

Algorithms on Autopilot: Bridging the Regulatory Gap in Global Competition Law

Madhulika Singh 

Faculty of Law, Jai Narain Vyas University, 342011, India

ABSTRACT: We live in the technological age, all our daily activities from shopping, eating, travel, entertainment, healthcare to finding your perfect date is backed by sophisticated technological tools and machines. Markets are digitalized and are increasingly relying on self-learning algorithms to analyze large and complex database, to offer to its customers better products and customized services. They simultaneously facilitate a new frontier of anti-competitive behavior called algorithmic collusion. This article examines the burgeoning 'Liability Gap' where traditional antitrust frameworks, affixed in the necessity of a human meeting of minds, fail to capture coordination achieved through machine learning. Through a comparative analysis of the legal landscapes in the United States, European Union, India, and Russia, this study highlights a global doctrinal crisis. The research finds that self-learning algorithms bypass the conventional ways of collusion create new dimensions of anti-competitive behavior. Therefore, this article proposes a shift from subjective intent to a standard of objective foresight. It concludes by recommending a three-pronged regulatory framework for algorithmic accountability.

Keywords: algorithmic collusion, antitrust liability, machine learning, competition act.

I. INTRODUCTION

Businesses across the economy are ever more counting on smart learning machines and algorithms, to strive in the changing market space. With the advancement of technology and easy availability of data analyzing tools, global giants like Amazon, Uber, Google, to name a few, to the local startups are investing in developing intelligent machines to optimize its business by understanding consumer choices, better logistical support, dynamic pricing decisions, amongst many other commercial decisions. The integration of algorithms and machine learning into commercial strategies has substantially changed the market dynamics.

While these synergies offer pro-competitive efficiencies, it simultaneously introduces the risk of algorithmic collusion. When firms coordinate market outcomes through automated systems rather than explicit human agreements, it poses a systemic challenge to the foundations of global antitrust law. This article provides a cross-jurisdictional analysis of this doctrinal crisis, examining the evolving legal landscapes of the United States, the European Union, India, and Russia. The current reliance on subjective intent of meeting of minds is increasingly obsolete in a landscape governed by Black Box algorithms. The core of the problem lies in the widening Liability Gap. The traditional legislative regime is still anchored on to the concurrence of will or meeting minds, however as algorithms achieve super competitive prices through tacit collusion, the regulatory gap arises. With this accountability gap the market suffers the economic harm of a cartel, but the law fails to find a "guilty" human actor to hold responsible.

The article is developed in the following structure: Section II provides a literature review of the algorithmic antitrust debate. Section III details the Material and Methodology, adopting a qualitative doctrinal approach combined with comparative legal analysis. Section IV transitions into the Jurisdictional and Data Analysis, where the article critically evaluates the current legal standing in the United States, the European Union, India, and Russia. Section V concludes with a three-pronged global recommendation.

II. RELATED WORK

The foundational body of literature on algorithmic collusion is the transition from traditional human centric cartel theories to the Black Box challenges posed by autonomous systems. Early formative works by Ezrachi and Stucke (2016) established a typology of algorithmic collusion models. They ranged from messenger model to hub and spoke to digital eye model, each more complex than the previous, without the need of explicit human intervention. Subsequent scholarship has focused heavily on the Intent Gap, with Harrington (2018) demonstrating how profit-maximization algorithms naturally gravitate toward stable, non-competitive pricing. Further the debate between conscious parallelism and machine learned coordination is learned through the Twombly case in United States. Furthermore, from the analysis of European academia it is suggested and advocated that effects-based approach should be adopted, and public distancing from an algorithm's collusive output should be the new threshold for corporate liability under Article 101 TFEU.

The recent literature and case analysis has shifted to bring to light the failure to capture Hub-and-Spoke Model cartels in platform-based economies. In the Indian context, the Samir Agrawal (2021) decision sparked a critical discourse led by scholars like Koradia (2022), who argued that the judiciary's insistence on a horizontal communication between drivers ignored the reality of centralized algorithmic control. This criticism is mirrored in the 2023 US RealPage litigation, which scholars cite as a pivotal attempt to bridge the liability gap between parallel conduct vis-à-vis illegal agreement to collude between the entities. Furthermore, the introduction of the Russian Fifth Antimonopoly Package in 2023 added a new dimension to the legislative literature, introducing the concept of the algorithm as an aggravating instrument of market crime. This article with the study and analysis of above mentioned esteemed scholarships has drawn to the inescapable conclusion that the Liability Gap is no longer a theoretical risk but a functional failure of existing statutes to keep pace with the technical reality of colluding algorithms, necessitating a move toward strict or vicarious liability models.

