

ILE COMPETITION AND COMPANY LAW JOURNAL

VOLUME 3 AND ISSUE 1 OF 2025

INSTITUTE OF LEGAL EDUCATION

ILE COMPETITION AND COMPANY LAW JOURNAL

APIS – 3920-0028 | ISSN - 2583-8385

(OPEN ACCESS JOURNAL)

Journal's Home Page – https://cclj.iledu.in/

Journal's Editorial Page - https://cclj.iledu.in/editorial-board/

Volume 3 and Issue 1 (Access Full Issue on - https://cclj.iledu.in/category/volume-3-and-issue-1-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in



© Institute of Legal Education

Copyright Disclaimer: All rights are reserve with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For more details refer https://cclj.iledu.in/terms-and-condition/

ILE COMPETITION AND COMPANY LAW JOURNAL

VOLUME 3 AND ISSUE I OF 2025

APIS – 3920-0028 | ISSN - 2583-8385

Published by

Institute of Legal Education

https://iledu.in

ALGORITHMIC ABUSE: DIGITAL GATEKEEPERS RESTRICTING CONSUMER CHOICE AND VIOLATING ANTI TRUST REGULATIONS

AUTHOR - PISHATI PRANAVA, STUDENT AT ALLIANCE UNIVERSITY

BEST CITATION - PISHATI PRANAVA, ALGORITHMIC ABUSE: DIGITAL GATEKEEPERS RESTRICTING CONSUMER CHOICE AND VIOLATING ANTI TRUST REGULATIONS, *ILE COMPETITION AND COMPANY LAW JOURNAL*, 3 (1) OF 2025, PG. 47-59, APIS – 3920-0028 | ISSN - 2583-8385.

Abstract

Algorithms are aimed at optimizing everything. Social media algorithms are integrated into the platform design process for a variety of use cases, including sorting data and ranking content at speeds and scales that people would be unable to achieve. Notably, algorithmic content filtering is the foundation of social media security, preventing unlawful, harmful, or inappropriate content. However, they have progressed to the point that personalising of this data may pose a threat to individuals' privacy and has become a topic of concern in the current times. In accordance with data, only a few huge enterprises continue to dominate the country's internet economy, and consumers face significant risks if these firms continue to consolidate market power. To address these concerns this paper attempts to conduct a comprehensive exploration of the interplay between the abuse of algorithm in today's age with regard to the unlawful anti-trust activities, with a particular focus on its ramifications in the Indian anti-trust laws. This paper also attempts to carefully examine the various functions that algorithm takes on in activities like terms of service, content moderation policies, or strategic partnerships. Digital emphasizing their potential for misuse and the associated security risks and delves into the legal and policy measures adopted by the Indian government to address these issues and to evaluate the provisions in the proposed Digital India Act, 2023 and the existing competition act, 2002, while having a comparative legal analysis to explore legal practices in European union and Canada, identifying structures, differences, and possibilities for legal reform.

Keywords: Algorithm, social media, Data Privacy, content moderation policies, proposed Digital India Act, Competition Act 2002, the General Data Protection Regulation 2016 (GDPR), Personal Information Protection and Electronic Documents Act (PIPEDA).

CHAPTER 1

INTRODUCTION

Algorithms are structured decision-making processes that automate computational procedures to generate decisional outcomes on the basis of data inputs[77]. Algorithms are used to perform a wide range of automated operations. In addition to executing mechanical tasks like an algorithm that predicts when an automobile's antilock braking system will activate, these activities can also involve providing expressive outputs like algorithms that determine a response from a virtual assistant or chatbot.

Algorithms are correlated with analytical competence. The era of big data has arrived because to developments in data science, particularly in the areas of data gathering and storage, which allow algorithms to incorporate a wide range of factors into their choices. Thus, this offers a degree of sophistication that would need a significant amount of time and effort for

[77] Michal S. Gal, *Algorithms as Illegal Agreements*, *Berkeley Technology Law Journal*, Vol. 34, No. 1, pp. 67-118 (2019) <https://www.jstor.org/stable/26755226>

ILE COMPETITION AND COMPANY LAW JOURNAL
VOLUME 3 AND ISSUE I OF 2025
APIS – 3920-0028 | ISSN - 2583-8385
Published by
Institute of Legal Education
https://iledu.in

the human intellect to reach. It follows that the rapid adoption of algorithms in business decision-making is not surprising. Numerous jobs include the use of algorithms, such as evaluating risk, deciding on optimal production and storage levels and locations, and reacting quickly to changes in demand conditions. They're employed in price decisions as well.

