Online Consumer Protection and E-Commerce: Building Trust in the Digital Economy* 8 (Mar. 2019), https://www3.weforum.org/docs/WEF_consumer_protection.pdf.
[6] European Commission, *European Commission and National Consumer Protection Authorities Sweep of E-Commerce Websites for "Dark Patterns"*, European Union Press Release (Jan. 30, 2023), europa.eu.
[7] Lei No. 8.078, de 11 de Setembro de 1990, Código de Defesa do Consumidor [CDC] [Consumer Protection Code], Diário Oficial da União [D.O.U.] (Braz.) [hereinafter CDC].

law remedies.[8] This highlights that, in Brazil, issues like coverage gaps have been resolved, whereas in the other jurisdiction, they have not. In case a company is found, they even have to bear a financial burden, which is capped at 2% of Brazilian revenue per infraction, up to BRL 50 million.[9] Brazil highlights that the consumer protection act should be drafted with the future in mind, in addition to the earlier inclusion of the consumer database, which made LGPD much more efficient. Lastly, Brazil gives data protection high regard, as seen in their 2021 constitutional amendment (PEC 17/2019), where they elevated data protection as a fundamental right.[10]

B. INDIA

Indian consumer protection is governed by the Consumer Protection Act CPA 2019.[11]As per CPA, the definition of consumer now explicitly includes e-commerce. India also has a special legislation that addresses consumer protection in the digital realm, known as Consumer Protection (E-Commerce) Rules 2020.[12] India, unlike the other regimes, underwent a major overhaul that replaced the earlier Consumer Protection Act of 1986. As per CPA Section 2(11) 2019, a data breach is considered a deficiency of service, and the consumer forum may award compensation as it deems fit.[13] The primary issue here is the application of the section, because consumer forums aren't privacy regulators; therefore, the subject-matter knowledge available to them will not be sufficient to adjudicate a privacy harm. India's data protection is primarily based on the DPDP Act; its implementation will be phased out in 2027.[14] While the seller already had to comply with the CPA, with the implementation of the DPDP Act, they now have to maintain dual compliance. In some cases, these compliances are contrary in nature, and neither Act specifies which will supersede the other. For example, DPDP Act erasure rights vs. record retention needed for consumer dispute resolution, where one regulatory compliance conflicts with the other.

The case of India highlights that privacy law can sometimes complicate rather than simplify the process for the seller, thereby directly affecting the consumer, as compliance reduces the ease of doing business and limits the consumer's options, unlike Brazil, where the privacy law complements the consumer protection. Due to the lack of implementation of the DPDP Act, this paper couldn't provide a concrete financial implication of a violation, unlike in Brazil.

---

[8] LGPD, *supra* note 3, art. 45; *see also* Baker McKenzie, *Key Data & Cybersecurity Laws: Brazil*, Global Data & Cyber Handbook, https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/latin-america/brazil/topics/key-data-and-cybersecurity-laws (last visited Sept. 3, 2026).
[9] Lei Geral de Proteção de Dados Pessoais (LGPD), Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 15.8.2018 (Braz.), art. 52, II, planalto.gov.in; *see also* Lawwwing, *Ecommerce Compliance in Brazil*, lawwwing.com (last visited Sept. 3, 2026) (summarizing the statutory penalty enforcement framework for cross-border digital merchants).
[10] Constituição Federal [C.F.] [Constitution] art. 5, LXXIX (Braz.), *amended by* Emenda Constitucional No. 115, de 10 de Fevereiro de 2022, Diário Oficial da União [D.O.U.] de 11.2.2022, planalto.gov.in.
[11] The Consumer Protection Act, No. 35 of 2019, India Code (2019) [hereinafter CPA 2019].
[12] Consumer Protection (E-Commerce) Rules, 2020, G.S.R. 429(E) (India).
[13] CPA 2019, *supra* note 11, § 2(11).
[14] *Data Privacy Laws by Country and U.S. State (2026)*, CDP.com, https://cdp.com/basics/international-u-s-data-privacy-laws-and-regulations-you-need-to-know/ (last visited Sept. 3, 2026).

