DATA PROTECTION AND MARKET COMPETITION: INDIA'S APPROACH TO BALANCING PRIVACY AND FAIR PLAY

ABSTRACT

This article critically analyses the convergence of data privacy and competition law in India, with particular emphasis on the challenges, overlaps in regulation, and new paradigms of the digital age. It discusses the historical development of legal frameworks that govern personal data and competition in markets, reviews significant judicial interventions and legislations, and determines sector-specific implications. It also outlines cross-disciplinary studies and international comparisons, and makes broad policy recommendations. The intention is to present a harmonized regulatory scheme that finds a balance between innovation and the protection of personal rights and competitive market forces.

Keywords: Data Privacy; Competition Law; Digital Economy; Regulatory Framework; Competition Commission of India

I. INTRODUCTION

The rapid proliferation of digital technologies and the concomitant explosion of data generation have transformed economic, social, and regulatory landscapes worldwide. In India, two closely interconnected legal regimes have emerged to play a central role in the governance of the digital economy: *data privacy law* and *competition law*. Data protection law is mainly focused on *safeguarding individual rights in relation to personal data processing*[156], while competition law is focused on *preventing anti-competitive conduct and promoting fair market competition*[157]. As data-driven digital platforms become the norm, the intersection of these regulatory regimes is both fraught with challenges as well as full of unparalleled opportunities for regulation. [158]

India's path towards strong data protection was triggered by a historic Supreme Court ruling affirming the right to privacy as a constitutional right under the Indian Constitution[159]. This ruling provoked further legislative efforts toward enacting a more comprehensive and robust regime for data protection. On the other hand, India has established its competition laws under the

[156] Dhiraj R Duraiswami, 'Privacy and Data Protection in India' (2017) 6(1) Journal of Law & Cyber Warfare 166, 167 <http://www.jstor.org/stable/26441284> accessed 13 March 2025.

[157] Aditya Bhattacharjea and Oindrila De, 'Cartels and the Competition Commission' (2012) 47(35) Economic and Political Weekly 14 <http://www.jstor.org/stable/41720077> accessed 13 March 2025.

[158] Anadi Tewari, 'A Critical Evaluation of India's Proposed Digital Competition Act' (2024) 5(1) Competition Commission of India Journal on Competition Law and Policy 79, 85 <https://doi.org/10.54425/ccijoclp.v5.197> accessed 13 March 2025.

[159] The Constitution of India 1950, art 21.

Competition Act, 2002, with operative oversight by the Competition Commission of India *(CCI)* to address issues of market concentration and dominance in the digital space. [160]

The intersection of competition law and data privacy is most applicable in today's times.[161] Data has become a strategic asset that fuels market dominance.[162] Dominant digital platforms leverage massive pools of personal data to optimize their services, create tailored user experiences, and construct high entry barriers.[163] These developments pose two critical questions to regulators: *How can they protect individual privacy without stifling innovation? How are anti-competitive actions constrained in a system where data plays a dual role as an economic commodity and as a potential risk factor?*

The article examines these questions by presenting an in-depth analysis of the development and interplay between data privacy and competition law in India. The discussion commences with a historical context and constitutional underpinnings of privacy rights, to be followed by a discussion on legislative developments and judicial interpretations. This is followed by the analysis of the development of competition law, statutory provisions, leading cases, and regulatory change. Later sections analyse overlapping areas of the two legal fields, establishing conflicts, overlaps, and regulatory complementarities. The article further contains a more detailed comparative examination with the European Union *(EU)* model and touches upon emerging challenges based on new technologies like artificial intelligence (AI) and blockchain. Finally, other sections review nascent trends - including the impact of quantum computing and the Internet of Things *(IoT)* - before finishing with inclusive policy suggestions and avenues for future research.

The central thesis is that while data privacy and competition law have traditionally pursued distinct objectives, their interdependence in the digital economy necessitates an integrated approach. This policy should protect the consumer's interest while avoiding behaviours that are monopolistic and at the same time push the frontiers of technology and economic growth.

II. EVOLUTION OF DATA PRIVACY LAWS AND COMPETITION LAWS IN INDIA

A. Privacy Laws in India

The concept of privacy in India has its roots in constitutional jurisprudence. In the past, privacy was not recognized as an independent right in legal context till the turning point in Justice K. S. Puttaswamy v Union of India[164]. The judgment of 547 pages contains six different opinions, with

[160] Anadi Tewari, 'A Critical Evaluation of India's Proposed Digital Competition Act' (2024) 5(1) Competition Commission of India Journal on Competition Law and Policy 79 <https://doi.org/10.54425/ccijoclp.v5.197> accessed 13 March 2025.

[161] Ibid, 93.

[162] Ibid, 101.

[163] Ibid, 93.

[164] *Justice K.S. Puttaswamy v Union of India* 2019 (1) SCC 1.

the binding authority in the unanimous order signed by all nine judges. This judgment overruled the previous judgments in M. P. Sharma[165] and Kharak Singh[166] and reaffirmed that the right of privacy is an integral facet of the right to life and personal liberty under Article 21[167], and also a part of the freedoms provided by Part III of the Constitution[168]. Although Justice Chandrachud's plurality opinion - authored on behalf of four judges - provides extensive reasoning on privacy as an element of human dignity, its views are not binding since a majority of five judges is required to establish precedent.

Until this landmark ruling, India did not have a separate independent law to safeguard personal privacy; rather, it was tackled through different legislative provisions. For example, the Indian Penal Code, 1860 *[now repealed by the implementation of the Bharatiya Nyaya Sanhita, 2023 (BNS)]* had special sections dealing with issues of privacy such as Section 354C[169] which made voyeurism an offence, Section 354D[170] which addressed stalking (including cyber stalking), and Section 228A[171] which protected the identity of some victims of crime.

Concurrently, the Information Technology Act, 2000, initially intended to legalize e-commerce and prevent cybercrime, was amended in 2008[172] to address larger digital issues such as phishing, voyeurism in cyberspace, and the theft of information. For instance, Section 66A[173], which limited abusive online messages, was finally struck down by the Supreme Court in Shreya Sighal v Union of India[174], whereas Sections 67[175] and 67A[176] penalized the transmission of obscene content, and Section 69A[177] authorized the government to block access to information dangerous to national security or public order.