The ability to process enormous amounts of data surpasses that of manual computing; algorithm and data together create a new social power; algorithm gradually gains the ability to allocate social resources; algorithm eventually emerges as a new kind of power. The ever-enhanced functional system of algorithms, which includes sorting, search, categorization, and self-optimization, reflects the power basis.

Nonetheless, given the speed at which the Internet and related markets are developing technologically and economically, it is crucial to consider whether antitrust laws in the digital Sector can effectively safeguard consumers without "causing harm from interfering in complex businesses that are both rapidly moving and not fully understood.[78]"

Data plays an important role in the digital industry, supporting the benefits of businesses like Google, Facebook, Amazon, and others. Due to these organisations' capacity to gather vast quantities of personal data of all kinds, customers can receive customised advertising. As more dimensions of data become available to each platform, it seems that the revenues produced from collecting more data from more individuals and on more people get larger, giving incumbent dominant service providers even more advantages[79].

Platforms that compel users to accept obscure, hard-to-understand terms of service that are updated frequently can easily maintain their advantages while keeping users from knowing how their personal data is being used for profit.

There are significant entrance barriers in digital markets. Due to their vast operational size and substantial data base, the leaders in search, social networking, and other platforms enjoy a significant cost advantage[80]. Without comparable customer bases or comparable economies of scales, which are both challenging to acquire swiftly and affordably, entrants typically cannot overcome these[81]. However, the advantages algorithms provide are so crucial sometimes the downsides are overlooked in order to facilitate organisations with these services.

The Puttaswamy caseff[82] is a significant acknowledgment of India's need for data protection. The Supreme Court highlighted the dangers of insufficient personal data protection, which can lead to profiling by combining personal data and leaving people vulnerable to ongoing electronic surveillance. Under Article 21 of the Constitution, the right to privacy was acknowledged as being inextricably linked to the right to life and liberty. The right to meaningful control over one's personal data and the right to informational privacy are just two of the several aspects of this right. In Puttaswamy, the Supreme Court noted that informational privacy through data protection aims to safeguard an individual's identity and autonomy.

The Puttaswamy decision also established the three-part criteria that the state must adhere to when attempting to restrict an individual's privacy: it must exist, have a valid purpose, and limit privacy in a way that is appropriate to those goals[83]. India presently uses the Information Technology Act of 2000 to set regulations governing data protection. The regulations impose duties on body corporates, including upholding a privacy policy and adhering to specific protocols for the

[78] Howard A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, University of Pennsylvania Law Review, Vol. 161, No. 6, pp. 1663-1705 (2013) <https://www.jstor.org/stable/235>
[79] Gene Kimmelman, *Syncing Antitrust and Regulatory Policies to Boost Competition in the Digital Market*, Models for Platform Governance, pp. 44-49, (2019)
[80] Maurice E. Stucke, Ariel Ezrachi, *How Digital Assistants Can Harm Our Economy, Privacy, and Democracy*, *Berkeley Technology Law Journal*, Vol. 32, No. 3, pp. 1239-1300 (2017)
[81] *Supra note 2*
[82] K.S. *Puttaswamy* (Retd.) & Anr. vs. Union of India & Ors.) AIR 2017 SC 4161
[83] *ibid*

acquisition, sharing, and conveyance of personal data. However, an advanced, technologically neutral framework for protecting personal data is needed in light of the expanding problems with data collecting and processing in both the public and commercial sectors. In order to do this, the government presented the parliament with the Personal Data Protection Bill, 2019[84] (PDP Bill). In addition to a notice-and-consent paradigm, the PDP Bill offers a rights-based approach to data protection, giving citizens the ability to access, amend, or remove their data, transfer it, and request to be forgotten.