III. MATERIAL & METHOD

The methodology of this study is rooted in doctrinal legal research, focusing on a qualitative and analytical examination of existing legal frameworks across four major jurisdictions: the United States, the European Union, India, and Russia. This study employs a systematic approach to identify, analyse, and synthesize legal principles, statutes, judicial precedents, regulatory roadblock to address the escalating 'liability gap' in algorithmic antitrust law.

1. DATA COLLECTION

- Primary Sources: the primary sources of data consist of the national statutes, the Competition Act, 2002; the US Sherman Act, and Russia's Federal Law No. 426-FZ), international treaties (TFEU), and landmark judicial pronouncements.
- Secondary Sources: Secondary data was collected from peer-reviewed journals, law review articles, reports from competition authorities (OECD and FAS Russia), and authoritative legal commentaries.

2. RESEARCH DESIGN

The study adopts a cross jurisdictional comparative qualitative design, utilizing an analytical and deductive reasoning framework. The selection of the United States, EU, India, and Russia was purposive. For these jurisdictions represent a spectrum of regulatory responses from the strictly intent-based US and Indian regime to the recent pragmatic legislative amendments in Russia, offering a comprehensive global perspective on the evolution of algorithmic antitrust enforcement.

The study analysed common doctrinal challenges posed by strictly worded legislation in each jurisdiction. Further the specific failure of 'concurrence of minds' principle exposes a profound regulatory lacuna across jurisdictions, where algorithmic black box colludes without human intervention. And later the study concludes with a prescriptive proposal to bridge the liability gap by advocating for shift towards need for vicarious liability for effects from algorithmic collusion and to move ahead with 'accountability by design' model.

IV. DATA ANALYSIS

This section aims to undertake a detailed comparative analysis of legal framework governing algorithmic collusion across four major jurisdictions. The study aims to have a thematic analysis of how each jurisdiction construes the evidentiary requirement to prove existence of cartels and what roadblocks are faced by the regulatory bodies to convict the new aged black box algorithms. The section evolves through, firstly defining some basic concepts like algorithm, algorithmic pricing, algorithmic collusion and typology of algorithm. Later the cross jurisdictional analysis unfolds.

1. BASIC CONCEPTS

1.1 Algorithm

Algorithm can be understood as a systematic arrangement of logical instructions or inputs mechanically fed, to generate a stipulated output. The intersection of algorithms with computational technology has increasingly amplified its expanse. Also, with advances in artificial intelligence and machines learning, combined with gigantic amount of data available and stored, highly sophisticated algorithms take shape.

Algorithms are designed to cater to varied application-based tasks. Ranging from simple ones like arrangement of numbers to complex digital encryption, they can be classified on the basis of the task performed as simple algorithms and deep learning algorithms, simple algorithms follow the chain of exact instructions fed into it in an orderly manner, only following the procedure it was previously instructed to conduct. Deep learning algorithms or Machine learning algorithms, use artificial intelligence to mechanically classify information, mimicking human brain. Such algorithms once fed with sequence to process market inputs, identify interrelation in prices, further leading to possibility of price collusion.

1.2 Algorithmic Pricing

The increasing role of algorithm in price setting across all the sectors in economy, has on one hand created supply-side & demand-side efficiencies and on the other has increased the possibility of price collusion amongst the competitors. The algorithmically set prices are receptive to variation in demand and supply, on the supply side it allows the businesses to have enhanced transparency, better managed inventory and competitive pricing which is achieved with feedbacks and trials, resulting in optimized commercial strategies. On the demand side the algorithms enable consumers to get goods and services suited to their needs at optimum price and best offer increasing the consumer welfare.

1.3 Algorithmic Collusion

Every business entity has intrinsic right to choose the prices of goods offered, often leading to mindful similarity in prices which is obvious for competitors having similar market conditions. However, the usage of algorithms facilitates the competitors to monitor each other's business strategy instantaneous, creating the groundwork for collusion. The advent of pandemic has made e-commerce an essential segment of the global retail. This digital marketplace is substantially dependant on algorithms for enhanced effectiveness and streamlined transactions, which apart from bringing competence also brings to the table potential anti-competitive harm.

which has been a burning topic of debate amongst the antitrust scholars and policy makers across jurisdiction.

1.4 Typology of Algorithms

The evolution of algorithms can be made comprehensible by understanding the extent of human intervention and decrees of implicit communication by machines themselves.

