XPLORE
PUBLICATIONS
www.xplorepublications.com

IJCLR

Chapter 22

Abstract

In: *DSGE 2026 | University of Mumbai (Department of LAW) | IFIM College | Book of Abstract*. ISBN 978-81-992602-2-0.

Data Monopolies and Criminal Abuse of Dominance in Digital Trade

Author- Antra Singh, Student B.A. LL.B. Parul University, Vadodara- antra2114@gmail.com
Co-Author- Amandeep Singh, Student MBL NLSIU, Bangalore- amanlawdelhi@gmail.com

Abstract

The rapid expansion of digital trade has led to the emergence of data-driven markets in which control over data has become a decisive factor in determining market power. This article examines the rise of data monopolies and argues that their dominance extends beyond conventional competition concerns into the realm of criminal liability. Major technology corporations such as Google, Amazon and Meta have leveraged vast data ecosystems, network effects and algorithmic infrastructures to consolidate unprecedented levels of economic and informational control. While existing legal frameworks, particularly competition law, have attempted to regulate such dominance, they largely treat abuses as civil or administrative violations, thereby underestimating the gravity and societal impact of certain digital practices.

This article reconceptualises abuse of dominance in the digital economy by analysing practices such as exploitative data harvesting, algorithmic manipulation, exclusionary conduct and predatory pricing through a criminal law lens. It argues that when such conduct results in large-scale harm affecting consumer autonomy, privacy rights and market fairness it may warrant criminalisation rather than mere regulatory penalties. The study critically evaluates the limitations of existing national and international governance mechanisms, including their fragmented nature and inability to effectively address cross-border digital harms.

In response, the article proposes a hybrid global governance framework that integrates competition law, criminal law and international trade regulation. Such a model seeks to ensure accountability of dominant digital platforms while maintaining a balance between regulation and innovation. By bridging doctrinal gaps between legal regimes, the study contributes to the evolving discourse on digital governance and offers a normative framework for addressing the challenges posed by data monopolies in the global digital economy.

Keywords

Data Monopolies, Abuse of Dominance, Digital Trade, Criminal Liability, Global Governance

Introduction

The expansion of digital trade understood as the cross-border exchange of goods, services and data through digital platforms has fundamentally reshaped the global economic landscape. At the centre of this transformation lies the data economy, where data functions as a critical economic resource, enabling firms to generate value, predict consumer behaviour and consolidate market power. The Organisation for Economic Co-operation and Development has recognised data as a 'core economic asset' driving productivity and innovation in the twenty-first century.[1]

In this context, a small group of multinational technology corporations such as Google, Amazon, Meta and Apple have emerged as dominant actors in digital markets. Their dominance is not merely a function of market share but is rooted in their ability to accumulate, process and control vast volumes of data. Shoshana Zuboff conceptualises this phenomenon as 'surveillance capitalism', where user data is commodified to predict and influence behaviour.[2] This marks a significant departure from traditional industrial monopolies, which were primarily based on control over physical resources or infrastructure.

The emergence of data monopolies represents a structural shift in competition dynamics. These entities benefit from network effects, economies of scale and data-driven feedback loops, which create high entry barriers and reinforce their market position. The United Nations Conference on Trade and Development has observed that a few digital platforms dominate global data flows, raising concerns regarding market concentration and digital inequality.[3] Consequently, traditional competition law tools appear increasingly inadequate to address the complexities of digital dominance.

More importantly, the nature of abuse of dominance in the digital economy is evolving beyond conventional anti-competitive practices. Conduct such as exploitative data harvesting, algorithmic manipulation, exclusionary platform practices and predatory pricing may, in certain circumstances, transcend regulatory violations and assume characteristics of criminal wrongdoing. Classical competition law scholarship, as articulated by Richard Whish and David Bailey, largely treats abuse of dominance as a civil or administrative issue.[4] However, the scale of harm caused by digital platforms impacting privacy, autonomy and democratic processes raises the question of whether certain forms of abuse warrant criminalisation.

Recent global developments, including intensified regulatory scrutiny in the European Union and debates on digital governance reported in leading outlets such as *The Financial Times* and *The Economist*, reflect a growing awareness of the risks posed by unchecked data monopolies. Yet, regulatory responses remain fragmented and jurisdictionally constrained, limiting their effectiveness in addressing cross-border digital harms.

Against this backdrop, this article examines whether existing global governance frameworks are equipped to address the criminal abuse of dominant positions by data monopolies. It argues that such practices cannot be confined to the domain of competition law alone. Instead, a hybrid governance model integrating competition law, criminal law and international trade regulation is necessary to ensure accountability while preserving innovation and economic growth in the digital economy.