Despite the fact that our right to privacy is protected by Article 21[85] of the Constitution, the information we share on digital platforms is frequently misused. Companies value our information for targeted advertising and other uses, much like they do with the information we share on social media or online shopping sites. There are still gaps in data protection, even with initiatives like the Personal Data Protection Bill. Users frequently lack control over and understanding of how their data is used. Legislation alone won't provide true safety; technology advancements and public awareness campaigns are also necessary[86]. In summary, even if it is acknowledged, protecting our right to privacy in the digital era is a difficult task that need for more than simply legislative protections.

Review of Literature

Michal S. Gal, *Algorithms as Illegal Agreements*, *Berkeley Technology Law Journal*, (2019)

The application of plus factors and facilitating techniques to algorithms is examined in this paper. The argument that the regulations in place are adequate to address algorithmic-facilitated coordination is disproved by the analysis. This study focuses on how customers and independent transactions can use algorithms to mitigate some of the negative consequences of supplier coordination that is facilitated by algorithms. it also addresses the appropriateness of the current legal mechanisms are to handle algorithmic-facilitated coordination without undermining the efficiency it creates, follows from the failures of such market solutions. The examination looks at three related issues that are fundamental to creating policies that improve welfare.

Niklas Kossow, Svea Windwehr, Matthew Jenkins, *Algorithmic transparency and accountability* (2021)

This paper aimed to outline algorithmic decision-making systems and discuss how opacity in their design and application may encourage unethical behaviour. Although more openness could (partially) solve this problem, the author contends that because algorithmic systems are inherently flawed, transparency is insufficient to eradicate the corruption that these systems encourage. Additionally, this research suggests that policymakers place more emphasis on accountability and transparency in relation to algorithmic system design, training, procurement, and deployment. In the end, the article argues that accountability in the context of algorithms requires a more comprehensive approach; transparency on its own is insufficient.

Bryan Casey, Ashkon Farhangi, Roland Vogl, *Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, *Berkeley Technology Law Journal*, (2019)

This paper focuses on the General Data Protection Regulation's (GDPR) "right to explanation" in social and economic significance. The author suggests that the "right to explanation" that GDPR supposedly offers significant legal ramifications for automated data processing system design, prototyping, field testing, and implementation. The safeguards inherent in the right might not require openness in the shape of a comprehensive, personalised explanation.

[84] Personal Data Protection Bill, 2019
[85] Article 21, The Constitution of India,1950
[86] Gene Kimmelman, *Syncing Antitrust and Regulatory Policies to Boost Competition in the Digital Market*, Models for Platform Governance, (2019).

ILE COMPETITION AND COMPANY LAW JOURNAL
VOLUME 3 AND ISSUE I OF 2025
APIS – 3920-0028 | ISSN - 2583-8385
Published by
Institute of Legal Education
https://iledu.in

However, an all-encompassing comprehension of the DPAs' interpretation shows that the real strength of the right comes from its complementary effects when paired with the algorithmic auditing and "data protection by design" approaches that are outlined in the following chapters of the Regulation.

Howard A. Shelanski, *Information, Innovation, and competition policy for the internet*, *University of Pennsylvania Law Review*, (2013).

The author of this paper presents the views of critics who have questioned the capacity of competition regulators to decide on advantageous regulations in the context of the complexity and rapid change in online markets. This paper addresses those criticisms, arguing that courts and antitrust agencies should assume against antitrust intervention in digital businesses because the error costs associated with over enforcing antitrust rules would be far higher than those associated with underenforcing them. It makes the case that non-price effects pertaining to innovation and information are especially significant for the functioning of online platforms, and that these effects may be the key to improving our comprehension of the costs associated with antitrust enforcement actions as well as the evaluation of the effects of conduct and transactions on competition in the digital industries.

Gene Kimmelman, *Syncing Antitrust and Regulatory Policies to Boost Competition in the Digital Market*, Models for Platform Governance, (2019).

This paper is aimed at understanding the anti-trust regulations in digital markets. The author argues that while antitrust laws can stop abuse, many subtle forms of discrimination are harder to stop. The author also underlined that further barriers are created by consumers' propensity to seek out quick, straightforward, one-stop buying on digital platforms. Customers typically "scroll down to see more search results, they agree to settings chosen by the service, they single-home on one platform, and they generally take actions that favour the status quo and make it difficult for an entrant to attract customers," according to the final report of the Stigler Committee on Digital Platforms (2019, 29).