However, these laws were made without taking into consideration the complex forms of data handling and digital environments that have developed within the last two decades, and therefore paved the way towards the complete data protection systems provided under the Digital Personal Data Protection Act, 2023.

One of the pivotal elements of the DPDP Act is its elaborate definition and coverage. The Act establishes personal data as *any information pertaining to identified or identifiable individuals and covers data*

---

165 *M. P. Sharma and Others v Satish Chandra, District Magistrate, Delhi, and Others* AIR 1954 SC 300.
166 *Kharak Singh v The State of U.P. & Others* AIR 1963 SC 1295.
167 The Constitution of India 1950, art 21.
168 The Constitution of India 1950, pt III.
169 Indian Penal Code 1860, s 354C.
170 Indian Penal Code 1860, s 354D.
171 Indian Penal Code 1860, s 228A.
172 Information Technology (Amendments) Act 2008.
173 Information Technology Act 2000, s 66A.
174 *Shreya Sighal v Union of India* AIR 2015 SC 1523.
175 Information Technology Act 2000, s 67.
176 Information Technology Act 2000, s 67A.
177 Information Technology Act 2000, s 69A.

gathered both offline and online when converted into digital form.[178] The regime prescribes consent as the basis of processing of data[179] and above everything *requires notifying people on the data collected, its purposes and can also withdraw consent at a moment's notice*.[180] At the heart of the Act is the establishment of the Data Protection Board of India, tasked with overseeing compliance and addressing grievances related to data breaches.[181] The layered structure tries to strike a balance between privacy rights of the individual and general public and state interests.

Since the Puttaswamy judgment[182], the Indian judiciary has played an active role in the developing debates regarding data privacy. The broad understanding of privacy rights has prompted courts to examine state surveillance and the duties of both public and private data controllers.

B. Competition law in India

India's modern competition law regime is primarily characterized by the Competition Act, 2002, which was later amended by the Competition (Amendment) Act, 2007 and most recently by the Competition (Amendment) Act, 2023, which were implemented to enhance market competition, safeguard consumer interests, and restrain anti-competitive behaviour. The Act[183] broke away from its previous regulatory approach by adopting a market model with a focus on economic efficiency and consumer interest. The hub of this legislative framework is the Competition Commission of India (CCI)[184] that has the authority to investigate and penalize practices like anti-competitive agreements, abuse of dominance, and failure to provide transparency in mergers and acquisitions. The key sections of the Competition Act, 2002 include *prohibition of anti-competitive agreements* under Section 3[185] *[Section 4 under the Amendment Act of 2023*[186]*]*; *prohibition of abuse of a dominant position* under Section 4[187] *[Section 5 under the Amendment Act of 2023*[188]*]*; *regulation of combination of enterprises (mergers, acquisitions, and amalgamations) that could distort market structure* under Sections 5 and 6[189] *[Sections 6 and 7 under the Amendment Act of 2023*[190]*]*; *establishment of the Competition Commission of India* under Chapter III[191]; as well as *its duties, powers and functions of commission outlined* under Chapter IV[192]. These

[178] Digital Personal Data Protection Act 2023, s 2.
[179] Digital Personal Data Protection Act 2023, s 4.
[180] Digital Personal Data Protection Act 2023, s 6.
[181] Digital Personal Data Protection Act 2023, s 18.
[182] *Justice K.S. Puttaswamy v Union of India* 2019 (1) SCC 1.
[183] Competition Act 2002.
[184] Competition Act 2002, s 7.
[185] Competition Act 2002, s 3.
[186] Competition (Amendment) Act 2023, s 4.
[187] Competition Act 2002, s 4.
[188] Competition (Amendment) Act 2023, s 5.
[189] Competition Act 2002, ss 5 and 6.
[190] Competition (Amendment) Act 2023, ss 6 and 7.
[191] Competition Act 2002, ch III.
[192] Competition Act 2002, ch IV.

provisions have established a robust legal foundation for maintaining fair competition in a rapidly changing market environment.[193]

The judiciary has had a critical role in interpreting the Competition Act[194] and influencing its enforcement across different industries. The landmark orders by the CCI have significantly touched the market regulation space, particularly in digital markets as well as traditional industries. In Indian Broadcasting and Digital Foundation & Another v Alphabet Inc. & Others[195], the CCI held that Google's imposition of a discriminatory and exorbitant service fee upon a small subset of 3% of app developers on the Google Play Store constituted an abuse of dominant position. Likewise, in Winzo Games Private Limited v Google LLC and Others[196], the CCI noted that Google's selective and non-transparent listing of real-money-gaming apps via indefinite pilot programs distorted competition and erected entry barriers for some developers.

Furthermore, in Bharti Airtel Ltd. v Reliance Industries Ltd. and Reliance Jio Infocom Ltd.[197], the CCI had scrutinized predatory pricing charges as well as abuse of dominant position. Reliance Jio's initial launch involved offering free telecommunication services for a couple of months in order to quickly acquire market share on the basis of fiscal support of Reliance Industries. The CCI had opined that such free availability was not anti-competitive practice, emphasizing market forces, choice of the buyer, and the digital power of Jio. The judgment imposed a narrow approach to the Competition Act, creating a disputed precedent for assessing dominance in a market.

These decisions reflect CCI's forward-looking role as a watchful competition enforcer, weighing its enforcement authority against due process concerns and encouragement of alternative dispute mechanisms that further enhance an effective establishment of market justice and accountability in India.

C. Regulatory Initiatives and Sector-Specific Interventions

Responding to the speedy expansion of digital markets, the Ministry of Corporate Affairs *(MCA)* constituted the Committee on Digital Competition Law *(CDCL)*. This was based on recommendations from the 53rd report of the Parliamentary Standing Committee on Finance,

---

[193] Aditya Bhattacharjea and Oindrila De, 'Cartels and the Competition Commission' (2012) 47(35) Economic and Political Weekly 14 <http://www.jstor.org/stable/41720077> accessed 13 March 2025.

[194] Competition Act 2002, s 7.

[195] *Indian Broadcasting and Digital Foundation & Another v Alphabet Inc & Others*, Case No 27 of 2023 (Competition Commission of India, 15 March 2024).