- The Messenger Model

In this model the algorithm only serves as a channel for the pre-existing human agreement. When agreement to collude is agreed into at the human level, and software is only deployed in place to supervise or enforce the collusion, it is the messenger model. Because a clear agreement exists, this scenario is easily prosecuted under traditional antitrust frameworks like Section 1 of the Sherman Act or Article 101 TFEU, in United States v. Topkins, such model was used, where a seller on Amazon used specialized software to synchronize prices for posters with those of competitors based on a prior agreement.[1] In India, the

Competition Commission of India (CCI) took a similar stance in the Airlines Cartel Case (2021), clarifying that while using software for revenue management is legal, its use as a tool to implement a common price-fixing understanding would trigger Section 3 liability.[2]

- Hub and Spoke Model

Using such a model, price coordination amongst the competitors (the spokes) is achieved through utilizing the same third-party pricing algorithm or off-the-shelf software (the hub). The competitors may not even be communicating with each other directly. Liability often depends on whether the competitors knew they were using the same pricing logic to stabilize the market. A notable example is the US case *Meyer v. Kalanick*, where it was argued that Uber's use of a common pricing algorithm for all drivers constituted a horizontal price-fixing conspiracy, though the court noted the difficulties of applying traditional "hub-and-spoke" theory to digital platforms.[3]

- The Predictable Agent Model

Under this model each competitor aligns its own algorithm that prioritizes price matching over competition, where the algorithm monitors and reacts to market signals to naturally reach a state of tacit collusion. Here, the legal standing is precarious, under US law, parallel pricing without "plus factors" is generally not illegal, as firms are simply responding to market conditions.[4] India too struggles with this typology because under Section 3 an agreement, arrangement, or understanding is required, therefore without a plus factor i.e. evidence of communication or a concerted action, the CCI too views this as independent, rational market behaviour.

- The Digital Eye Model

Under this model there is no human intervention to collude, the algorithms are given a broad objective to maximize profits and they on their own through trial and error maintain stable, super-competitive price equilibrium. This creates a significant Liability Gap in almost all jurisdictions, as current laws require an 'agreement' or 'concerted practice' concepts that necessitate human agency to hold accountability of intent. While the Competition (Amendment) Act, 2023, has broadened the CCI's powers to investigate "digital markets," Indian jurisprudence still lacks a mechanism to hold firms liable for the unintended, self-learned collusive outcomes of an AI.[5]

2. JURISDICTIONAL ANALYSIS

2.1 European Union

Algorithms and smart learning machines are increasingly being adopted for efficacy and enhanced competitiveness in businesses. European Commission's 'Final Report on the E-Commerce Sector Inquiry', highlights the increasing use of algorithms in businesses, as smart learning machines are being adopted by two third of the online businesses for monitoring and adjusting to competition. Diversity of collusive conduct with advancement in the market structure has posed before the competition authorities' intricate problems, which has thus led to unceasing evolution of competition jurisprudence through the following legislation and a few from the vast catena of judgements are discussed below.

2.1.1 Legislation

The competition rules of the European Union (EU) contained in Article 101 and 102 of the Treaty on the Functioning of the EU (TFEU) very simplistically lay down the law for the member states. The continuous technological revolution, increased data harvesting and storage, with assistance of advanced algorithms pose the challenge of interpretation and application of these legislations before the authorities.

The regulatory framework provided for in Article 101, prohibits all agreement, decisions and practices that may affect trade between member states or limits competition. The definition covers all forms of collusive agreements, emphasizing on the essence rather than on the form, thus covering within its ambit various forms of explicit and implicit agreements, informal communications and any sort of meeting of mind. Article 101 TFEU is sufficiently worded to cover in its range any form of explicit collusion, and any 'agreement, decisions or practices' for which evidence of 'concurrence or meeting of minds' between the undertakings to distort competition can be proved.

The liberal interpretation of Article 101 TFEU has helped clear the grey area through series of cases. The tricky situation arises when there is lack of explicit conduct and no ‘meeting of minds’ can be shown, but an anti-competitive coordination can be seen to exist between the undertakings. The blur around the situation was relatively cleared with the introduction of the concept of ‘concerted practice doctrine’, wherein any communication between the undertakings presumptively attracts liability, if it influences decisions in the market and is capable of causing negative effect on competition in the market.[6]

Article 102 provides innovative rescue to the anti-competitive tacit collusion problem, where the undertakings are in collective dominant position. Dominant undertakings of the market have special responsibility,[7] thus the communication between such “collectively dominant undertakings” can be tackled under this provision if the abuse of dominant position leads to tacit collusion, then this collusion can be charged without the need of proof of “meeting of minds”.[8] Further the question that arises for consideration is whether the undertakings escape liability arising from collusion caused by communication amongst algorithms, especially the Blackbox algorithms?