Gryz, J. & Rojszczak, *M., Black box algorithms and the rights of individuals: no easy solution to the "explainability" problem*, Internet Policy Review,(2021)

This article describes how the General Data Protection Regulation (GDPR), which was enacted by the EU in 2016, gives persons who are the subject of automated decision-making (ADM) the right to an explanation. The researcher also partially relied on this article on the aspect where the authors conclude that the best course to follow would be to use certification frameworks to benchmark automated decision-making algorithms. This would strike a balance between the need to guarantee appropriate protection of individuals' rights and the reasonable expectations of AI technology providers to have their intellectual property rights protected.

Francesco Ducci, *CHAPTER IX Competition Law and Policy Issues in the Sharing Economy*, Law and the "Sharing Economy": Regulating Online Market Platforms, (2018)

This paper backs up the claim that the rise of sharing economy platforms has sparked concerns about competition law, despite their beneficial role in giving many small providers access to the market and encouraging creative ways to offer goods and services. These concerns are primarily related to the worry that these platforms could encourage new types of anti-competitive behaviour and set the stage for potential abuses of market power. These concerns seem to be supported by emerging case law and data regarding the growing market shares and concentration levels held by dominant sharing economy platforms. These data and case law also point to the possibility of the need for more ad hoc enforcement of competition laws due to the unique characteristics of sharing economy markets.

Eric Tucker, Uber and the Unmaking and Remaking of Taxi Capitalisms: Technology, Law, and Resistance in Historical Perspective, Law and the "Sharing Economy": Regulating Online Market Platforms, (2018)

In this paper, the author addresses platform capitalism, and the need to understand that capitalism operates in a variety of ways across time and geography and is not a static system while discussing about Uber. He suggests that this understanding is used in the discussion of the many forms of capitalism, but the main points of contention are the political context in which capitalism operates and the degree to which it is ingrained in certain institutional arrangements. Here, the inner workings of capitalist accumulation regimes are of more interest. This research specifically investigates and attempts to explain the various ways in which workers get absorbed into platform capitalism.

Ryan Calo, Alex Rosenblat, *The taking economy: uber, information and power, Columbia Law Review*, (2017)

The paper addresses how sharing economy companies, like Uber and Airbnb, enable safe online transactions between random users. This generates economic and other benefits, but it also brings up issues that legal literature has started to address, such as racial bias, worker justice, and safety. However, a basic critique of the sharing economy based on power and knowledge asymmetry is absent from the literature.

Jai Vipra and Dhruv Somayajula, *Ensuring Coherence between Personal Data Protection and Algorithmic Accountability: The Role of Fairness, Accountability and Transparency*, Vidhi Centre for Legal Policy(2022).

This article discusses how the status of various rights in the digital domain affects a particular right's ability to be protected. It also emphasises the need to enforce privacy laws in a digital world beset by widespread socioeconomic issues. This suggests that there are significant overlaps between privacy laws and other laws designed to safeguard different rights in a digital environment, and that these overlaps may make it more difficult to resolve disputes and protect rights when comparing the GDPR and PDP bill's accountability and transparency.

Research Problem-

While the digital revolution has brought about greater transparency, connectivity, and search capabilities, it hasn't necessarily resulted in the low rates that many customers had anticipated. An important concern for competition policy is raised by the Internet's and associated markets' rapid technological and economic transformation. While algorithms were developed to maximise user engagement, which can result in content curation based on user preferences and conduct, customised suggestions, and personalised advertisements, it can potentially limit consumer choices by offering customers a more limited selection of options that correspond with their prior preferences or the platform's business objectives, this might decrease the range of options available to consumers.

Research Questions-

1. How do algorithms used by digital gatekeepers affect user experiences and consumer decisions on digital platforms?
2. How can platforms with established algorithm use their control over the market and prioritise their own products or services while limiting competition?
3. What regulatory frameworks and policies are effective in resolving these issues raised under antitrust laws?
4. What ethical implications arise from abuse of algorithm to regulate content on the internet and alter public discourse?