[196] *Winzo Games Private Limited v Google LLC and Others*, Case No 42 of 2022 (Competition Commission of India, 28 November 2024).

[197] *Bharti Airtel Ltd v Reliance Industries Ltd and Reliance Jio Infocom Ltd*, Case No 3 of 2017 (Competition Commission of India, 9 June 2017).

titled *Anti-Competitive Practices by Big Tech Companies*.[198] Led by the Secretary of MCA, the committee examined the need for a separate competition law for digital markets.[199] In 2024, it presented its report, *Report of the Committee on Digital Competition Law*[200], and a Draft Bill, which proposed stricter regulations in areas like e-commerce, digital advertising, and fintech. All these regulatory measures have been aimed at curbing steps causing hoarding of information and algorithmic manipulation, possibly ultimately harming consumer well-being and market entry.[201] The CCI strategy now combines the old school economic analysis with data analytics, to make sure enforcement plans take note of the details of the digital economy. [202]

The Commission's targeted interventions not only address overt anti-competitive practices but also promote an ecosystem in which innovation and consumer choice are preserved. Such a two-track approach seeks to reconcile the requirement of market discipline with the nurturing of technological advancement.[203]

D. Expanding the Framework: Data-Driven Market Analysis

Traditional methods of assessing market power - relying heavily on pricing and market share - are increasingly inadequate in digital markets where data plays a central role.[204] As online platforms use vast quantities of data to build competitive advantages, regulators require new analytical toolkits that will capture intangible assets, network effects, and algorithmic efficiencies.[205] This new model now perceives data as a fundamental part of market dynamics, requiring interdisciplinary collaboration among economists, data scientists, and lawyers.[206]

And so, not only does this latest model of market analysis translate into the quantitative elements of competition, but it also provides qualitative analysis on the impact of data-driven practices on consumer welfare and market integrity.[207]

---

[198] Standing Committee on Finance, *Anti-Competitive Practices by Big Tech Companies* (Fifty-Third Report, Seventeenth Lok Sabha, Ministry of Corporate Affairs, 2022-2023) <https://eparlib.nic.in/bitstream/123456789/1464505/1/17_Finance_53.pdf> accessed 13 March 2025.

[199] Ibid.

[200] Ministry of Corporate Affairs, Government of India, *Report of the Committee on Digital Competition Law* (2024) <https://prsindia.org/files/parliamentry-announcement/2024-04-15/CDCL-Report-20240312.pdf> accessed 13 March 2025.

[201] Anadi Tewari, 'A Critical Evaluation of India's Proposed Digital Competition Act' (2024) 5(1) Competition Commission of India Journal on Competition Law and Policy 79, 94 <https://doi.org/10.54425/ccijoclp.v5.197> accessed 13 March 2025.

[202] Ibid, 100.

[203] Ibid, 92.

[204] Ministry of Corporate Affairs, Government of India, *Report of the Committee on Digital Competition Law* (2024), 94 <https://prsindia.org/files/parliamentry-announcement/2024-04-15/CDCL-Report-20240312.pdf> accessed 13 March 2025.

[205] Competition Commission of India, *Journal on Competition Law and Policy*, vol 1 (December 2020), 16 <http://164.100.58.95/sites/default/files/whats_newdocument/Volume1-Dec-2020.pdf> accessed 14 March 2025.

[206] Ministry of Corporate Affairs, Government of India, *Report of the Committee on Digital Competition Law* (2024), 94 <https://prsindia.org/files/parliamentry-announcement/2024-04-15/CDCL-Report-20240312.pdf> accessed 13 March 2025.

[207] Ibid, 108.

III. CONVERGENCE OF DATA PRIVACY AND COMPETITION LAW

A. Data as a Strategic Asset in the Digital Economy

In today's digital economy, data is viewed as a strategic resource that fuels innovation and competitiveness.[208] Large digital platforms use vast amounts of consumer data to customize services, fine-tune algorithms, and support market positions.[209] This two-sided application of data - as a force for efficiency and a possible source of anti-competitive influence - requires a harmonized regulatory framework that protects individual privacy while supporting fair competition.[210]

The two sides of data as economic value and privacy threat best express the underlying tension between data protection and competition law objectives. On the one hand, it is important to ensure strong privacy protections for the rights of individuals. On the other hand, a regime that is too strict may hinder innovation-critical data flows.[211]

B. Regulatory Overlaps and Conflicts

The convergence of data protection and competition law is likely to create regulatory interactions and conflicts. For example, the DPDP Act's strict provisions concerning data localization - for reasons of safeguarding data security and national sovereignty - could potentially hinder the free flow of data essential to spreading competition and innovation. On the other hand, a relaxed regime of data protection may enable dominant companies to concentrate their data resources and undertake anti-competitive behaviour.[212]

Arguably the most contentious of these is the issue of data localization. On the side of having such a requirement, it is argued that this enhances security and enables domestic legal protection to be enforceable. It is, however, asserted that this would reinforce the market position of the giants and curtail competition by discouraging new entrants.[213]

C. Judicial Responses to Digital Dominance

Judicial remarks too have come to recognize the multi-dimensional impact of digital dominance. In a historic order, the CCI moved against what it believed was an exploitation of market power

[208] Ibid, 93.
[209] Ibid, 94.
[210] Ibid, 108.
[211] Ibid, 97.
[212] Ibid 39.
[213] Ibid.

by Meta in the form of its WhatsApp app in Re: Updated Terms of Service and Privacy Policy for WhatsApp Users[214]. The inquiry was into the 2021 revision of WhatsApp's privacy policy that required users to agree to enhanced data gathering and sharing procedures as a condition of service, and there was no alternative but to opt-in. The decision is especially significant inasmuch as it is the first time that the CCI has taken privacy - an aspect hitherto associated with data protection legislation - into account while dealing with a non-price dimension of competition, thereby broadening regulatory horizons.

In its order, the CCI not only levied a monetary fine of INR 213.14 crore on Meta and WhatsApp - the first time the new CCI (Determination of Monetary Penalty) Guidelines, 2024[215], were applied - but also required fundamental structural reforms. The remedies necessitated a prohibition on the sharing of WhatsApp user data with other Meta entities for ad targeting and banned making sharing of such data a condition of using WhatsApp services in India. These remedies seek to bar Meta from using its over-the-top messaging dominance to obtain an unfair competitive advantage in the online display ad market.