2. Conceptual Framework

A. Data Monopolies

Data monopolies refer to the concentration of control over vast datasets in the hands of a few dominant firms, enabling them to exercise significant influence over markets, consumers and competitors. In the digital economy, data is not merely an input but a strategic asset that enhances predictive capabilities, innovation and competitive advantage. The Organisation for Economic

Co-operation and Development recognises data as a key driver of economic activity and market power.[5]

The emergence of data monopolies is closely linked to network effects and economies of scale**.** Network effects occur when the value of a service increases with the number of users, thereby reinforcing the dominance of established platforms. Simultaneously, economies of scale in data collection and processing enable firms to lower marginal costs while expanding their reach. This creates high entry barriers for new competitors. As noted by the United Nations Conference on Trade and Development, a small number of global digital platforms control a significant share of data flows and digital markets.[6]

Prominent examples include platform ecosystems developed by Google, Amazon and Meta, which integrate multiple services search, advertising, e-commerce and social networking into interconnected data-driven environments. These ecosystems enable continuous data extraction and reinforce market dominance, making competition increasingly difficult.[7]

B. Abuse of Dominance

Traditionally, abuse of dominance has been understood within competition law as the misuse of market power by a dominant firm to eliminate competition or exploit consumers. Legal frameworks such as Article 102 of the Treaty on the Functioning of the European Union (TFEU) and similar provisions in national laws focus on practices like predatory pricing, refusal to deal and discriminatory conduct.[8] Scholars such as Richard Whish and David Bailey conceptualise abuse primarily as a civil or administrative wrong addressed through regulatory intervention.[9]

However, in the digital economy, the scope of abuse has expanded significantly. First, data hoarding involves the excessive accumulation and exclusive control of user data, preventing competitors from accessing essential inputs. Second, algorithmic manipulation allows firms to influence consumer choices, search rankings and market visibility, often in opaque and non-transparent ways. Third, exclusionary practices**,** such as self-preferencing and platform bias, distort competition by privileging a firm's own services over those of rivals.

These practices demonstrate that abuse of dominance in digital markets is not merely economic but also informational and behavioural. As Shoshana Zuboff argues, the extraction and control of behavioural data enable firms to shape user conduct, thereby extending their power beyond traditional market boundaries.[10]

C. Criminal Dimension

The evolving nature of abuse of dominance raises a critical question: **when does such conduct transcend civil liability and become criminal?** While competition law traditionally imposes fines and regulatory sanctions, certain forms of abuse may warrant criminalisation due to their intent, scale and societal impact.

Conduct may assume a criminal dimension where there is intentional exclusion of competitors through unfair or deceptive means, predatory pricing with malicious intent aimed at eliminating market rivals, or exploitative data practices that violate privacy and autonomy. These actions may result in widespread harm, including market distortion, consumer exploitation and infringement of fundamental rights.

The distinction between civil and criminal liability lies in the degree of culpability and harm. Civil liability focuses on market correction and economic efficiency, whereas criminal liability emphasises punishment, deterrence and moral condemnation. As noted in Andrew Ashworth's *Principles of Criminal Law*, criminalisation is justified where conduct causes serious harm and involves a high degree of fault.[11]

In the context of digital markets, the integration of criminal law into competition regulation reflects an emerging recognition that certain abuses of dominance are not merely regulatory infractions but socially harmful acts requiring stronger sanctions. This necessitates a rethinking of existing legal frameworks to address the complex interplay between market power, data control and criminal accountability.

3. Digital Trade and Global Governance

The regulation of digital trade within the framework of global governance presents complex legal and institutional challenges. Digital trade, encompassing cross-border data flows, e-commerce and digital services, has increasingly come within the ambit of international trade law. However, existing frameworks were designed for the exchange of tangible goods and traditional services, rendering them only partially effective in addressing the realities of a data-driven economy. The World Trade Organization plays a central role in governing international trade, yet its rules struggle to adequately capture the nuances of digital markets and data flows.[12]

International trade law traditionally focuses on principles such as non-discrimination, market access and fair competition. While these principles are relevant to digital trade, they do not sufficiently address issues such as data ownership, localisation, privacy and platform dominance. The World Trade Organization has initiated discussions through its Joint Statement Initiative on e-commerce, but progress remains limited due to divergent interests among member states.[13] Consequently, digital trade governance remains fragmented and underdeveloped at the multilateral level.

One of the key challenges lies in recognising data as a trade asset. Unlike traditional commodities, data is intangible, non-rivalrous and capable of being replicated at near-zero cost. Despite this, it holds immense economic value, forming the backbone of digital platforms and services. The United Nations Conference on Trade and Development has emphasised that data is now a critical factor of production, comparable to labour and capital in its economic significance.[14] This reconceptualisation raises important legal questions regarding ownership, control and the equitable distribution of benefits arising from data flows.