C. Comparative Analysis

Based on the case study above, the paper demonstrates that privacy legislation does not independently affect consumer rights. The efficiency of the act is based on the integration and sequencing of the privacy along with the Consumer Protection Statute. As seen in the Brazilian jurisdiction, where the LGPD is built on the CDC, Art. 45 routed breaches to consumer remedies, thereby supporting and strengthening the current consumer rights framework.[15] Integrating both the legislation produces convergences and clearer redress. India's jurisdiction has shown a different impact of privacy legislation. The DPDP Act, layered separately onto the CPA 2019, produced overlapping and sometimes contradictory compliance obligations. This dual compliance burdens the seller and reduces the consumer-facing outcomes. Neither model completely addresses the problem. The Brazilian jurisdiction offers structural integration, but lacks real-world enforcement. the indian jurisdiction offers a broadened statutory definition of "consumer" and a dedicated E-commerce rule, but suffers from overlapping and compliance burden. The solution should take structural integration from Brazil's approach and definitional breadth from India's approach. The next section will discuss the solution to the problem outlined above.

IV. Solution

This paper proposes a three-part solution taking advantage of the strengths of both jurisdictions. It is recognised, however, that no model is without gaps, including Brazil's. First, future privacy legislation should incorporate proactive legislative clarification to resolve conflicts between data privacy and consumer protection statutes at the drafting stage, rather than leaving it to courts or forums to resolve post-dispute. This speaks directly to the contradiction identified in the Indian context between the rights to erasure under the DPDP Act and the record retention requirements of the CPA for consumer disputes, with neither Act specifying which prevails. While this builds on the logic of LGPD Article 45, which routes Brazilian data breaches into CDC consumer remedies, the proposed clarification should go beyond Article 45 to address procedural conflicts such as erasure versus retention, and not just breach-remedy routing. Second, this paper recommends requiring the opinion of a subject matter expert in cases concerning a data breach. Consumer forums that deal with claims under provisions such as Section 2(11) of the CPA 2019[16] do not have any specific expertise in privacy, and therefore, before any claim involving a data breach or privacy harm is adjudicated by these forums, there should be a mandatory opinion of an expert, either in the form of a data protection authority or a data protection officer or a technical assessor. Expert opinion is an indispensable element of judgment and preserves the institutional expertise that Brazil's ANPD can bring without the need to build a whole new regulatory body. Third, this paper proposes a special committee to review the integration between privacy and consumer protection statutes annually. Indeed, a

[15] LGPD, *supra* note 3, art. 45.
[16] CPA 2019, *supra* note 11, § 2(11).

review mechanism of this sort should not be limited to the Indian context alone since even Brazil's integrated model is empirically untested at scale. The committee's mandate should be restricted to three concrete functions: reviewing reported conflicts between the two statutes, evaluating outcomes of breach cases decided with the assistance of expert opinion and recommending amendments to the harmonisation clause as and when necessary.

This solution addresses the coverage gap and privacy regulation, which both jurisdictions are facing. These three solutions, when applied together, complement each other and solve the issues we discussed in section 2: personal data employed, ODR system and lack of information on the part of the consumer.

V. Conclusion

This paper has discussed the central question of whether data privacy legislation strengthens or complicates consumer rights. While analysing this question, the paper analyses two distinct jurisdictions: India and Brazil. Based on the study, the paper finds that data privacy has an effect on the overall consumer rights, depending on integration and cross-reference to other statutes. Brazil had an integrating framework where consumer protection acts and data privacy were made in such a way that both complemented each other; on the contrary, India highlights that framework sequencing produced overlapping, sometimes contradictory obligations. Further, this paper found that neither system was flawless, as Brazil was untested at scale, and India's definitional breadth provides it with an edge in broadening the scope of protection. To solve these problems, this paper proposed 3 solutions, including a proactive harmonisation clause, a mandatory expert opinion in data breach cases, and an annual review, so that upcoming issues can be identified and prepared for in advance through proactive legislation. The paper acknowledges its limits, as there was sufficient financial literature on financial data regarding GDPR, but insufficient for Brazil and unavailable for India due to the implementation in 2027. The lessons from this paper are not limited to India or Brazil since they address universal problems. These solutions can be employed by policymakers drafting privacy legislation globally.