The consequences of this ruling are wider than this case and set a precedent for treating privacy as a factor in assessing competition in future cases. Thus, the CCI has brought about a change in the approach to examining practices in the digital market, potentially influencing global regulatory approaches.

WhatsApp and Meta challenged the CCI's decision before the Delhi High Court[216], as well as the Supreme Court followed by its dismissal by the Delhi High Court. The Supreme Court too upheld the CCI's authority, ruling that once the regulator has established a prima facie case of a violation and initiated proceedings, its actions are not subject to a jurisdictional bar.[217] The Supreme Court insisted that the inquiry must go ahead without delay, with any arguments of Meta and WhatsApp to be scrutinized on their merits by the CCI. The CCI subsequently issued another order on the same issue in 2024 examining the judgments of the Delhi High Court and the Supreme Court.[218]

The decision is set to leave a lasting legacy on the digital industry, affirming the necessity for technology firms to weigh innovative business models against equitable competitive conduct and strong consumer privacy protections.

---

[214] *Re: Updated Terms of Service and Privacy Policy for WhatsApp Users*, Suo Moto Case No 01 of 2021 (Competition Commission of India, 24 March 2021).

[215] The Competition Commission of India (Determination of Monetary Penalty) Guidelines 2024.

[216] *WhatsApp LLC & Anr v Competition Commission of India*, LPA 163/2021 & CM APPLs 15908/2021, 16893/2021, 18800/2021, 18910/2021, 46058/2021, 46059/2021, 46655/2021.

[217] *Meta Platforms Inc v Competition Commission of India & Anr*, SLP (C) No 17121/2022.

[218] *Re: Updated Terms of Service and Privacy Policy for WhatsApp Users*, Suo Moto Case No 01 of 2021 (Competition Commission of India, 18 November 2024).

D. Interdisciplinary Perspectives and Scholarly Debates

The confluence of competition law and data privacy has stimulated a rich inter-disciplinary discussion between technologists, economists, and legal scholars.[219] Scholars contend that data need to be thought of as a regulatory commodity in and of itself - one that bridges the gap between economic hegemony and individual privacy. Their claim is that established legal silos are not suited to meet the intricacies of data markets but rather need a combined effort in order to get into equilibrium the cross-cutting goals of protection of privacy and market fairness.[220]

A focus of other research is on the threat posed by regulatory arbitrage, where firms exploit competition and privacy law differences to build market power while appearing to satisfy regulatory requirements.[221] Comparative analysis, particularly addressing the EU's harmonized approach, demonstrates that synchronized regulatory models can achieve a balance between innovation, privacy, and competition that is interesting to the Indian context.[222]

IV. ADDRESSING COMPETITION AND DATA GOVERNANCE IN THE DIGITAL ECONOMY

A. The Role of the Competition Commission of India

The CCI is the central regulatory body in imposing competition law in India. Charged with administering the Competition Act, 2002, the CCI has increasingly developed its approach to meet the specific challenges of digital economy.[223] The Commission has in recent years reviewed the behaviour of dominant digital platforms - particularly in industries like e-commerce and digital advertising - to ensure that data aggregation and algorithmic manipulation are not undermining market fairness.[224]

The evolving approach of the CCI now incorporates advanced data analytics to assess market dominance, examining quantitative factors like market share and qualitative factors like data control and algorithmic transparency. This is meant to be an all-encompassing strategy to address

---

[219] Ministry of Corporate Affairs, Government of India, *Report of the Committee on Digital Competition Law* (2024), 97 <https://prsindia.org/files/parliamentry-announcement/2024-04-15/CDCL-Report-20240312.pdf> accessed 13 March 2025.
[220] Ibid, 108.
[221] Ibid, 112.
[222] Ibid, 59.
[223] Anadi Tewari, 'A Critical Evaluation of India's Proposed Digital Competition Act' (2024) 5(1) Competition Commission of India Journal on Competition Law and Policy 79, 80 <https://doi.org/10.54425/ccijoclp.v5.197> accessed 13 March 2025.
[224] Ibid, 81.

the multifaceted aspects of digital competition and to render enforcement tools efficient in an increasingly dynamic environment.[225]

B. Judicial Engagement with Data-Centric Competition Cases

Judicial intervention in data-driven market conduct has increased significantly. Courts are also increasingly sensitive to the fact that the accumulation of vast data reservoirs by market incumbents can lead to exclusionary behaviour harming competition.[226] In a number of rulings, the courts have highlighted data transparency in processing and concurred that strong privacy safeguards can act as a curb on anti-competitive conduct.[227] To provide just one example, in examining digital mergers for their likely impact on the market, the judges have been adding data analytic issues and concepts of algorithmic fairness to what they are considering.[228]

C. Policy Synergies and Coordination Among Regulators

Greater coordination among data protection authorities and competition agencies is required to regulate effectively in the digital economy. In India, the DPDP Act would most likely coordinate closely with the CCI so that enforcement becomes mutually reinforcing.[229] Coordination among agencies may be in various forms, including joint investigations, collective data analysis, and joined-up regulatory guidelines tackling privacy and competition issues simultaneously. Such a collaborative structure is particularly critical in industries whose data practices have significant impacts on the market dynamics. [230]

D. Sectoral Impact Analysis: Case Studies from the Digital Economy

Thorough sectoral analyses also indicate the converging opportunities and challenges for competition law and data privacy. In e-commerce, for example, top platforms use massive amounts of consumer data to improve supply chain management and personalize user experience.[231] Although these conducts fuel operational efficiency and maximize customer satisfaction, they also potentially raise entry barriers for more modest players.[232] Regulatory oversight of the industry has

---

[225] Ibid.
[226] Competition Commission of India, *Journal on Competition Law and Policy*, vol 1 (December 2020), 3 <http://164.100.58.95/sites/default/files/whats_newdocument/Volume1-Dec-2020.pdf> accessed 14 March 2025.
[227] Ibid, 4.
[228] Ibid, 33.
[229] Ministry of Corporate Affairs, Government of India, *Report of the Committee on Digital Competition Law* (2024), 40 <https://prsindia.org/files/parliamentry-announcement/2024-04-15/CDCL-Report-20240312.pdf> accessed 13 March 2025.
[230] Ibid.
[231] Competition Commission of India, *Journal on Competition Law and Policy*, vol 1 (December 2020), 53 <http://164.100.58.95/sites/default/files/whats_newdocument/Volume1-Dec-2020.pdf> accessed 14 March 2025.
[232] Ibid, 54.

