INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 2 | Issue 4 [2024] | Page 212 - 227

HARMONIZING COMPETITION AND DATA PRIVACY: ADVANCING REGULATORY COLLABORATION IN DIGITAL MARKETS

- **Madhav Goswami[1] & Vaishnavi Sharma[2]**

ABSTRACT

The Digital Personal Data Protection Act (DPDP) and the Data Protection Board's subsequent creation raise the possibility of conflicts between the Board and the Competition Commission of India (CCI) over data and competition problems. This regulatory overlap may go beyond jurisdictional issues and give rise to particular disputes in which advancing competition in a data-driven market can come into conflict with the goal of data protection. This paper provides a summary of previous regulatory disputes in India as well as the strategies used to settle turf wars. It highlights the necessity of an efficient system centred on coordination and cooperation across regulators to address issues, given the lack of cogent procedures in the past. By presenting this framework, the study emphasizes how crucial it is to balance data protection and competition in order to get the best possible result that protects user privacy and promotes competitive marketplaces.

Keywords: *DPDP, CCI, Data Protection Board, Coordination, Disputes.*

INTRODUCTION

The well-known difficulties presented by data-driven digital platforms have been brought to light by the recently filed civil antitrust action against Apple Inc. The Department of Justice (DOJ) brought two similar antitrust claims against Google in 2023, claiming that the company has an

[1] B.COM. LL.B. (Hons.) - V Year, Institute of Legal Studies and Research, GLA University, Mathura.
[2] BBA.LL.B. (Hons.)- V Year, JECRC University, Jaipur.

unfair competitive advantage in the digital market due to its use of user data to dominate the ad tech industry and its prioritization of its own services in search results. The accusations made against these internet behemoths highlight how important data is in online marketplaces. Data plays a complicated and quickly changing role with significant ramifications for both consumers and corporations. The price has historically been used as a metric to quantify customer welfare in competitive literature. However, the way that consumer welfare is assessed in data-driven marketplaces has undergone a significant conceptual change. It is increasingly evaluated based on data accessibility, usage, and gathering. The realization that data has a major impact on market competition dynamics is what is driving this shift. Moreover, the information asymmetry is produced by vague, intricate, and lengthy consent terms for data collecting, which predominantly benefit dominant digital platforms. Second, companies may learn about the preferences and interests of their customers thanks to consumer data, which makes platforms to maximize the experience of the user. On the basis of statistics, this adds to network effects that raise entry barriers, which affects market competitiveness. companies that rely on data to make decisions use zero-price tactics, which influence customer behaviour and provide companies with big datasets an unfair edge. In the long run, using data in this manner damages citizens' privacy and presents anti-competitive issues. Because of these concerns, lawmakers and regulators are now closely examining data-driven business models and the market dynamics of digital platforms. The historic 2019 Facebook decision provides an example of what updated antitrust laws taking data-related issues into account might look like. However, a revised legal toolkit would actively strive to reform the regulatory environment for effective implementation, in addition to requiring antitrust law to take into account data protection-related problems, such as lack of user control over personal data. The Data protection regulators and competition regulators will have to collaborate closely. It would call for the creation of a regulatory framework that recognizes these overlaps and, when appropriate, makes use of data protection principles. This strategy is based on well-established procedures in other regulatory areas; for instance, banking and finance are governed by a number of regulators, including securities and insurance watchdogs as well as central banks. In terms of adopting and executing an examined regulatory strategy, India lags behind. Due to previous problems in India, where ambiguous jurisdictions and a lack of a structure for regulators to confer on overlapping concerns, establishing such an approach is especially important. Issues have led to turf wars. These disputes, like the one over banking merger control between the Competition Commission of India (CCI), a cross-sectoral regulator, and the Reserve Bank of India (RBI), a sectoral regulator, have caused a great deal of uncertainty and delays, with costs to the market, the regulated entities, and the regulators. There is presently no roadmap to direct this process, despite

the CCI's recent recognition that privacy and data protection issues need to be incorporated into the framework of competition policy. Data concerns are not even covered by the planned Competition (Amendment) Act 2023.