The governance of digital trade is further complicated by jurisdictional conflicts among major global actors, particularly the United States, the European Union and countries of the Global South. The United States generally adopts a market-driven, liberal approach that favours free cross-border data flows and minimal regulatory intervention. This model supports innovation and the global expansion of technology firms such as Google and Amazon, but has been criticised for insufficient safeguards relating to privacy and market concentration.

In contrast, the European Union has developed a rights-based regulatory framework, exemplified by stringent data protection laws such as the General Data Protection Regulation (GDPR). The EU approach prioritises individual privacy, data protection and competition regulation, often imposing significant compliance obligations on digital platforms. This has led to increased scrutiny of dominant firms like Meta and Apple, reflecting a more interventionist stance.[15]

Meanwhile, countries in the Global South adopt diverse and often evolving approaches, balancing the need for digital development with concerns over data sovereignty and economic dependence. Many developing states advocate for data localisation measures and greater control over domestic data resources to prevent exploitation by foreign technology firms. However, such measures may also create barriers to trade and limit participation in the global digital economy.[16]

These divergent regulatory models contribute to a broader fragmentation problem in global digital governance. The absence of a unified international framework results in overlapping and sometimes conflicting legal regimes, increasing compliance costs and legal uncertainty for businesses operating across borders. It also creates enforcement challenges, particularly in cases involving transnational data flows and digital platforms that operate simultaneously in multiple jurisdictions.

Furthermore, existing global institutions lack the enforcement capacity and normative clarity required to address the intersection of digital trade, competition law and criminal liability. As digital markets become increasingly interconnected, the limitations of fragmented governance structures become more pronounced. The need for coordinated international regulation is therefore essential to ensure fair competition, protect consumer rights and prevent the abuse of dominance in digital trade.

In this context, global governance must evolve to address the unique characteristics of the digital economy. This includes recognising data as a strategic resource, harmonising regulatory approaches and integrating legal frameworks across trade, competition and criminal law. Without such reforms, the current fragmented system will remain inadequate to effectively regulate data monopolies and their growing influence in global digital trade.

4. Case Studies of Data Monopolies

The emergence of data monopolies is best understood through the operational practices of major digital platforms. Corporations such as Google, Amazon and Meta exemplify how control over data translates into market dominance, raises concerns of abuse, and, in certain instances, approaches the threshold of criminality.

A. Google: Search Dominance and Algorithmic Control

Google has established a near-monopolistic position in the global search engine market, driven by its ability to collect, process and monetise vast amounts of user data. Its dominance is reinforced by network effects, default settings on devices, and integration across services such as search, advertising and mobile operating systems. The accumulation of user data enables continuous improvement of algorithms, thereby strengthening its competitive advantage.

Regulatory authorities, particularly in the European Union, have found that Google engaged in self-preferencing practices, notably favouring its own comparison shopping services in search results.[17] Such conduct demonstrates how algorithmic control can distort market competition. Additionally, concerns have been raised regarding the opacity of algorithms and their potential to manipulate consumer behaviour.

From a criminal law perspective, the question arises whether such conduct constitutes intentional exclusion or deception. While competition law has imposed significant fines, these remedies remain civil in nature. However, where algorithmic manipulation is used deliberately to mislead users or suppress competitors, it may arguably approach forms of economic fraud or abuse involving intentional harm. The difficulty lies in establishing mens rea (criminal intent) within complex algorithmic systems.

B. Amazon: Data Advantage and Platform Self-Preferencing

Amazon represents a dominant force in e-commerce, operating both as a marketplace and a direct seller. Its access to granular data on third-party sellers including pricing strategies, consumer preferences and sales performance creates a significant competitive advantage. This dual role has led to allegations that Amazon uses proprietary data to replicate successful products and prioritise its own offerings.[18]

Such practices raise concerns of exclusionary conduct and unfair competition, as independent sellers may be systematically disadvantaged. The European Commission has investigated Amazon for allegedly using non-public seller data to distort competition within its marketplace.[19] Furthermore, Amazon's pricing strategies have been scrutinised for potentially engaging in predatory pricing aimed at eliminating competitors.

The transition from regulatory violation to criminal conduct depends on the presence of deliberate exploitation and harm. If data obtained under conditions of trust is used deceptively to undermine competitors, such conduct could be interpreted as a breach of fiduciary obligations or even fraudulent misappropriation. However, current legal frameworks largely address these issues through administrative penalties rather than criminal sanctions. This highlights a gap in addressing the severity of data-driven abuses.

C. Meta Platforms: Data Exploitation and Privacy Violations

Meta, as the operator of major social networking platforms, exercises dominance through its control over social data and digital advertising markets. Its business model relies heavily on the collection and monetisation of user data, creating a vast repository of behavioural information. This data-driven dominance is reinforced by network effects and high switching costs for users.