seen demands for greater transparency in the use of data and algorithmic decision-making, and the CCI having taken a hybrid model that blends qualitative and quantitative evaluations of market effect.[233]

Similarly, in the online advertising market, data concentration by a handful of companies has also brought issues of monopolistic behaviour. While targeted advertising has revolutionized how businesses do marketing, it has also brought about market concentration that has the potential to constrain consumer choice. Specific regulatory intervention in these industries is necessary to ensure that data-driven innovation doesn't happen at the cost of competitive balance.[234]

V. COMPARATIVE ANALYSIS BETWEEN INDIA AND THE EUROPEAN UNION

A. Foundational Similarities

Both the EU and Indian competition regimes conceptualize abuse of dominance as the misuse of market power that distorts competition.[235] In the EU, Article 102 of the Treaty on the Functioning of the European Union *(TFEU)* forbids such conduct by dominant undertakings. Likewise, the Indian Competition Act, 2002 also defines abuse of dominance as conduct that has a negative impact on competitors, consumers, and general market conditions. The determinative role played by both sets of systems depends crucially upon the rigorous definition of the "relevant market" through vehicles such as the EU's Small but Significant Non-transitory Increase in Price *(SSNIP)* test[236], as well as corresponding analytical techniques applied in India. Such a definition of the market facilitates the determination of whether an enterprise has a dominant position.

From a data protection perspective, both jurisdictions recognize that personal data itself can constitute an element of market power. In the EU, the General Data Protection Regulation *(GDPR)* identifies data minimization, informed consent, and lawful processing as core principles. India's DPDP Act, 2023 similarly seeks to protect informational privacy, though its enforcement is at an earlier stage. Both regimes thus acknowledge that privacy and competition are interlinked, particularly in digital markets where user data is a key asset.

B. Divergent Regulatory Approaches

[233] Ibid, 55.

[234] Ministry of Corporate Affairs, Government of India, *Report of the Committee on Digital Competition Law* (2024), 38 <https://prsindia.org/files/parliamentry-announcement/2024-04-15/CDCL-Report-20240312.pdf> accessed 13 March 2025.

[235] Competition Commission of India, *Journal on Competition Law and Policy*, vol 1 (December 2020), 57 <http://164.100.58.95/sites/default/files/whats_newdocument/Volume1-Dec-2020.pdf> accessed 14 March 2025.

[236] Ibid, 3.

A key divergence lies in how each jurisdiction addresses digital markets. The EU has taken a proactive stance with ex-ante regulation through the Digital Markets Act *(DMA)* and the Digital Services Act *(DSA)*.[237] These rules are aimed at identifying "*gatekeepers*" - major online platforms with considerable market power - and subjecting them to obligations to make them contestable, fair, and transparent prior to any abusive behaviour taking place.[238] Enforcement is centralized through the European Commission, assisted by Regulation 1/2003, which enables uniform application of competition rules across member states.

Moreover, the EU framework integrates *data protection obligations* under the GDPR alongside competition enforcement. For example, dominant platforms cannot rely on blanket consents to process personal data, as clarified by the Court of Justice of the European Union *(CJEU)* in the Meta Platforms decision[239], where combining user data across services without explicit consent was found to breach both GDPR and competition law principles. This demonstrates the EU's holistic view that the misuse of personal data can reinforce dominance and therefore requires regulatory intervention.

On the other hand, the Indian strategy remains anchored in its legacy competition paradigm. India's Competition Act, 2002 regulates market behaviour, although its enforcement in the rapidly evolving digital economy is in the process of evolving.[240] While there is discussion and proposal for having a dedicated Digital Competition Law, India currently has to manage with conventional investigative powers wielded by the CCI and decided by the Competition Appellate Tribunal.[241] This indicates a regulatory environment that is gradually adapting to the issues of digitalization.

C. Enforcement and Judicial Oversight

In the EU, robust judicial oversight by the CJEU has led to a rich body of case law - such as the Hoffman La Roche[242] and the Google Shopping[243] cases - that demonstrates stringent scrutiny of dominant firms. The EU's centralized power ensures uniform action within the internal market. Significantly, the CJEU has reinforced that data protection rules under the GDPR must be read in

---

[237] European Commission, 'Sneak Peek: How The Commission Will Enforce The DSA & DMA - Blog Of Commissioner Thierry Breton' (5 July 2022) <https://ec.europa.eu/commission/presscorner/detail/en/statement_22_4327> accessed 14 March 2025.

[238] Ibid.

[239] *Meta Platforms Inc. & Ors. v Bundeskartellamt*, Case C-252/21.

[240] Anadi Tewari, 'A Critical Evaluation of India's Proposed Digital Competition Act' (2024) 5(1) Competition Commission of India Journal on Competition Law and Policy 79, 80 <https://doi.org/10.54425/ccijoclp.v5.197> accessed 13 March 2025.

[241] Ibid.

[242] *Hoffmann-La Roche & Co AG v Commission of the European Communities*, CJCE Case No 85/76 (Court of Justice of the European Union, 13 February 1939).

[243] *Google and Alphabet v Commission*, Case C-48/22 P (European Court of Justice, 10 September 2024).

harmony with competition law, ensuring that personal data exploitation cannot be justified solely on efficiency grounds.

As against this, even though the Indian CCI has been able to deter anti-competitive behaviour effectively, its process of enforcement is slower and more uncertain, particularly in advanced digital marketplace matters.[244] The interaction between competition and data protection law in India remains underdeveloped, as the CCI has not yet established a consistent framework for evaluating how misuse of personal data may constitute abuse of dominance.

D. Objective Justification and Flexibility

Both regimes permit leading companies to raise objective justifications in limited situations. The EU's case law has nonetheless developed to require a strict test so as to make certain that any pro-competitive gain does not undermine the general integrity of the market.[245] In the specific context of data protection, companies in the EU must show that their processing of personal data is strictly necessary for the performance of a contract or a legitimate interest under the GDPR, which is scrutinized alongside competition principles.