It is anticipated that the Digital Personal Data Protection Act would have a major influence on digital business models and the dynamics of competition. Coordination of regulations will probably be more difficult when it comes to data-related competition problems. Both regulators in this case, i.e., the CCI and the Data Protection Board created by the Digital Personal Data Protection Act are cross-sectoral, in contrast to other conflicts between sectoral and cross-sectoral regulators. Therefore, it is essential to take a synergistic approach to digital antitrust. In order to extract principles to promote competitive digital markets, this paper will offer broad-level recommendations for preventing and addressing regulatory conflicts between the CCI and the Data Protection Board, building on our work on a normative framework for competition regulation and data protection overlaps in India.

INDIA'S REGULATORY TURF BATTLES: EXAMINING THE CAUSES AND CONSEQUENCES: -

This section focuses at the causes of regulatory turf wars and the ensuing cost externalities that affect the market and enterprises. An analysis of Indian case histories shows that overlapping jurisdictions, different interpretations of legislative requirements, and jurisdictional inconsistencies in legal interpretations are the main causes of these conflicts. The main causes of regulatory conflicts, backed by case studies, are listed below:

1. LEGISLATIVE AMBIGUITY THAT RESULTS IN A WIDE JURISDICTIONAL OVERLAP:

Each regulator's unique legislation has ambiguous language that causes overlapping jurisdiction and makes it difficult to distinguish one regulator from another. For regulators, this ambiguity difficulties while putting policies in place to resolve conflicts that emerge between market players. Regulatory disputes in India are largely caused by unclear guidelines regarding the roles of each agency. Here are two notable historical examples:-

A. The Petroleum and Natural Gas Regulatory Board (PNGRB) and CCI [2011]:-

With the main goal of overseeing the petroleum and natural gas industry in India, the PNGRB was founded in 2006 under the Petroleum and Natural Gas Regulatory Board Act.

Its mission is to protect the interests of consumers by encouraging fair trade and a healthy level of competition among businesses in the industry. This duty is comparable to the CCI's overarching mandate to control competition in all national sectors.
Reliance complained to the CCI in 2011 that its competitors, Hindustan Petroleum, Bharat Petroleum, and Indian Oil Corporation, had organized a cartel to provide aviation fuel to Air India. The three businesses contested the CCI's jurisdiction over the dispute during the investigation. They subsequently complained to the Delhi High Court, arguing that the PNGRB had jurisdiction over the case. It was unclear whether authority was best suited to handle the situation because of the two regulators' wide overlapping jurisdiction.
claimed anti-competitive actions by market players. They subsequently complained to the Delhi High Court, arguing that the PNGRB had jurisdiction over the case. It was unclear whether authority was best suited to handle the situation because of the two regulators' wide overlapping jurisdiction claimed anti-competitive actions by market players. Even though the PNGRB Act did not give the sector regulator exclusive authority, the High Court granted an interim ruling declaring that the CCI lacked jurisdiction over the case. This ruling cast doubt on the CCI's ability to regulate the petroleum and natural gas industry and weakened its authority. Additionally, it made market players hesitant, which affected investments and made it more difficult for the sector to run smoothly.

B. CCI and Telecom Regulatory Authority of India (TRAI) [2017]:-

The Telecom Regulatory Authority of India Act of 1997 created the TRAI in order to foster competition and guarantee the expansion of the Indian telecom industry. Another legislative obligation that TRAI shares with the CCI is to provide a framework that promotes fair competition in the market. Reliance Jio complained to the CCI in 2017 about alleged cartelization by Vodafone, Airtel and Idea, the leading telecom providers in the sector. The incumbents contended that the TRAI, as the sector-specific regulator, was the proper body to handle matters pertaining to telecommunications services and contested the CCI's jurisdiction to look into the case. The Supreme Court of India heard this case and decided that the TRAI has the authority to initially ascertain the parties' rights and responsibilities. The CCI's authority would then be used if the TRAI thought that anti-competitive behaviour had taken place. The prolonged court disputes and the ensuing ambiguity affected the nation's regulatory environment and created an uneasy business climate for the telecom sector.