One of the most significant controversies involving Meta is the Cambridge Analytica scandal, which exposed the large-scale harvesting and misuse of personal data without informed consent.[20] This incident demonstrated how data exploitation could extend beyond commercial practices into political manipulation, affecting democratic processes. Regulatory responses included fines and stricter data protection enforcement, particularly under European Union law.

From a criminal law perspective, such practices raise serious concerns regarding privacy violations, deception and unlawful data processing. The unauthorised use of personal data, especially where it results in societal harm, may meet the threshold for criminal liability in certain jurisdictions. Unlike traditional competition abuses, these actions directly infringe upon individual rights, thereby strengthening the case for criminalisation.

D. Comparative Analysis: From Dominance to Criminality

Across these case studies, a common pattern emerges: dominance is achieved through data accumulation, reinforced by technological infrastructure, and maintained through practices that may exclude competitors or exploit users. While competition law has addressed these issues through fines and regulatory interventions, it often fails to capture the broader societal harm caused by such conduct.

The transition from abuse of dominance to criminal conduct depends on key factors, including intent, scale of harm and the nature of the violation. Practices such as intentional algorithmic manipulation, deceptive data exploitation and predatory strategies aimed at eliminating competition may justify criminal scrutiny. However, enforcement remains challenging due to jurisdictional limitations, evidentiary complexities and the absence of clear legal standards for criminal liability in digital markets.

These case studies illustrate the urgent need to rethink existing legal frameworks. The conduct of data monopolies cannot be fully addressed within the confines of traditional competition law. Instead, a more integrated approach incorporating criminal law principles is necessary to ensure accountability in the digital economy.

5. Legal Framework Analysis

A. Competition Law

Competition law remains the primary legal mechanism for addressing the dominance of digital platforms. In the European Union, enforcement has been particularly robust, reflecting a proactive approach to regulating digital markets. The European Commission has utilised Article 102 of the Treaty on the Functioning of the European Union (TFEU) to impose significant penalties on dominant firms for abusive practices, including self-preferencing and exclusionary conduct.[21]

Landmark decisions against Google illustrate the EU's willingness to address digital dominance through traditional antitrust tools.

More recently, the European Union has introduced the Digital Markets Act (DMA), a forward-looking regulatory instrument aimed at preventing unfair practices by "gatekeeper" platforms. The DMA shifts from ex post enforcement to ex ante regulation, imposing obligations on large platforms to ensure fair competition and data access.[22] This reflects an acknowledgment that traditional competition law is insufficient to address the speed and scale of digital markets.

In contrast, the United States has historically adopted a more cautious approach, prioritising consumer welfare and innovation. However, this stance is evolving, with increasing scrutiny of Big Tech by agencies such as the Federal Trade Commission (FTC) and the Department of Justice (DOJ). Cases against firms like Amazon and Meta signal a shift towards recognising the anti-competitive risks posed by data monopolies.[23] Nonetheless, US antitrust law continues to face challenges in adapting to data-driven market dynamics, particularly in defining market power and harm.

In India, the Competition Commission of India enforces the Competition Act, 2002, which prohibits abuse of dominant position under Section 4. The CCI has increasingly focused on digital markets, investigating practices of major platforms and recognising the role of data in conferring dominance.[24] Recent policy discussions, including proposals for a Digital Competition Law, indicate India's intent to strengthen its regulatory framework in line with global developments.

B. Criminal Law Interface

While competition law primarily addresses abuse of dominance through civil and administrative remedies, the interface with criminal law remains limited but is gradually expanding. Certain practices associated with data monopolies such as fraud, data misuse and consumer exploitation may fall within the ambit of criminal offences under national legal systems.For instance, deceptive data practices, including the unauthorised collection or misuse of personal data, may constitute fraud or breach of trust in certain jurisdictions. Similarly, algorithmic manipulation designed to mislead consumers or distort market outcomes could potentially attract criminal liability where intent and harm can be established. Andrew Ashworth notes that criminal law is justified where conduct involves serious harm and culpability, particularly where regulatory mechanisms prove insufficient.[25]

Despite these possibilities, the application of criminal law to digital market abuses remains rare. This is largely due to evidentiary challenges, including proving intent (mens rea) in complex algorithmic systems and attributing liability within large corporate structures. Moreover, most jurisdictions prefer regulatory enforcement, viewing competition issues as matters of economic policy rather than criminal wrongdoing.

However, there is a growing recognition that certain forms of abuse particularly those involving large-scale data exploitation or systemic deception may warrant criminal sanctions. This is especially relevant in cases where digital platforms impact not only markets but also fundamental rights such as privacy and autonomy.