2.1.2 Judicial Interpretation

Euras Case (2016)

This was one of the first cases of antitrust violation involving automated systems, where a tour agency, Eturas had capped upper limit for discounts at 3% and informed all its business partners about it, the restriction was kept in check using price restricting algorithms. In such cases of collusion, the explicit agreement to collude already exists, the algorithm only facilitates the implementation of the same. The decision of Court of Justice of the EU (CJEU) held only the agencies having knowledge of the anticompetitive practice, liable. Thus, highlighting that, the use of price maintenance and restricting algorithms by itself is not infringement and to establish anticompetitive conduct participation and consent is important.

Google Search (AdSense) Case (2019)

In this particular case Google was found to have abused its dominant position, infringing Article 102 TFEU, by following “relaxed exclusivity” policy [9] under which the most lucrative commercial space on the search result page was reserved for Google’s Adverts, further it also controlled competitor’s advert’s performance. Online advertisement markets are operated by intricate algorithms that principally decide the space allocation for adverts, thus customising search results for targeted customers. The tech giant was fined €1 494 459 000, for the infringement caused from 2006 to 2016, controlling over 70% of the market share.

Amazon Case (2019)

The world’s leading digital retailer is alleged to have caused antitrust infringement, and is accused of using data of third-party sellers selling on its platform, further the marketplace is also accused of favouring product offers and merchants that use Amazon’s logistics. The company plays dual role of being an online retailer and also a marketplace, often putting it in conflict of interest. The investigation highlights the squabble between the third-party retailers and Amazon’s own retail services. It is alleged that the price monitoring algorithms, price Amazon’s own products at a price below than that of the competing third-party seller, thus reserving the “Amazon Buy Box” for its sellers.[10] The antitrust authority is yet under the process of investigating several such services offered by the company, by gathering relevant data from major stakeholders of the industry.

2.2 Russia

The Russia markets are fostering grounds of budding digital technologies, and are powered by smart machines and algorithms, strengthening its digital infrastructure. Russian Government along with the antitrust agency of the country, Federal Antimonopoly Service (FAS), has been especially vigilant about the rapidly evolving digital economy and the policy development thereof has been comprehensive.

2.2.1 Legislative Framework

The fair principles of competition are enunciated in Constitution of the Russian Federation that proscribes monopolization & unfair competition [11] and supports an economic space in support of competition [12]. Further the specific law pertaining to antitrust is the “Federal Law on the Protection of Competition” wherein under Section 11, any agreement sprouting from a concerted action and resulting in an anti-competitive

conduct, leading to consequences listed hereunder, is prohibited. The term “agreement” is defined under section 4 (18) and is wide enough to cover an agreement in documented or oral form.

The antitrust framework underwent a systematic shift in 2023, wherein government enacted ‘Fifth Antimonopoly Package’ through Federal Law No. 301-FZ, which became effective on September 1, 2023.[13] The legislation formally transitioned the Russian regime from a reactive stance to a proactive digital enforcement model. These amendments introduced Article 10.1 into the Law on Protection of Competition, which codifies criteria for ‘Dominant Position’ in the digital era. In accordance with the amendment, an entity that possesses a significant ‘Network Effect’, which is numerically defined as, that the share of transactions performed between sellers and buyers through the digital platform exceeds 35% of the total volume of transactions performed on the relevant commodity market in value terms; and exceeds the revenue threshold of 2 billion rubles in the last calendar year.[14]

Prior to the legislative formalization of the Fifth Antimonopoly Package, the FAS had already established a normative baseline through its ‘Recommendations on Practices in the Use of Information Technologies in Trade’. [15] The recommendations contain elementary rule of using new technologies, like pricing algorithms, by the companies, suggesting that such algorithms may be used for determining one’s own pricing policy, monitoring competition, managing, maintaining and forecasting demand, thus such business policy decisions should not contradict the antitrust laws of the country. By establishing these ‘elementary rules’ of digital conduct, the FAS effectively signalled the transition toward the instrumental liability now codified in Federal Law No. 426-FZ, where the use of such pricing software to facilitate coordination is treated as an aggravating factor

2.2.2 Judicial Development

FAS with the objective to tackle the challenge posed by the digital economy with the significant increase in use of algorithms, in 2017 initiated a case against LG Electronics Russia on an allegation that the company used special software to coordinate and monitor retail prices, the prices of the electronic products were surged on the basis of market analysis conducted by specialized algorithms.[16] It became one of the first cases where a price algorithm came under the scanner of the Antitrust Agency. Later in 2018 the antitrust agency slapped the company with fine of RUB 2.5 million (\$39,721) for fixing and maintaining prices of smartphones.