2. A COMMON LEGISLATIVE LANGUAGE RESULTING IN JURISDICTIONAL OVERLAP:

A more focused legislative overlap, as opposed to a general mandate, is the second cause of regulatory conflict. It happens when the sectoral regulator is given the legislative power to monitor and deal with "anti-competitive behaviour" in the market. They do this by using language that is exactly the same as the Competition Act and by imitating the CCI's function. We have entailed three well-known instances of this kind of dispute which are entailed as follows:-

A. CCI and Delhi Electricity Regulatory Commission [2017]:-

The Delhi Electricity Regulatory Commission (DERC) is empowered by the Electricity Act of 2003 to order a licensee to stop entering into agreements or abusing its dominant position in a way that would negatively affect competition in the electricity industry. The CCI's legislative authority is almost the same as these. The CCI accused BSES Rajdhani Power, Yamuna Power, and North Delhi Power of abusing their dominating positions by participating in unfair and discriminatory conduct in notices sent out in 2017. The DERC questioned the CCI's intervention, claiming that the power Act gave it the authority to deal with market participants' anti-competitive behaviour in the power sector. The distinct tasks that two regulators are supposed to play are blurred when they have the same statutory obligations, which raises the possibility of regulatory conflicts. This case went to court, which decided that the DERC should handle certain technical and sector-specific electricity-related concerns first, followed by the CCI. The CCI's authority was weakened by this decision, and market players were left in the dark by the protracted legal dispute. This case went to court, which decided that the DERC should handle certain technical and sector-specific electricity-related concerns first, followed by the CCI. The CCI's authority was weakened by this decision, and market players were left in the dark by the protracted legal dispute

B. CCI and Securities and Exchange Board of India (SEBI) [2021]:-

Under the SEBI Act of 1992, SEBI was founded. The purpose of this Act is to prevent unfair trading practices through SEBI's regulatory framework. In "[inspecting], [investigating], and [initiating] proceedings against credit rating agencies," SEBI also takes on a supervisory function. The CCI's duties and those of the legislature intersect. The National Highway Authority requested bids from many credits rating companies, including CRISIL, India Ratings and Research, CARE Ratings, and ICRA, in 2021 in order to rate its bonds. An informant complained to the CCI after the agencies submitted proposals with comparable prices. However, SEBI argued that the issue

was within its regulatory jurisdiction and objected to the CCI's jurisdiction. Citing its mandate to look into anti-competitive conduct in all sectors, including those governed by other statutory authorities, the CCI moved forward in spite of SEBI's objections. This issue came from the CCI and SEBI, two regulators, having essentially the same legal language, which confused their respective functions. Both the market participants and the regulatory environment were impacted by this conflict.

C. CCI and RBI [2013]:-

The Reserve Bank of India Act of 1934 established the RBI. Apart from governing the nation's monetary policy, the RBI is also in charge of overseeing the banking industry in India and managing bank mergers and acquisitions as well as those of their subsidiaries. The RBI has argued that the banking industry should be exempt from the competition commission's purview, particularly when it comes to mergers and acquisitions, since it is thought to possess the necessary knowledge and skills to handle such issues. Due to the denial of this motion, there were instances in which the RBI and CCI shared concurrent jurisdiction over bank mergers and acquisitions. However, the government finally made an exception for Regional Rural Banks (RRB) established under the RRB Act of 1976 in 2017. These banks would be exempt from CCI approval for five years in order to merge. The decision to reduce the number of regulatory approvals was decided in the public interest, given the strain on the banking industry.

3. SECTORAL REGULATORS AND THE CCI (HORIZONTAL REGULATOR):

The establishment of a free-market economy and the protection of market competition depend heavily on competition legislation. To handle complex, industry-specific problems, sectoral regulators have been established in India's market-driven economy. With its "ex-ante regulatory" approach, these regulators foresee possible problems and take action before they materialize. Sectoral regulators use this strategy to force market participants to behave in a particular manner and concentrate on "attenuating the effects of market power" by supporting the structured growth of their specific industries. The CCI, on the other hand, takes a "ex-post regulatory" stance and deals with problems that emerge when market actors' actions affect competition. By using this strategy, the CCI aims to address market participants' misuse of their dominating power. The CCI and sectoral regulators have different statutory responsibilities, but they both seek to improve economic performance and avoid market power concentration. Conflicting rulings and