C. Gaps in the Existing Framework

Despite increasing regulatory attention, significant gaps persist in the legal framework governing data monopolies. One of the most critical issues is the lack of clear thresholds for criminal liability. While competition law identifies abusive conduct, it does not clearly delineate when such conduct should be treated as criminal. This ambiguity limits the ability of enforcement agencies to pursue stronger sanctions against harmful practices.

Another major challenge is weak cross-border enforcement**.** Digital platforms operate globally, while legal jurisdictions remain territorially bound. This creates difficulties in investigating and prosecuting transnational abuses, particularly where data flows across multiple jurisdictions. Institutions such as the World Trade Organization have yet to develop comprehensive mechanisms to address these issues within the context of digital trade.[26]

Additionally, the phenomenon of regulatory arbitrage allows firms to exploit differences between national legal regimes. By operating in jurisdictions with weaker regulations or enforcement mechanisms, data monopolies can circumvent stricter laws, thereby undermining global governance efforts. This fragmentation not only reduces the effectiveness of existing frameworks but also creates an uneven playing field for businesses and states.

Furthermore, there is a lack of coordination between competition law, criminal law and data protection regimes. These legal domains often operate in silos, leading to gaps in enforcement and accountability. As digital markets continue to evolve, the absence of an integrated legal approach becomes increasingly problematic.

Conclusive Remark on case study

The current legal framework addressing data monopolies is characterised by strong competition law enforcement in certain jurisdictions, an emerging but underdeveloped criminal law interface, and significant structural gaps. While initiatives such as the EU's Digital Markets Act and evolving antitrust approaches in the United States and India represent important steps forward, they remain insufficient to address the full spectrum of challenges posed by data-driven dominance.

To effectively regulate digital markets, it is essential to develop a coherent legal framework that bridges the divide between competition law and criminal law while addressing cross-border enforcement challenges. Without such integration, the existing system will continue to struggle in holding data monopolies accountable for increasingly complex and potentially harmful practices.

6. The Problem of Criminal Abuse of Dominance

The rapid evolution of digital markets has exposed fundamental limitations in existing legal frameworks, particularly in addressing the criminal dimensions of abuse of dominance by data monopolies. While competition law has traditionally served as the primary tool for regulating market power, it is increasingly evident that its mechanisms are inadequate to respond to the scale, speed and societal impact of digital abuses.

One of the principal shortcomings of current law is slow enforcement**.** Competition law proceedings especially in jurisdictions such as the European Union and the United States are often prolonged, involving extensive investigations, economic analysis and judicial review. For instance, cases pursued by the European Commission against Google have taken several years to conclude, by which time market structures may already have been irreversibly altered.[27] In fast-moving digital markets, such delays significantly undermine the effectiveness of regulatory intervention, allowing dominant firms to entrench their position further.

A second critical issue is the insufficiency of civil penalties. Competition law primarily relies on fines and behavioural remedies to address abusive conduct. However, for large technology corporations such as Amazon and Meta, financial penalties often represent only a marginal cost of doing business. The deterrent effect of such sanctions is therefore limited, particularly when weighed against the substantial economic benefits derived from anti-competitive practices. As a result, firms may continue engaging in borderline or unlawful conduct, treating regulatory fines as an acceptable risk.

Beyond procedural and remedial limitations, the nature and scale of harm caused by data monopolies further highlight the inadequacy of existing frameworks. First, there is significant market distortion, where dominant firms leverage data advantages to exclude competitors, manipulate pricing and control market access. Such distortions undermine the principles of fair competition and innovation that competition law seeks to protect.

Second, consumer exploitation has become a defining feature of digital markets. Through practices such as opaque data collection, algorithmic manipulation and targeted advertising, platforms can influence consumer behaviour in ways that compromise autonomy and informed choice. These practices often occur without meaningful consent, raising serious concerns regarding fairness and accountability.

Third, and perhaps most critically, data monopolies pose democratic risks. The control and processing of vast amounts of personal and behavioural data enable platforms to shape public discourse, influence political outcomes and amplify misinformation. The Cambridge Analytica controversy involving Meta demonstrated how data misuse can extend beyond economic harm to affect democratic institutions and processes.[28] Such risks transcend the traditional scope of competition law and require a broader legal response.

In light of these challenges, it is necessary to reconsider the legal characterisation of certain forms of abuse of dominance. This article argues that some practices particularly those involving intentional exclusion, deceptive data exploitation and large-scale societal harm should be recognised as forms of criminal misconduct. Criminalisation would introduce stronger deterrence through punitive sanctions, including fines, corporate liability and, where appropriate, individual accountability for decision-makers.