Later in 2017 FAS began investigating another interesting case of specialized software in Valeria and Egamed case [17], involving the use of Auction Robots by the companies to participate in bidding. Antitrust concerns arose as number of participants were using similar auction robots, leading to coordinated bids and strategy, thus leading to them setting the prices for the tender. [18]

FAS Russia strives to complement and align national legislation with the international antitrust goals, thus constant endeavors are made to achieve international cooperation. FAS Russia cooperates with member states of BRICS, Commonwealth of Independent States (CIS) and Eurasian Economic Union. [19] Russia along with the member states of CIS drafted “Report on Competition Policy Development in Digital Economy” to devise infrastructural and institutional changes for the digital economy. The aim ahead is to establish strengthened enforcement agencies at both national and international level to bridge the emerging gaps in digital economy.

2.3 United States of America

Algorithms and advanced machine learning have been on the radar of United States antitrust agencies as well as, is a much-debated topic amidst the antitrust experts and academia. Federal Trade Commission (FTC) along with U.S Department of Justice (DOJ) Antitrust Division are the agencies responsible to enforce antitrust laws in U.S. FTC has long experience of dealing with a catena of cases involving use of data to materialize anti-competitive conduct, and several being under investigation.

2.3.1 Legislative Framework

The Sherman Act, Section 1 forbids ‘contracts, combinations and conspiracies’ that causes restraint of trade. While the term ‘agreement’ does not find place in the language of the section, with course of development of judicial rulings the ‘contracts, combinations and conspiracies’ have understood to mean existence of some form of ‘agreement’ among market players leading to anti-competitive behavior. The U.S

Supreme Court has clarified as to what encompasses by the term agreement to mean, that there should exist 'unity of purpose or a common design and understanding or meeting of minds' [20] to limit competition.

Algorithms are smart enough to by-pass the conventional modes of concluding agreements, thus competition experts are of understanding that, competitors simply retorting to each other's prices without an agreement of any sort will not attract the provision of Section 1, Sherman Act. DOJ & FTC in the Policy Paper before Organisation for Economic Co-operation and Development (OECD) opines that, "core principle of free market competition is that firms adjust pricing in response to competitive conditions, including the prices charged by competitors".[21] The touchstone for the applicability of Section 1 is "evidence of an overt act of communication" [22], the question that encircles around this parameter is with regard to the extent of explicitness of the communication between the competitors. The concern is how far may we move away from direct, detailed, and reciprocal exchanges of assurances on a common course of action and yet remain within the statutory and conceptual boundaries of an agreement.

The challenge of collusion posed by algorithm can be looked into from yet another perspective, i.e., of Section 5 of the Sherman Act. The understanding reached between the parties leading to supercompetitive prices could be construed as "unfair method of competition". The FTC is of the view that cases pertaining to algorithmic collusion, involving no traces of an "overt act of communication" though not being per se proscribed, can be scrutinised under the rule of reason approach.[23] The effect of per se rule or the rule of reason approach on anti-competitive conduct triggered through algorithms and machine learning software is yet mostly unexplored, thus the extent of viability of this interpretation is still dependent upon outcomes of research program and the analysis therefrom.

2.3.2 Judicial Development

In the *United States v. David Topkins* (2015), US Department of Justice (DOJ) initiated the first criminal prosecution, convicting on the charges of algorithmic pricing. Topkins, an executive at a poster-selling firm, conspired with other sellers on the Amazon Marketplace to fix prices. The meeting of minds occurred between human actors and algorithms were subsequently coded to set the prices in conformity with agreement.[24]

Similar to the Topkins case, another case named *United States v. Daniel Aston and Trod Ltd.* (2015), the director of UK based company was convicted for conspiring with competitors, to collude by monitoring competitor data and maintaining same non-competitive pricing. The case was strategic for displayed the DOJ's willingness to prosecute extraterritorial algorithmic collusion that impacts American consumers.[25]

Next significant development in the US Jurisdiction can be observed in the case of *Meyer v. Kalanick* (2016). The case brought in light the problems of proving hub and spoke model, by proving a "horizontal agreement" among competitors who only interact through a vertical platform. The plaintiff alleged that Uber's CEO, Travis Kalanick, orchestrated a horizontal price-fixing scheme by requiring all independent drivers (the spokes) to use Uber's common pricing algorithm (the hub).[3] The critical question that came to light was whether or not the unilateral acceptance of a platform's algorithm by thousands of independent actors constitute an agreement to fix prices?