interpretations of matters pertaining to competition may result from the different ex-ante and ex-post regulatory methods. As a result, it may become more difficult for market participants to predict and conform to regulatory expectations, which could negatively affect the formation of a predictable regulatory environment and reduce the effectiveness of competition policy. Consequently, this could hinder equitable competition, impact market dynamics and regulatory legitimacy, and compromise the overarching objective of cultivating a competitive market.

COMPREHENDING THE CONTRAST: DATA PROTECTION AND COMPETITIVE GOALS

A major component of consumer trust in digital marketplaces is data security. It includes safeguards to keep private information safe from abuse, breaches, and illegal access. The EU's General Data Protection Regulation (GDPR) and other regulatory frameworks place a strong emphasis on individual privacy rights while enforcing strict guidelines for data collection, processing, and storage. These guidelines seek to stop abusive behaviour while encouraging accountability and openness in the use of data. Competition law, on the other hand, works to prohibit anti-competitive practices like monopolies and market abuse in order to guarantee fair competition for businesses. Competition authorities concentrate on preventing activities that hinder innovation and consumer choice in the digital sphere, such as unfair data access limitations, data-driven market domination, and exclusionary strategies.
There is a conflict between fostering competition and protecting privacy when data protection regulations are unintentionally weakening established companies, stifling innovation, or erecting obstacles for smaller businesses. In order to balance competitiveness and data privacy, a forward-thinking approach that puts customer welfare, innovation, and trust first is necessary. By adopting cooperative regulatory structures, utilizing technology, and encouraging global collaboration, policymakers can successfully negotiate the intricacies of digital marketplaces. In the end, managing the intensity of disputes guarantees that the two objectives of good data protection and competitiveness are mutually reinforcing rather than antagonistic.

TYPES OF CONFLICTS IN THE CONTESTABLE MARKETS

Conflicts between sectoral and cross-sectoral regulators, as previously said, hinder the efficient operation of the market and impose real costs on consumers and enterprises. Because both the CCI and the Data Protection Board are cross-sectoral regulators, data-related competition issues are anticipated to present even more regulatory coordination challenges. Due to requirements in

the Digital Data Protection Act and possible market-related concerns, this section will categorize the many conflict scenarios that may emerge in the fields of data protection and competitiveness. The setting for the analysis will be the search engine market, and it will be grounded in the contestable market theory.

(A): Data security and competitive effects resulting from the state of the law

1. Required consent for the acquisition of data: According to the DPDP Act's Section 6, sub-section 1, Data Fiduciaries must first get the Data Principals' "free, specific, informed, unconditional, and unambiguous consent" before gathering, using, or disclosing their personal information. By providing more authority to data principals throughout data processing and fostering transparency, this clause makes getting consent the legal basis for all data-related activities. Nonetheless, incumbent companies may have a major edge over more recent rivals thanks to this clause. Due to the additional "barrier" of gaining agreement and creating databases, which incumbents with established databases might not face, potential entrants in the market may confront obstacles to entry.

2. An Exception to the requirement for consent for data collection: The DPDP Act also specifies exceptions to obtaining consent before collecting data under Section 7, Subsection B. Although most of the time, data fiduciaries must obtain consent before using data, government organizations, their agents, and companies that handle data for "National Security" purposes are excluded from this rule and do not have to ask customers for consent. Consumer data privacy suffers when an exception to the law requiring consent is introduced. By keeping and using data for purposes other than those listed, it gives organizations who handle it the chance to take advantage of it. Data principals may lose control over their data as a result of power asymmetries between data fiduciaries and principals, which is a violation of their right to privacy. Additionally, the exception to this requirement has detrimental effects on competitiveness. The probability of database aggregation may increase as a result of the public sector actors' higher exemptions for data processing compared to private sector enterprises.