However, the effectiveness of criminalisation depends on global coordination. Given the transnational nature of digital platforms, isolated national approaches are insufficient. Divergent legal standards create enforcement gaps and enable regulatory arbitrage. Therefore, a harmonised international framework is required to define clear thresholds for criminal liability, establish jurisdictional cooperation and ensure consistent enforcement across borders. Institutions such as the World Trade Organization and other multilateral bodies could play a role in facilitating such coordination, although significant reforms would be necessary.

Ultimately, the problem of criminal abuse of dominance lies in the mismatch between traditional legal tools and contemporary digital realities. As data monopolies continue to expand their influence, the failure to adequately address their conduct risks not only economic inefficiency but also broader societal harm. Recognising and criminalising the most egregious forms of abuse is therefore an essential step towards ensuring accountability and safeguarding the integrity of digital markets.

7. Proposed Governance Model

The increasing complexity of digital markets and the inadequacy of existing legal frameworks necessitate a reconceptualised governance model capable of addressing both the economic and criminal dimensions of data monopolies. This section proposes a hybrid, multi-layered framework that integrates competition law, criminal law and international cooperation to effectively regulate the abuse of dominance in digital trade.

A. Hybrid Framework

At the core of the proposed model lies the integration of competition law and criminal law. Traditionally, competition law has focused on maintaining market efficiency through civil and administrative remedies, while criminal law has been reserved for conduct involving moral culpability and significant harm. However, in the digital economy, certain forms of abuse such as intentional exclusion, deceptive data exploitation and large-scale manipulation blur the boundaries between these domains.

A hybrid framework would allow regulatory authorities to differentiate between ordinary anti-competitive conduct and aggravated forms of abuse**.** While standard cases could continue to be addressed through fines and behavioural remedies, more severe violations—characterised by intent, systemic harm and deception—would trigger criminal liability. This dual approach ensures proportionality while enhancing deterrence.

Furthermore, effective governance requires international cooperation, as digital platforms operate across multiple jurisdictions. Institutions such as the World Trade Organization and the Organisation for Economic Co-operation and Development can play a pivotal role in facilitating dialogue, harmonising standards and promoting coordinated enforcement. Without such cooperation, fragmented national approaches will continue to be undermined by regulatory arbitrage and jurisdictional conflicts.

B. Global Digital Authority (Proposed Institution)

To address the limitations of existing institutions, this article proposes the establishment of a Global Digital Authority (GDA) a specialised international body tasked with overseeing digital market governance. The GDA would not replace national regulators but would function as a coordinating and standard-setting entity.

First, the GDA would develop uniform data governance standards, including rules on data collection, processing, sharing and protection. These standards would aim to balance innovation with accountability, ensuring that data-driven business models do not compromise competition or fundamental rights.

Second, the GDA would facilitate cross-border enforcement mechanisms. This includes information sharing between national authorities, joint investigations and coordinated sanctions against multinational digital platforms. Given the global operations of firms such as Google and Meta, such mechanisms are essential to prevent jurisdictional loopholes.

Third, the GDA could act as a dispute resolution forum, addressing conflicts arising from divergent national regulations and ensuring consistency in the application of digital governance norms. By providing a centralised platform for coordination, the GDA would help reduce fragmentation and enhance regulatory effectiveness.

C. Key Reforms

The success of the proposed governance model depends on the implementation of several targeted legal reforms**.**

1. ***Defining "Criminal Abuse of Dominance"***

A clear and universally accepted definition of criminal abuse of dominance is essential. This should include elements such as intentional exclusionary conduct, deceptive data practices, large-scale consumer harm and significant impact on market structure or democratic processes. Establishing such thresholds would provide legal certainty and enable consistent enforcement across jurisdictions.

1. ***Data-Sharing Obligations***

To reduce entry barriers and promote competition, dominant platforms should be subject to mandatory data-sharing requirements**,** subject to privacy safeguards. This would prevent data hoarding and enable smaller firms to compete more effectively. Regulatory frameworks such as the EU's Digital Markets Act provide a useful starting point, but global harmonisation is necessary to ensure uniform application.

1. ***Algorithmic Transparency and Accountability***

Given the central role of algorithms in shaping digital markets, there is a need for greater transparency and oversight. Platforms should be required to disclose key aspects of their algorithms, particularly where they influence market outcomes or consumer behaviour. Independent audits and regulatory supervision can help ensure that algorithmic systems are not used to engage in discriminatory or manipulative practices.

The proposed governance model seeks to bridge the gap between existing legal frameworks and the realities of the digital economy. By integrating competition law with criminal law, establishing a Global Digital Authority and implementing targeted reforms, it offers a comprehensive approach to addressing the challenges posed by data monopolies. Such a model not only enhances accountability but also preserves the innovative potential of digital markets, ensuring that global digital trade remains both competitive and equitable.