Recent significant milestone pertaining to break down of a hub and spoke model was in the case of *In Re RealPage, Rental Software Antitrust Litigation*. The allegations pertained to sharing of non-public data by the landlords with RealPage's "YieldStar" software, which then used an algorithm to suggest rental prices. Even without direct landlord-to-landlord emails, the vertical relationship with RealPage facilitated a horizontal alignment of prices, which is a per se violation of the Sherman Act.[26]

2.4 India

2.4.1 Legislative Framework

The foundation of Indian competition law is Section 3 of the Competition Act, 2002, which prohibits any agreement in respect of production, supply, or distribution that causes an Appreciable Adverse Effect on Competition (AAEC) within India.[27] Section 3(3) provides a "rebuttable presumption" that horizontal agreements (cartels) cause an AAEC. Further to prove an agreement under the Act, "arrangement, understanding, or action in concert," whether or not it is formal or in writing.

The traditional definition was insufficient to handle the complexities of algorithmic collusion. The Competition (Amendment) Act, 2023, introduced a significant proviso to Section 3(3). The amendment attempted to bridge the gap by introducing provisions for ‘Hub-and-Spoke’ arrangements, effectively broadening the scope to include entities that are not engaged in identical or similar trade but participate in or facilitate a horizontal agreement. Post the amendment, for the hub to be made liable its ‘intent’ to participate is sufficient, regardless of whether it has taken any steps to actively engage in it or not, however an existing agreement between the spokes still remains to be established. If a platform’s algorithm is designed to align competitor prices, the platform can no longer claim it is a mere neutral intermediary.

2.4.2 Judicial Interpretation

A significant development towards transparency for algorithmic manipulation can be observed in the case of *Matrimony.com v. Google* (2018), The CCI found Google guilty of ‘Search Bias’. where its algorithm was manually or structurally tuned to favor Google’s own services over competitors.[5] CCI made it evident that even if a process is automated, the design choices made by the humans behind the code can be held liable if they produce an anticompetitive effect.[28]

A landmark case in the domain of hub and spoke model is, *Samir Agrawal v. ANI Technologies Pvt. Ltd.* (Ola/Uber), which progressed from the CCI to the National Company Law Appellate Tribunal (NCLAT) and finally to the Supreme Court of India. The allegation here pertained to automated pricing algorithms used by ride-sharing platforms to facilitate hub and spoke cartel amongst cab drivers. Both CCI and the Apex Court held there must be a horizontal agreement between the spokes (the drivers) to use the hub (the platform) to fix prices for proving existence of hub and spoke cartel. The Court clarified that the algorithm was a vertical service provider, and drivers who act as independent contractors did not ‘agree’ with one another to fix prices; they merely accept the platform’s terms.[29]

3. CROSS-JURISDICTIONAL ANALYSIS OF THE ‘LIABILITY GAP’ AND THE WAY FORWARD

The advent of the digital age and the proliferation of data-driven markets have reshaped the landscape of competition law across all jurisdictions. In this section of the paper the author wishes to discuss the liability gap that has arisen due to self-learning nature of algorithms, in spite of robust regulatory framework. The tradition legislative framework requires ‘meeting of minds’, showing the intention to collude between the individuals to impute the liability on faulting undertaking(s). However, in the case of advanced self-learning algorithms which does not require intent to collude, but rather has a mathematical objective function to fix prices. Thereby creating a liability gap, where the market suffers the harm of a cartel (e.g.: high prices), but the law cannot find a ‘guilty party’ to punish.

3.1 The United States

The U.S. Supreme Court, in *Bell Atlantic Corp. v. Twombly*, established that ‘conscious parallelism’, where companies simply following each other’s prices, provided the decision is taken independently, is not held to be illegal. The logic behind conscious parallelism is that in transparent market the players are aware that cutting prices will ultimately lead to losses for all. To establish tacit collusion ‘plus factors’ including evidence of communication are to be proved.[30] The delinquency arises when algorithms are designed to be ‘predictable’ to each other to match prices without any human-to-human interaction.

Though with a recent paradigm shift in its interpretational approach, DOJ in the case of *In Re RealPage*, argued that if the all the competitors (the spokes) handover their pricing power to a common algorithm (the hub) they would have created an illegal horizontal agreement, even if they never communicated with each other directly. The final decision of the cases is underway, paving way for a new era of algorithmic accountability.

3.2 India

The Indian legal framework is constricted in its scope, the root of the emergency arises from the definition of agreement, where the legislative intent and the interpretation require concordance of wills or a meeting of minds.[27] Furthermore, to establish a hub and spoke cartel model, a strict requirement of proving horizontal link between the spokes is sine qua non. Section 3(3) of the Act is the CCI’s most powerful tool because it allows for a presumption of AAEC. But without foundational proof of an agreement, the

presumption of harm doesn't kick in. In the recent case of Samir Agarwal v. CCI, CCI and later Supreme Court of India emphasised upon the strict requirement of establishment of horizontal agreement between the spokes.