3. Notice must be given before data is collected and processed: According to the DPDP Act's Section 5, Subsection 1, data fiduciaries must notify data principals before requesting their consent to process personal data. It is required that this notice include precise information about the personal information that will be gathered and the reason for processing it. In terms of data protection, such comprehensive information helps consumers by limiting potential for data exploitation and increasing processing procedure transparency. Due to the

rigorous standards that data fiduciaries must meet for the handling and use of personal data, this transparency in turn fosters confidence between data principals and fiduciaries. Although this clause protects customer privacy, it also imposes fees and compliance requirements on new companies. These expenses could include legal advice to make sure the notification conforms with the law and administrative charges for keeping notices current and handling requests from data subjects.

4. An Exemption to the notice requirement for data collection and processing: The Central Government may exclude specific data fiduciaries or classes of data fiduciaries, including particular startups, from certain requirements pertaining to the provision of a notice for the purpose of data collecting under Section 17, Subsection 1 of the DPDP Act.
This clause's exception may reduce openness and lead to power disparities between fiduciaries and data principals. Data protection opportunities may suffer if accountability procedures for organizations managing personal data are weakened. Additionally, the exception to this clause has detrimental effects on competitiveness. Companies in the public sector could be able to outperform those in the private sector, which are probably going to encounter more regulatory obstacles.

5. Reporting of personal data breach by all firms: Every personal data breach must be promptly reported by data fiduciaries to the Data Protection Board of India, along with details about the impacted data principals, according to Section 8, Subsection 6 of the DPDP Act.
Data protection benefits from this clause since it guarantees that data principals are notified of any infractions, enhancing transparency and giving them more authority over their data. However, there are detrimental effects on market competitiveness from this clause. Rapid data breach detection may necessitate technology investments, such as putting privacy-by-design principles into practice, which smaller businesses may not be able to pay. Companies may also favour bigger organizations with better breach prevention capabilities for processing second-hand data, which could result in data concentration among a small number of key participants. The possibility of concentration may make fair competition more difficult, even though data gathering is not always an obstacle to entry.

6. Redress of grievances by a Data Fiduciary: According to the DPDP Act's Section 13, Subsection 1, data principals have the right to file a grievance redressal if the organizations that handle their data don't follow data protection guidelines. By giving data principals efficient ways to handle issues pertaining to their data, this clause seeks to empower them. By creating

accountability through the implementation of fines for non-compliance, data fiduciaries and consent managers are incentivized to establish and uphold strong standards for the protection of personal data. Nonetheless, larger companies may find it easier to comply with the regulations than smaller companies because they have more financial and technological resources. This can therefore result in increased entry barriers and less market competitiveness.

(B): Competitive consequences resulting from market dynamics and data protection

1. Data Portability for Businesses: By reducing the strain on data transfers, data portability would allow customers to quickly move between providers and take their data with them. While the lack of this clause has little effect on data security, it has a big impact on market competition. Greater control over data would probably be provided by a data portability provision, which would improve data protection by giving people more authority over their data. In contrast, the absence of this clause could have a detrimental effect on market competitiveness. High switching fees between service providers may result in customer lock-in, which deters users from moving because they are afraid of losing their data. Customer lock-in like this could make the market more vulnerable to dominant players' exclusionary tactics. The market's competition is also harmed when businesses have consumer security since switching is expensive. The idea is that behavioural, legal, and technological obstacles could appear not just while gathering data but also when storing and using (analysing) it. Therefore, rather of focusing only on gathering vast amounts of data, regulators should make sure that consumers can freely switch products or platforms at anytime, anyplace. By lowering switching costs and minimizing potentially dangerous network effects, adding a data portability clause would improve the Act, which in turn, threatens competition in the marketplace.

2. Data-driven marketplaces through Mergers and Acquisitions: It is not specifically forbidden by the DPDP Act for organizations with similar data-driven operations to consolidate. An example is the Facebook-WhatsApp merger, in which WhatsApp notified Facebook that it intended to share user data. Without such a clause, people's rights to data privacy in the marketplace are compromised. Businesses can consolidate their market dominance by gathering more consumer data by permitting mergers between similar data-driven companies. Due to the difficulty new companies have gaining enough critical mass to enter the market, this concentration makes it more difficult for more effective newcomers to overtake incumbents. Additionally, companies with a competitive edge and improved customer service are those who make use of

prior data and patterns that are unavailable to new rivals. This further hinders market competition and increases entry barriers.