India, by contrast, focuses on balancing competitive fairness with market pragmatism, consistent with its general policy of economic liberalization and gradual reform.[246] Under the DPDP Act, 2023, certain legitimate uses of personal data are allowed, but the lack of explicit integration with competition law makes the Indian system more fragmented and less rigorous in comparison.

Overall, though the EU and India both seek to avoid market abuse of dominance, the EU is more active and centrally directed - particularly in the digital market - and explicitly integrates data protection principles into its competition framework. India is still developing its regulatory strategy, both in terms of competition law and data protection, and has yet to fully establish the institutional and legal mechanisms that ensure privacy and fair competition are addressed in a coherent and complementary manner. This comparative review therefore highlights not only the divergence in enforcement styles but also the critical gap between the EU's mature integration of data protection with competition law and India's emergent dual-track approach.

VI. DATA GOVERNANCE IN THE AGE OF ARTIFICIAL INTELLIGENCE

[244] Anadi Tewari, 'A Critical Evaluation of India's Proposed Digital Competition Act' (2024) 5(1) Competition Commission of India Journal on Competition Law and Policy 79, 80 <https://doi.org/10.54425/ccijoclp.v5.197> accessed 13 March 2025.

[245] Ministry of Corporate Affairs, Government of India, *Report of the Committee on Digital Competition Law* (2024), 57 <https://prsindia.org/files/parliamentry-announcement/2024-04-15/CDCL-Report-20240312.pdf> accessed 13 March 2025.

[246] Ibid, 24.

Emerging technologies such as artificial intelligence (AI), machine learning, and blockchain are reshaping the digital economy.[247] These technologies, which rely heavily on extensive datasets and sophisticated algorithms, have profound implications for both data privacy and competition law. AI-driven platforms are capable of processing vast quantities of personal data to predict consumer behaviour, optimize operations, and even influence market outcomes.[248] However, such capabilities pose essential questions about the ethical use of information, algorithmic discrimination, and future market power concentration.[249]

AI systems in particular raise a dual challenge: *first*, they create risks of entrenched dominance where access to large datasets fuels a self-reinforcing cycle of innovation and market power; *and second*, they heighten data protection concerns where automated profiling, facial recognition, and behavioural targeting threaten informational self-determination[250]. The GDPR already addresses some of these issues by granting individuals rights against fully automated decision-making under Article 22[251], but applying these rights effectively in complex AI contexts remains difficult. For instance, algorithmic opacity, or the so-called "black box problem", makes it hard to verify whether AI-driven outcomes are fair, lawful, and non-discriminatory.

From the regulatory side, the EU has taken the lead with the proposed AI Act[252] (expected to come into effect in 2026), which classifies AI systems based on risk categories like unacceptable risk (e.g., social scoring), high risk (e.g., biometric surveillance, credit scoring), and limited/minimal risk. High-risk AI will face strict obligations relating to transparency, human oversight, and accountability.[253] The AI Act thus complements the GDPR and competition law by ensuring that innovation does not come at the expense of fundamental rights or fair market structures. Enforcement will likely require coordination between data protection authorities, competition regulators, and specialized AI supervisory bodies.

---

[247] David Treat and Michael Klein, 'Immersive technology, blockchain and AI are converging – and reshaping our world' (World Economic Forum, 21 June 2024) <https://www.weforum.org/stories/2024/06/the-technology-trio-of-immersive-technology-blockchain-and-ai-are-converging-and-reshaping-our-world/> accessed 14 March 2025.

[248] Ibid.

[249] Nenavath Sreenu and Som Sekhar Verma, 'Enhancing economic growth through digital financial inclusion: An examination of India' (2024) 16(4) Transnational Corporations Review, 2 <https://doi.org/10.1016/j.tncr.2024.200091> accessed 14 March 2025.

[250] Heike Schweitzer, Jacques Crémer und Yves-Alexandre de Montjoye, 'Competition Policy for the Digital Era' (2019) Working Paper No. 6 des Forschungsinstituts für Recht und digitale Transformation, European Commission, 71-75 <https://www.rewi.hu-berlin.de/de/lf/oe/rdt/pub/working-paper-no-6/@@download/file/Schweitzer%20et.%20al.,%20Competition%20policy%20for%20the%20digital%20era.pdf> accessed 22 September 2025.

[251] General Data Protection Regulation, art 22.

[252] The EU Artificial Intelligence Act, Regulation (EU) 2024/1689.

[253] 'The EU Artificial Intelligence Act' EU Artificial Intelligence Act, <https://artificialintelligenceact.eu/> accessed 22 September 2025.

India, by contrast, is still in the process of shaping its AI regulatory framework. NITI Aayog's National Strategy for Artificial Intelligence[254] emphasized AI for social good, while recent initiatives under Digital India focus on AI-enabled governance and ethical AI principles. However, India lacks a comprehensive legislative framework akin to the EU AI Act. Instead, governance is evolving through policy guidelines, voluntary ethical frameworks, and sector-specific applications. The DPDP Act, 2023 provides a starting point by regulating how personal data used for AI training and deployment must be processed lawfully, but the explicit treatment of algorithmic accountability and competition issues is still missing.

In the context of competition law, AI further complicates enforcement. Pricing algorithms can lead to tacit collusion where competitors' systems adjust prices dynamically without explicit agreements, blurring the line between legal parallel behaviour and prohibited cartelization.[255] Similarly, recommendation algorithms and targeted advertising may amplify entry barriers by favouring incumbents with richer datasets.[256] Both EU and Indian regulators are beginning to explore how algorithmic collusion and data-driven exclusionary practices can be tackled through existing abuse of dominance provisions.

Moreover, the application of AI in commercial processes creates new regulatory challenges that traditional legal norms are only beginning to address. Algorithmic transparency, responsibility in computerized decision-making, and the possibility of data abuse present novel regulatory challenges.[257] For instance, regulators are now forced to consider issues of how to make AI systems fair and unbiased, and how to prevent them from inadvertently perpetuating monopolistic market structures. This will also imply assuring that data protection and competition law are inclusive of ethical considerations of AI, as well as digital responsibility.[258]

---

[254] 'National Strategy for Artificial Intelligence' (2018) NITI Aayog, <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf> accessed 22 September 2025.