8. Conclusion

The rise of data monopolies marks a fundamental shift in the structure of global economic power. Corporations such as Google, Amazon and Meta are no longer merely market participants; they function as power centres that control vast data ecosystems, influence consumer behaviour and shape digital markets across jurisdictions. Their dominance is sustained not only through economic strength but through control over information, algorithms and digital infrastructures that are increasingly indispensable to modern trade.

This transformation has also altered the nature of abuse of dominance. What was once understood primarily as a civil or regulatory issue within competition law has evolved into a more complex phenomenon with broader societal implications. Practices such as data hoarding, algorithmic manipulation and exploitative data extraction extend beyond traditional anti-competitive conduct, raising concerns relating to privacy, autonomy and even democratic integrity. The scale and intentionality of such practices suggest that certain forms of abuse can no longer be adequately addressed through civil penalties alone.

Accordingly, this study has emphasised the urgent need for global coordination in regulating digital markets. Existing legal frameworks remain fragmented, with varying approaches adopted by different jurisdictions, leading to enforcement gaps and regulatory arbitrage. Institutions such as the World Trade Organization and the Organisation for Economic Co-operation and Development must play a more proactive role in fostering harmonised standards and facilitating cross-border cooperation. Without such coordination, national efforts will continue to fall short in addressing the transnational nature of digital platforms.

Equally important is the recognition of criminal accountability as a necessary component of digital governance. Where abuse of dominance involves intentional deception, large-scale harm or infringement of fundamental rights, the imposition of criminal liability may be justified to ensure effective deterrence and accountability. Integrating criminal law principles into the regulatory framework would signal a shift from purely economic regulation to a more holistic approach that acknowledges the societal impact of digital market practices.

Looking ahead, the challenge lies in designing a governance framework that balances regulation with innovation. Overregulation risks stifling technological progress, while under-regulation allows unchecked concentration of power. The future of digital trade therefore depends on the development of a coherent, adaptive and globally coordinated legal regime one that recognises data monopolies as central actors in the digital economy while ensuring that their power is exercised responsibly, transparently and within the bounds of law.

Outcome

This article demonstrates that the rise of data monopolies exemplified by dominant digital platforms such *as Google, Amazon and Meta poses significant systemic risks to fair competition, consumer welfare and the integrity of global digital trade. By analysing the evolution of market dominance in the data-driven economy, the study highlights how existing legal frameworks, particularly competition law, are insufficient to address the scale and complexity of modern digital abuses.*

The article further establishes that certain forms of abuse of dominance especially those involving intentional exclusion, exploitative data practices and large-scale societal harm transcend the boundaries of civil or administrative wrongs and warrant recognition as criminal conduct. It underscores the necessity of redefining legal thresholds to incorporate criminal accountability where harm is substantial and deliberate.

Ultimately, the study concludes that the development of a hybrid global governance framework, integrating competition law, criminal law and international cooperation, is essential for addressing the challenges posed by data monopolies. Such an approach is critical to ensuring accountability, preventing regulatory arbitrage and fostering a fair, transparent and equitable digital economy that supports both innovation and global trade.

Bibliography

1. Aaronson SA, 'Data Is Different: Why the World Needs a New Approach to Governing Cross-Border Data Flows' (2018) 2 *Digital Policy, Regulation and Governance* 1.
2. Ashworth A, *Principles of Criminal Law* (7th edn, Oxford University Press 2013).
3. Bork RH, *The Antitrust Paradox: A Policy at War with Itself* (Free Press 1978).
4. Cadwalladr C and Graham-Harrison E, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica' *The Guardian* (London, 17 March 2018).
5. Calo R, 'Digital Market Manipulation' (2014) 82 *George Washington Law Review* 995.
6. Case AT.39740 *Google Search (Shopping)* [2017] European Commission Decision.
7. Case AT.40099 *Google Android* [2018] European Commission Decision.
8. Competition Act 2002 (India).
9. Craig P and de Búrca G, *EU Law: Text, Cases, and Materials* (7th edn, Oxford University Press 2020).
10. Crémer J, de Montjoye YA and Schweitzer H, 'Competition Policy for the Digital Era' (2019) European Commission Report.
11. European Commission, 'Antitrust: Commission Opens Investigation into Amazon's Use of Seller Data' (Press Release, 2019).
12. Ezrachi A and Stucke ME, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press 2016).
13. Graef I, *EU Competition Law, Data Protection and Online Platforms* (Kluwer Law International 2016).
14. Information Technology Act 2000 (India).
15. Khan LM, 'Amazon's Antitrust Paradox' (2017) 126 *Yale Law Journal* 710.
16. Organisation for Economic Co-operation and Development, *Data-Driven Innovation: Big Data for Growth and Well-Being* (OECD 2015).
17. Organisation for Economic Co-operation and Development, *OECD Digital Economy Outlook 2020* (OECD Publishing 2020).
18. Posner RA, *Antitrust Law* (2nd edn, University of Chicago Press 2001).
19. Regulation (EU) 2016/679 (General Data Protection Regulation).
20. Regulation (EU) 2022/1925 of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act).
21. Stucke ME and Grunes AP, 'Debunking the Myths over Big Data and Antitrust' (2016) 68 *Antitrust Law Journal* 339.
22. United Nations Conference on Trade and Development, *Digital Economy Report 2019: Value Creation and Capture* (United Nations 2019).
23. United Nations Conference on Trade and Development, *Digital Economy Report 2021* (United

Nations 2021).