3. Search results are being manipulated by a large tech platform to the advantage of platform users: Current market participants who manipulate outcomes for their own subsidiary companies restrict consumer choice and enable companies to erode competition and data protection rights. To prioritize its own goods and services, for example, Google altered its search engine algorithm, frequently at the expense of rivals and outside websites. By strategically utilizing its supremacy as a search engine, Google was able to nearly five times its income and drastically reduce market competition. A user would need to navigate 42% of the way down the page to get to the first "organic" search result, according to a research. By implementing an improved notice and consent process based on user opt-in, Apple has also made it far more difficult for third-party apps to gather data, while exempting its own apps from this requirement. Giving larger companies the freedom to set their own data gathering compliance standards increases entry barriers and may force smaller companies out of the market.

IMPACT OF CONFLICT SEVERITY ON DATA SECURITY AND COMPETITION OBJECTIVES

Market structure, legal frameworks, and the degree of data dependency in business models are some of the variables that affect how serious conflicts are between data security and competitive goals. From minor tensions where changes can be made without causing significant harm to serious conflicts that could jeopardize the objectives of competition or privacy, conflicts can take many different forms.

(A): Conflicts of Low Severity: Complementary Modifications

Competition and data privacy goals can coexist with small regulatory changes in low-severity conflict situations. Requiring transparency in data-sharing agreements, for instance, may improve competitiveness by levelling the playing field and safeguarding consumer privacy. Smaller businesses can compete with data-rich incumbents in these situations by implementing focused actions, such requiring interoperability standards, without jeopardizing user privacy.

(B): Moderate-Severity Conflicts: Balancing Trade-Offs

Trade-offs are a common feature of moderate conflicts. Data portability rights, for example, which are intended to empower consumers under privacy rules, may unintentionally benefit dominating platforms. While allowing consumers to share their data increases consumer choice, it can also provide companies that can better exploit this data at scale a stronger competitive edge. Legislators must create regulations that promote competitiveness without compromising privacy norms. One way to lessen these dangers is to develop neutral data portability platforms.

(C): Conflicts of High Severity: Zero-Sum Conundrums

In high-severity conflicts, accomplishing one goal compromises the achievement of the other. Competition authorities might, for instance, require competitors to share data in order to stop market domination. However, this kind of sharing could violate data security rules by disclosing private information. Damage management becomes the regulatory focus in these circumstances, necessitating strong safeguards and compromise measures.

Furthermore, the Global economic landscape has changed due to the quick growth of digital markets, which has created a lot of room for innovation and development. On the other hand, it has also created a number of difficulties that call for cautious regulatory action. Among these difficulties, the confluence of data privacy issues and competition goals is especially important. As policymakers work to reconcile these frequently at odds goals, the degree of conflict that results from their interaction becomes a critical factor in determining the regulatory outcomes. One instance of a high-severity dispute is Google's acquisition of Fitbit. Critics raised privacy concerns by claiming that the acquisition will provide Google access to private health information. Authorities in charge of competition were also concerned about Google's increasing hegemony in the digital market. In an effort to strike a balance between privacy and competition, regulations have responded by enforcing restrictions on data usage. Nonetheless, the case demonstrates how regulatory skills are strained by such conflicts. Moreover, the concerns have also been raised about Meta's (previously Facebook) exploitation of data to sustain its supremacy. Mandates for interoperability present serious privacy concerns, but they may also increase competition by enabling smaller firms to interact with Meta's platforms. User trust could be weakened by unauthorized data access during integration. The necessity of cooperative regulatory approaches that address issues of data security and competition is highlighted by this case. A Low-to-Moderate conflict is exemplified by the EU's GDPR. Even if GDPR improves privacy, small businesses and startups are disproportionately affected by the expenses of compliance, which lowers competition.