[255] Frédéric Marty and Thierry Warin, 'Deciphering algorithmic collusion: Insights from bandit algorithms and implications for antitrust enforcement' (2025) 3 Journal of Economy and Technology, 34-43 <https://doi.org/10.1016/j.ject.2024.10.001> accessed 22 September 2025.

[256] Amelia Fletcher, Peter L Ormosi and Rahul Savani, 'Recommender Systems and Supplier Competition on Platforms' (2023) 19(3) Journal of Competition Law & Economics, 397-426 <https://doi.org/10.1093/joclec/nhad009> accessed 22 September 2025.

[257] Nenavath Sreenu and Som Sekhar Verma, 'Enhancing economic growth through digital financial inclusion: An examination of India' (2024) 16(4) Transnational Corporations Review, 2 <https://doi.org/10.1016/j.tncr.2024.200091> accessed 14 March 2025.

[258] Ministry of Corporate Affairs, Government of India, *Report of the Committee on Digital Competition Law* (2024), 98 <https://prsindia.org/files/parliamentry-announcement/2024-04-15/CDCL-Report-20240312.pdf> accessed 13 March 2025.

Regulators must assume more flexible and varied regulatory tools if they are going to be equipped to address rapid technological change.[259] Tests such as regulatory sandboxes - under which new technologies and business models can be tested in safe environments - are an attractive solution. Regulators can learn valuable lessons about the actual consequences of digital innovation without deterring growth from sandboxes.[260] Moreover, cooperation across disciplines between legal experts, technologists, economists, and industry stakeholders is essential to establish robust regulatory instruments that can effectively manage current and future challenges to data governance.[261]

VII. EMERGING CHALLENGES AND FUTURE DIRECTIONS

A. Criticism of the DPDP Act, 2023

The DPDP Act has faced criticism on multiple fronts. First, the Act[262] does not provide compensation to harmed data principals in the case of data breaches, a right that had been granted under the Information Technology Act, 2000[263], and which was enacted under the EU's GDPR[264]. The "Voluntary Undertaking" clause (Section 32[265]) is highly debated, as it enables data fiduciaries to avoid penalties by simply making a self-declared undertaking, potentially weakening enforcement. Additionally, the autonomy of the Data Protection Board has been queried because its members would be nominated by the central government directly, as opposed to the 2019 Bill[266] providing for a selection committee.

The Act also omits the right to data portability and the right to be forgotten, both previously proposed and essential for transparency and individual autonomy and upheld in judgments like Rout v State of Odisha[267]. Finally, governmental exceptions permit the state to process personal data without permission for the reasons of security or public order and create concern of mass surveillance and individual profiling.[268] These criticisms identify important loopholes in the Act that will be able to erode its capability to provide strong data protection.

---

[259] OECD, 'Regulatory Sandboxes in Artificial Intelligence' (OECD Digital Economy Papers No 356, July 2023), 13 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/07/regulatory-sandboxes-in-artificial-intelligence_a44aae4f/8f80a0e6-en.pdf> accessed 14 March 2025.

[260] Ibid, 8.

[261] Ibid, 19.

[262] Digital Personal Data Protection Act 2023.

[263] Ajay Kumar Bisht and Neeruganti Shanmuka Sreenivasulu, 'Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023' Data Privacy - Techniques, Applications, and Standards (IntechOpen 2024) <https://www.intechopen.com/chapters/1190882> accessed 14 March 2025.

[264] General Data Protection Regulation, art 82.

[265] Digital Personal Data Protection Act 2023, s 32.

[266] Personal Data Protection Bill 2019.

[267] *Subhranshu Rout v State of Odisha* 2020 SCC OnLine Ori 878.

[268] Pameela George, 'India's surveillance landscape after the DPDPA' (IAPP, 6 February 2025) <https://iapp.org/news/a/india-s-surveillance-landscape-after-the-dpdpa> accessed 14 March 2025.

B. Enhancing Inter-Agency Coordination

The intersecting jurisdictions of data protection and competition law require greater cooperation between regulatory authorities. Formal cooperation mechanisms - for example, inter-agency working groups, coordinated investigations, and common data analysis procedures - will be necessary to ensure that action in one field does not unwittingly compromise the goals of the other. This type of coordination can help in the establishment of a better argument for an integrated regulatory framework for addressing the complexity of the digital economy in a stronger manner.[269]

C. Addressing Regulatory Arbitrage and Ensuring Global Compliance

The borderless nature of digital information inherently ensures that regulatory arbitrage is an ongoing challenge. Differences in national regulatory regimes can be utilized by businesses to construct market leadership or evade regulation.[270] India will thus have to upgrade its standards to the international best-practice level and internalize them in accordance with local requirements.[271] Facilitating active interaction among international regulatory bodies to reduce heterogeneity across national regimes and make Indian digital markets competitive and robust is possible.[272]

D. The Impact of Quantum Computing on Data Security and Privacy

As quantum computing moves from theory to practice, its impact on data security cannot be overemphasized. Quantum computers possess unmatched computing abilities, which will democratize data analysis but also make existing cryptography methods obsolete. In data privacy, the emergence of quantum computing would make many traditional security measures redundant, thus opening the need for designing quantum-resistant algorithms. This technological change will have implications for both data protection and competition law, since the capacity to process and analyse data at quantum speeds can create new types of market advantage and compound fears of monopolies of data.[273]

E. The Proliferation of Internet of Things (IoT) Devices

The pervasive growth of the Internet of Things *(IoT)* brings new levels of sophistication to the world of data. With billions of devices networked - from appliances in the home to sensors in

[269] Ibid, 40.
[270] Ibid, 59.
[271] Ibid, 62.
[272] Ibid, 63.
[273] Ankit Singh, 'The Impact of Quantum Technology on Data Security' (AZO Quantum, 29 May 2024) <https://www.azoquantum.com/Article.aspx?ArticleID=524> accessed 14 March 2025.

industry - data is being produced at an unparalleled rate. This development poses inherent issues concerning the collection, storage, and utilization of individuals' personal information and complicates common perceptions of privacy. Consolidation of data from different IoT devices can, in competition law terms, aid the concentration of market power by incumbent firms in novel ways. Regulators will have to develop regulation that addresses the specific challenge of the IoT ecosystem while not fettering innovation through overzealous data protection.[274]

At the global level, new technologies and digital innovation increasingly transform the competitive landscape. Regulatory policies in advanced economies increasingly are taking proactive measures to balance data privacy and competition concerns. What can be learned from these markets - from the United States to the European Union - is the need for an anticipatory regulatory strategy that is capable of responding to evolving rapid technological change. For India, it will be important to align with these international trends while responding to domestic realities in order to create a competitive and secure digital economy. International dialogue and cooperation will also be needed to continue addressing challenges that cross national borders, including cyber threats and data breaches.