24. United States v Google LLC (2020) US District Court.
25. Varian HR, ‘Artificial Intelligence, Economics, and Industrial Organization’ (2019) 33 *Innovation Policy and the Economy* 399.
26. Whish R and Bailey D, *Competition Law* (9th edn, Oxford University Press 2018).
27. World Trade Organization, *World Trade Report 2020: Government Policies to Promote Innovation in the Digital Age* (WTO 2020).
28. Zuboff S, *The Age of Surveillance Capitalism* (Profile Books 2019).

--- 1. Organisation for Economic Co-operation and Development, *OECD Digital Economy Outlook 2020* (OECD Publishing 2020).[↩](#fnref1) 2. Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).[↩](#fnref2) 3. United Nations Conference on Trade and Development, *Digital Economy Report 2021* (UN 2021).[↩](#fnref3) 4. Richard Whish and David Bailey, *Competition Law* (9th edn, OUP 2018).[↩](#fnref4) 5. Organisation for Economic Co-operation and Development, *OECD Digital Economy Outlook 2020* (OECD Publishing 2020).[↩](#fnref5) 6. United Nations Conference on Trade and Development, *Digital Economy Report 2021* (UN 2021).[↩](#fnref6) 7. Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).[↩](#fnref7) 8. Consolidated Version of the Treaty on the Functioning of the European Union \[2012\] OJ C326/47, art 102.[↩](#fnref8) 9. Richard Whish and David Bailey, *Competition Law* (9th edn, OUP 2018).[↩](#fnref9) 10. Shoshana Zuboff (n 3).[↩](#fnref10) 11. Andrew Ashworth, *Principles of Criminal Law* (7th edn, OUP 2013).[↩](#fnref11) 12. World Trade Organization, *World Trade Report 2020: Government Policies to Promote Innovation in the Digital Age* (WTO 2020).[↩](#fnref12) 13. World Trade Organization, ‘Joint Statement Initiative on E-commerce’ (WTO, ongoing negotiations).[↩](#fnref13) 14. United Nations Conference on Trade and Development, *Digital Economy Report 2021* (UN 2021).[↩](#fnref14) 15. Paul Craig and Gráinne de Búrca, *EU Law: Text, Cases, and Materials* (7th edn, OUP 2020).[↩](#fnref15) 16. Susan Ariel Aaronson, ‘Data Is Different: Why the World Needs a New Approach to Governing Cross-Border Data Flows’ (2018) 2 *Digital Policy, Regulation and Governance* 1.[↩](#fnref16) 17. Case AT.39740 *Google Search (Shopping)* \[2017\] European Commission Decision.[↩](#fnref17) 18. Lina M Khan, ‘Amazon’s Antitrust Paradox’ (2017) 126 *Yale Law Journal* 710.[↩](#fnref18) 19. European Commission, ‘Antitrust: Commission Opens Investigation into Amazon’s Use of Seller Data’ (Press Release, 2019).[↩](#fnref19) 20. Carole Cadwalladr and Emma Graham-Harrison, ‘Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica’ *The Guardian* (London, 17 March 2018).[↩](#fnref20) 21. Consolidated Version of the Treaty on the Functioning of the European Union \[2012\] OJ C326/47, art 102.[↩](#fnref21) 22. Regulation (EU) 2022/1925 of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act).[↩](#fnref22) 23. Lina M Khan, ‘Amazon’s Antitrust Paradox’ (2017) 126 *Yale Law Journal* 710.[↩](#fnref23) 24. Competition Commission of India, *Market Study on E-commerce in India* (2020).[↩](#fnref24) 25. Andrew Ashworth, *Principles of Criminal Law* (7th edn, OUP 2013).[↩](#fnref25) 26. World Trade Organization, *World Trade Report 2020* (WTO 2020).[↩](#fnref26) 27. Case AT.39740 *Google Search (Shopping)* \[2017\] European Commission Decision.[↩](#fnref27) 28. Carole Cadwalladr and Emma Graham-Harrison, ‘Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica’ *The Guardian* (London, 17 March 2018)[↩](#fnref28)