With greater resources, larger companies can adjust more readily and solidify their market positions. Strict privacy laws might have unexpected repercussions, which emphasizes the need for complex rules that safeguard privacy while assisting smaller players. Conflict severity has a significant impact on data security and competition goals, influencing how regulations for the digital market are developed. Regulators are faced with the difficulty of striking a balance between these conflicting priorities when tensions escalate. Low-severity disagreements can be resolved in complementary ways, but high-severity conflicts require creative thinking and teamwork.

SUGGESTIONS FOR HANDLING THE SITUATION OF CONFLICT SEVERITY EFFECTIVELY

1. Cooperation in Regulatory Structures: Businesses, stakeholders, and regulators must work together to manage conflicts effectively. Regulators of competition and data privacy must cooperate to align their objectives. Shared expertise and coordinated enforcement are made possible by joint task forces, as observed in certain jurisdictions.

2. Innovation-Based Solutions: Innovations in technology can lessen conflict. Data sharing is made possible by privacy-enhancing technologies (PETs) like federated learning and differential privacy, which preserve individual privacy. These solutions offer a compromise that allows businesses to compete on insights derived from data without going against privacy standards.

3. Regulations Particular to a Sector: Industry-specific regulations can be tailored to solve particular problems. For example, because of the sensitive nature of the data involved, healthcare and financial services need to have more stringent data protection. Acknowledging the diverse effects of data security on competitiveness across industries guarantees appropriate regulatory reactions.

4. International Standards and Cooperation: International cooperation is necessary since digital markets are global in scope. By harmonizing competition and data privacy rules across jurisdictions, regulatory fragmentation and compliance requirements are decreased. Global standards alignment initiatives include the OECD's guidance on cross-border data transfers.

5. Adaptable Rules and Sandbox Settings: Regulatory frameworks must be flexible in light of the quickly changing digital landscape. Regulatory sandboxes offer valuable insights into potential

conflicts by allowing corporations to explore innovative models under supervision. Policymakers can update legislation based on actual results thanks to dynamic regulations.

CONCLUSION

This paper outlines the main causes of regulatory conflicts in India and their effects on regulators, regulated entities, and the market, drawing from the body of existing literature on the topic. We make three suggestions to lessen the possibility of regulatory conflicts which are entailed as follows:-

1. Clearly defined Roles: In the process of creating regulators, duties are frequently outlined without precise limits or instructions. Clearly defining these elements in the accompanying legislation is crucial to reducing uncertainty in their particular duties, aims, and functions. To guarantee that regulators are held to high standards and held accountable, accountability and transparency procedures must to be put in place. Additionally, by using this strategy, it will be easier to ensure that each regulator fulfils their specific duties. Establishing precise criteria for making decisions about whether there are "sufficient grounds" to move further with an investigation initiated by a Data Principal is necessary, for example, in the case of the Data Protection Board. This precision is essential to preventing ambiguity and maintaining equity in all circumstances.

2. Reduction in the Number of Jurisdictional Overlaps: In India, unclear legislative language is a major cause of regulatory disputes, leading to overlapping jurisdiction and hazy boundaries between two separate authorities. It is essential to take other market regulators' tasks into account when developing legislation in order to avoid conflicting or competing activities. It is crucial to update the law in situations where there is legislative overlap to give regulators direction on how to make the required compromises to settle conflicts. Regarding anti-competitive actions, for example, the Delhi power Commission asserted jurisdiction over the power industry, although the CCI oversees competition in all industries. Including precise instructions, like which regulator should look at a case first, could help with resolution, keep issues from going to court, and save a lot of time and money.

3. Institutionalized and Formalized Coordination System: The Effective Coordination between the regulators should be facilitated in the event of a regulatory conflict via a formal, legally established coordination mechanism. Each regulator's unique roles, responsibilities, and accountability should be clearly mapped out. Establishing a central coordination regulator would