F. Interdisciplinary Approaches for Future Regulatory Synergies

Convergence of digital technologies in the future requires transdisciplinary solutions involving law, economics, computer science, and public policy knowledge. Collaborative research studies, academic symposia, and cross-sector collaborations can be used to craft innovative regulatory responses that are flexible and resilient. These cross-disciplinary initiatives must work towards bringing theoretical models and real-world enforcement closer to each other, so that regulatory schemes can continue to be effective in a period characterized by sudden technological changes. These collaborative efforts will be crucial to designing policies that not only safeguard individual rights but also ensure a fair playing field in the digital market.

G. Future Policy Recommendations

Based on the comprehensive analysis provided above, the following policy suggestions are made to develop a robust regulatory framework in India for the future:

i. Develop an Integrated Regulatory Framework: Establish common guidelines that harmonize the needs of data protection and competition law. The framework should

[274] Sachin Kumar, Prayag Tiwari and Mikhail Zymbler, 'Internet of Things is a Revolutionary Approach for Future Technology Enhancement: A Review' (2019) 6 Journal of Big Data 111 <https://doi.org/10.1186/s40537-019-0268-2> accessed 14 March 2025.

merge the key statutory provisions of the Competition Act, 2002 and the DPDP Act so that the regulatory provisions are aimed at complementing one another.

ii. Invest in Regulatory Infrastructure: Enhance the strength of the CCI as well as the proposed Data Protection Authority by investing in technology, training, and cross-disciplinary research. Better infrastructure will enable regulators to carry out sophisticated data analytics and economic analysis in digital markets.

iii. Foster Interdisciplinary Research and Collaboration: Invite collaborations between regulatory agencies, industry players, and academic institutions. These research collaborations can lead to innovative regulatory designs that meet the complex challenges in the intersection of privacy, competition, and new technologies.

iv. Promote Transparency and Public Accountability: Make regulatory processes and enforcement action transparent and publicly accountable, which helps to build business and consumer confidence.

v. Encourage International Regulatory Dialogue: Actively engage in international and bilateral negotiation to coordinate regulation and prevent regulatory arbitrage.

vi. Adopt Flexible and Adaptive Regulatory Tools: Leverage regulatory sandboxes and pilot schemes to conduct experimental trials of new policies in real time so that the legal framework remains adaptive to technological advancement.

VIII. COMPARATIVE CASE STUDIES AND SECTOR-SPECIFIC IMPLICATIONS

A. E-Commerce and Digital Advertising

The e-commerce sector points out the complex interplay between competition law and data privacy. Large e-commerce platforms accumulate huge consumer data to facilitate efficiencies in logistics, customize customer care, and simplify operations.[275] While such strategies enhance operating performance, they also create formidable barriers to entry for smaller competitors.[276] Extensive research within the marketplace indicates that non-discriminatory algorithmic regulation and open data practices are crucial to maintaining the competitive equilibrium. Regulatory steps which mandate disclosure of usage practices and provide mechanisms for consumer redress have proved to be promising in lowering anti-competitive behaviour without hindering innovation.[277]

[275] Competition Commission of India, *Journal on Competition Law and Policy*, vol 1 (December 2020), 53 <http://164.100.58.95/sites/default/files/whats_newdocument/Volume1-Dec-2020.pdf> accessed 14 March 2025.
[276] Ibid, 54.
[277] Ibid, 55.

B. Financial Services and Fintech Innovations

The financial industry, driven by fast-paced fintech evolution, also poses regulatory concerns at the nexus of data privacy and competition law.[278] Fintechs place extensive dependence on consumer data to provide customized services, assess risks, and enable digital payments.[279] But problems like data leakage and market concentration of market leaders need to be seriously addressed through regulation.[280] Here, the regulatory bodies have to walk a tight rope - facilitating fintech innovations to grow while having strict data protection and competitive fairness laws.[281] Industry case studies indicate the necessity of strong and dynamic regulatory frameworks, which allow for rapid innovation without infringing on consumer rights or market integrity.[282]

IX. CONCLUSION

The convergence of data protection and competition law in India is a multilateral regulatory problem reflecting broader digital transformations. Decisive verdicts like that in the Puttaswamy case, and the dynamic implementation of the Competition Act, 2002, have reflected India's commitment to individual freedoms and market fairness as its data management and competitive forces transform with previously unseen velocities in AI, quantum computing, and IoT. The article sketched the development of these areas of law, surveyed their interfaces, and examined regulatory and judicial reaction to digital dominance. It contrasts India's response with international paradigms - above all, the EU model - and charts emerging challenges and avenues for future research. In-depth case studies of e-commerce, digital advertising, and fintech also underscore the need for comprehensive, forward-looking strategies in a changing digital landscape. Policy suggestions emphasize inter-agency coordination, international cooperation, cross-disciplinary research, and forward-looking regulation. Through an integrated, responsive strategy, India can safeguard consumer privacy, promote fair competition, and encourage innovation. Ultimately, the intersection of data protection and competition law represents an opportunity to redefine the legal landscape for the digital economy. As India emerges as a global digital economy, collaborative and innovative regulatory direction is required for a vibrant, inclusive, and globally competitive marketplace.

---

[278] Nenavath Sreenu and Som Sekhar Verma, 'Enhancing economic growth through digital financial inclusion: An examination of India' (2024) 16(4) Transnational Corporations Review, 2 <https://doi.org/10.1016/j.tncr.2024.200091> accessed 14 March 2025.
[279] Ibid, 3.
[280] Ibid, 4.
[281] Ibid, 5.
[282] Ibid, 6.