To resolve this the Indian regulators are heading towards a more pragmatic approach of Ex-Ante regulation, with the Draft Digital Competition Bill, 2024. Under the proposed law, instead of trying to prove an agreement after it happens, which becomes impossible with blackbox algorithms, certain types of algorithmic behaviour like self-preferencing or price parity will be prohibited ex ante, before the actual harm may be caused. This approach targets the Systemically Significant Digital Intermediaries (SSDIs), which are identified as entities which are susceptible to market concentration, these include search engines, social networking services, operating systems, and web browsers.[31]

3.3 *European Union*

Unlike USA and India, the legislative ambit of European Union is much wider. Article 101 TFEU prohibits not only the 'agreements' but also 'concerted practices' a much broader category that covers coordination between businesses which, without having reached a formal agreement, knowingly substitute practical cooperation for the risks of competition.[32] Furthermore EU is increasingly applying a logic of special responsibility to firms deploying high-speed pricing algorithms. The reasoning behind is that if an entity is deploying use of blackbox algorithms to determine prices, it later cannot claim ignorance to collusive results of algorithms. The entity deploying such an automated system is presumed to have accepted the risk that the system might coordinate with others. The intent is rooted in the decision to use the algorithm, not in specific pricing outcomes.

3.4 *Russia*

The Russian model deals with the problem of liability gap by applying a purely punitive solution to the algorithmic collusion challenge. The legislative framework categorizes algorithms as an aggravating instrument, thereby circumventing the complex maze of 'meeting of minds' that paralyze other jurisdictions. The Federal Law No. 426-FZ, which amended the Russian Code of Administrative Offences, formally recognized the use of digital algorithms in cartel agreements as a statutory aggravating circumstance.[33] The algorithm is considered as a weapon used in crime, which makes the crime aggravated. However, the crisis still exists as that initial human intent or meeting of minds, is yet a prerequisite to frame the conduct as an offence. This creates a persistent loophole, that while the law increases penalties for human-led cartels that utilize digital tools, it remains silent on autonomous algorithmic coordination where no such human orchestration can be proven.[34]

V. CONCLUSION

The article thereby proceeds to suggestions to bridge the evidentiary and conceptual gap. The thorough study of the jurisdictions across the globe, it can be said that a shift from subjective intent (meeting of mind) to intentional delegation (objective foresight) is required. Regulators must recognize that the act of deploying a high-frequency pricing algorithm into a concentrated market constitutes a foreseeable risk of coordination. To this end, this article proposes a three-pronged global recommendation:

- Adoption of Vicarious Algorithmic liability: where firms are held responsible for the learned behavior of their digital agents. The algorithm age requires regulators to see algorithm not merely as a tool but as a 'Digital Agent' acting on behalf of the firm. If the algorithm optimizes for a collusive equilibrium, the firm cannot claim ignorance of the machine's logic.
- Codification of Digital Plus Factors: The Legislature should move to codify specific circumstantial technical behaviours that satisfy the "agreement" requirement without needing concurrence of wills. By defining statutory plus factors, the burden of proof shifts, allowing regulators to infer a concerted practice from the technical architecture itself.
- Implementation of Compliance by Design Algorithmic models: this recommendation draws its idea from Privacy by Design in General Data Protection Regulations. It is a preventive recommendation that moves enforcement from the courtroom to the engineering phase algorithmic development by the enterprises.

FUNDING STATEMENT

This research received no external funding.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