guarantee that regulators can spearhead a concerted attempt to settle a disagreement, upholding this procedure. A "Central Regulatory Coordination Body" would serve as the structure for managing and ensuring the quality of a nation's regulations and regulatory process. Central coordinating regulators have been established in Canada, Chile, Colombia, El Salvador, Mexico, Peru, and the United States. These countries have also witnessed improvements in important areas of national priorities and increased public participation. The creation of a central regulating authority in India could preserve market integrity while expediting the resolution process and saving the courts' time and resources. An overview of previous regulatory disputes in India and the procedures employed to settle them is given in this study. It highlights the necessity for efficient dispute resolution methods in light of the absence of cogent procedures in the past. The goal is to reduce the possibility of conflicts by implementing role clarity and minimizing overlapping jurisdictions. Nevertheless, regulatory disputes could still arise even with effective implementation. Thus, the enforcement of coordination and cooperation procedures among regulators is the main focus of the paper. Finally, it emphasizes how crucial it is to strike a balance between data protection and competition in order to arrive at the best possible solution that preserves user privacy while enabling markets to operate competitively.

REFERENCES

- Arun Sundararajan, *The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism* (2016).
- Maurice E. Stucke & Ariel Ezrachi, *The Rise of Behavioural Discrimination*, 37 Yale J. Reg. 75, 85–87 (2020).
- Pamela Jones Harbour, *The Privacy-Competition Nexus: A Regulatory Perspective*, 43 Harv. J. L. & Pub. Policy 75, 82 (2020).
- Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 585 (2014).
- Michal S. Gal & Daniel L. Rubinfeld, *Data Standardization*, 94 N.Y.U. L. Rev. 737 (2019).
- Jonathan B. Baker, *Beyond Schumpeter vs. Arrow: How Antitrust Fosters Innovation*, 74 Antitrust L.J. 575, 587–89 (2007).
- Inge Graef, *Reconciling Data Protection and Competition Law in Digital Markets*, 8 J. Eur. Competition L. & Prac. 347, 349 (2017).
- U.S. Department of Justice, *Competition and Monopoly: Single-Firm Conduct Under Section 2 of the Sherman Act* (2008).

- Organisation for Economic Co-operation and Development (OECD), *Data-Driven Innovation: Big Data for Growth and Well-Being* 112–18 (2015).
- European Commission, *Shaping Europe's Digital Future*, COM (2020) 67 final, at 19 (2020).
- *Federal Trade Commission v. Facebook, Inc.*, No. 20-3590, slip op. at 15-16 (D.C. Cir. Mar. 25, 2021).
- General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.
- Competition Act, 2002, No. 12 of 2003, § 4 (India).
- Sherman Antitrust Act, 15 U.S.C. §§ 1–7 (1890).
- European Data Protection Board, *Guidelines 8/2020 on the Targeting of Social Media Users* (last visited Nov. 14, 2024), https://edpb.europa.eu.
- Fiona M. Scott Morton et al., *Stigler Report: Committee on Digital Platforms* 75 (Sept. 2019), https://research.chicagobooth.edu/stigler/publications/committee-reports/digital-platforms.
- European Commission, *Merger Control and Privacy: Challenges in the Digital Age*, https://ec.europa.eu/competition (last visited Nov. 15, 2024).
- European Commission, *Google/Fitbit Merger Case Analysis*, Case No. COMP/M.9660, ¶ 56 (2020).
- Google LLC v. European Commission, Case T-612/17, ¶¶ 72–74 (Gen. Ct. 2021).
- Microsoft Corp. v. Commission of the European Communities, Case T-201/04, 2007 E.C.R. II-3601.
- The Petroleum and Natural Gas Regulatory Board Act, 2006, No. 19, Acts of Parliament, 2006 (India).
- The Telecom Regulatory Authority of India Act, 1997, No. 24, Acts of Parliament, 1997 (India).
- The Electricity Act, 2003, No. 36, Acts of Parliament, 2003 (India).
- The Securities and Exchange Board of India Act, 1992, No. 15, Acts of Parliament, 1992 (India).
- The Reserve Bank of India Act, 1934, No. 2, Acts of Parliament, 1934 (India).
- The Regional Rural Banks Act, 1976, No. 21, Acts of Parliament, 1976 (India).
- David McCabe & Tripp Mickle, U.S. Moves Closer to Filing Sweeping Antitrust Case Against Apple, N.Y. TIMES, Jan. 5, 2024.