REFERENCES

- [1]. A. Ezrachi & M. E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*. Cambridge, MA: Harvard University Press, pp. 35-37, 2016.
- [2]. *In Re: Alleged Cartelization in the Airlines Industry*, Suo Motu Case No. 03 of 2015, Competition Commission of India, Feb. 22, 2021.
- [3]. *Meyer v. Kalamick*, Federal Supplement, 3rd Series, vol. 174, 2016, p. 817 (U.S. District Court for the Southern District of N.Y.).
- [4]. *Bell Atl. Corp. v. Twombly*, U.S. Reports, vol. 550, 2007, pp. 553–54.
- [5]. *Matrimony.com Ltd. v. Google LLC*, SCC OnLine CCI, vol. 1, 2018 (Competition Commission of India).
- [6]. *T-Mobile Netherlands BV v. Raad van bestuur van de Nederlandse Mededingingsautoriteit*, European Court Reports, vol. I, 2009, p. 4529, paras. 51–52 (Court of Justice of the European Union).
- [7]. European Commission, “Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings,” *Official Journal of the European Union*, C 31, Feb. 5, 2004. [Online].
- [8]. A. Parziale, “Regulating Algorithms in The European Data-Driven Economy: The Role of Competition Law and Civil Liability,” *Opinio Juris in Comparatione*, vol. 1, no. 1, pp. 97–117, 2020. [Online]
- [9]. European Commission, “Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising,” European Commission, IP/19/1770, 2019. [Online]
- [10]. European Commission, “Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon,” European Commission, IP/19/4291, 2019. [Online]
- [11]. *Constitution of the Russian Federation*, art. 34, cl. 2.
- [12]. *Constitution of the Russian Federation*, art. 8.
- [13]. Russian Federation, “On Amendments to the Federal Law ‘On Protection of Competition’,” Federal Law of the Russian Federation, No. 301-FZ, July 10, 2023. [Online].
- [14]. Federal Antimonopoly Service (FAS) of the Russian Federation, “The Fifth Antimonopoly Package: New Rules for Digital Markets,” Federal Antimonopoly Service of the Russian Federation, 2023. [Online]
- [15]. Federal Antimonopoly Service (FAS) of the Russian Federation, “Recommendations on practices in the use of information technologies in trade, including related to the use of price algorithms,” Federal Antimonopoly Service of the Russian Federation, 2021. [Online]
- [16]. Business Standard, “LG Electronics faces anti-trust violation case in Russia,” *Business Standard*, June 29, 2017. [Online]
- [17]. Federal Antimonopoly Service (FAS) of Russia, “Case against a cartel that used auction robots,” *Federal Antimonopoly Service of the Russian Federation*, June 29, 2017. [Online].
- [18]. K. Tarkhova and V. Alifirov, “Antitrust Concerns Arising from Big Data and ‘Pricing Software’ in Russia,” *Kluwer Competition Law Blog*, June 13, 2019. [Online]
- [19]. Intergovernmental Group of Experts on Competition Law and Policy, “Competition Issues in the Digital Economy,” United Nations Conference on Trade and Development (UNCTAD), July 11, 2019. [Online].
- [20]. *Monsanto Co. v. Spray-Rite Service Corp.*, 465 U.S. 752, 764 (1984).
- [21]. “Algorithms and Collusion - Note by the United States,” Organisation for Economic Co-operation and Development (OECD), DAF/COMP/WD(2017)41, 2017. [Online]
- [22]. J. E. Harrington, Jr., “Developing Competition Law for Collusion by Autonomous Artificial Agents,” *Journal of Competition Law & Economics*, vol. 14, no. 3, pp. 331–363, Sept. 2018. [Online]
- [23]. “FTC Issues Statement of Principles Regarding Enforcement of FTC Act as a Competition Statute,” *Federal Trade Commission*, August 13, 2015. [Online]
- [24]. *U.S. v. Topkins*, No. 3:15-cr-00201, 2015 (U.S. District Court for the Northern District of California). [Online].
- [25]. *U.S. v. Aston*, No. 3:15-cr-00419, Aug. 27, 2015 (U.S. District Court for the Northern District of California). [Online]
- [26]. *In Re RealPage, Inc., Rental Software Antitrust Litig.*, No. 3:23-md-03071, 2023 WL 9004806 (M.D. Tenn. Dec. 28, 2023). [Online].
- [27]. *The Competition Act, 2002*, Act No. 12 of 2003, section 3, 2003.
- [28]. A. Roy, “Anti-competitive Agreement and Competition Law,” in *Competition Law in India: A Practical Guide*, 2nd ed. Alphen aan den Rijn, The Netherlands: Kluwer Law International, 2024, ch. 2, pp. 45–112.



-
- [29]. *Samir Agrawal v. Competition Commission of India*, Supreme Court Cases, vol. 3, 2021, p. 136 (India).
- [30]. M. S. Gal, "Algorithms as Illegal Agreements," *Berkeley Technology Law Journal*, vol. 34, no. 1, pp. 67–118, 2019. [Online].
- [31]. PRS Legislative Research, "Committee Report Summary: Digital Competition Law," *PRS Legislative Research*, March 12, 2024. [Online]
- [32]. European Union, "EU Rules on Concerted Practices and Agreements Between Companies," *EUR-Lex*, 2024.
- [33]. *Federal Law on Amendments to the Code of Administrative Offences of the Russian Federation*, Public Law No. 426-FZ, August 4, 2023.
- [34]. A. Ezrachi and M. E. Stucke, "Sustainable Offline and Online Cartels," in *Research Handbook on Cartels*, P. Whelan, Ed., Cheltenham, UK: Edward Elgar Publishing, 2023, ch. 2, pp. 34–56.