ILE COMPETITION AND COMPANY LAW JOURNAL
VOLUME 3 AND ISSUE I OF 2025
APIS – 3920-0028 | ISSN - 2583-8385
Published by
Institute of Legal Education
https://iledu.in

Objectives-

- To understand the direct effect of misuse of algorithms on consumer decision on digital platforms.
- To evaluate the control of organizations with algorithms over the market
- To assess the regulatory framework and policies that are currently effective in solving issues of both privacy and competition
- To assess the ethical implications, which arise from abuse of algorithm to regulate content on the internet and alter public discourse
- To provide recommendations and suggestions that are appropriate and effective for Indian context.

Hypothesis-

The unregulated use of algorithms by established platforms in India has potential to harm consumers by limiting choices and increasing prices.

Methodology-

The researcher will use a doctrinal methodology to examine the legal implications of algorithm abuse and limiting consumer choices. The researcher gathered primary data from legal databases such as JSTOR, HeinOnline, google scholar, Scconline and Manupatra, as well as material published on the websites of European union and related documents. In addition, secondary data was incorporated from a number of official sources, such as books, websites, codes, and existing surveys. The researcher will employ comparative legal analysis to explore legal practices in European union and Canada, identifying structures, differences, and possibilities for legal reform.

Scope & Limitation of the study-

The study mostly analyses existing laws, regulations, court decisions, and legal principles of European union and Canada as Indian laws are not framed for the purpose of regulating the misuse of algorithm. As a result, it may lack reliable information on the real experiences, views, and cases for algorithm abuse in India as it is so far not regulated or mandated algorithmic transparency under any act. Furthermore, the findings develop from other countries, making it difficult to analyse their direct impact in India. As a result, the researcher faced challenges due to the limited availability of prior research on this subject and constrained access to pertinent data sources.

CHAPTER -2 PRACTICES THAT CONSTITUTE ALGORITHMIC ABUSE

These algorithms are capable of learning from massive amounts of data, and once that data is internalized, they are capable of making decisions experientially or intuitively like humans[87]. The majority of internet platforms employ algorithms to present users with content that is more appropriate for them. This improves the platform's usability and enables it to profit from it. Additionally, in order for these platforms to compete in the market and survive against its competitors, their algorithms must always be upgraded regularly. The platform gains a competitive edge in the market thanks to the algorithm, but this comes with a risk of algorithm misuse that could negatively impact consumers' ability to make decisions, violate their rights and interests, and upend the order of fair competition in the Internet platform market.

Driven by the goal of profit maximisation, Internet platforms have intentionally designed and utilised unreasonable algorithm technology behaviours in order to maintain their daily operation as well as innovation and development[88]. This has left them unable to strike a balance between the development of technology and social ethics, which has resulted in a series of algorithm abuse behaviours.

[87] Wachter, S., Mittelstadt, B., & Russell, C, *Counterfactual explanations without opening the black box: Automated decisions and the GDPR.* Harv. JL & Tech., 31, 841. (2017)
[88] Michal S. Gal, *Algorithms as Illegal Agreements*, *Berkeley Technology Law Journal,* vol 34:67, pp 67-118. (2019)

The short video platform uses the 143-recommendation algorithm to push users false and vulgar content, and it adds unnecessary user tags[89]. Takeout platforms based on big data technology implement the user "kill" operation; members and non-members, iOS and Android system users differ in terms of commodity prices and commodity delivery costs[90]. The short video platform pushes vulgar and false information to users, adds user tags arbitrarily, and creates "addictive recommendations" using the recommendation algorithm; similar behaviours are seen in the precise matching of recommendations made by the e-commerce platform and social platform search results.

Users should be aware of if they are being misused by the algorithm as part of its duty. The phenomenon known as "algorithm abuse → user unknown → more abused by the algorithm" is caused by the algorithm's technical barriers, the asymmetry of consumer information, and the user's lack of choice in the process—which consists of only passively accepting the platform's rules—which means that the user is not immediately aware that they are being abused by the algorithm[91].

The use of "black boxes," or obscure and secretive online algorithms, poses a serious threat to algorithm exploitation of this kind. These operate in a way where the user can only provide data as input and see the outputs that come from the inputs' based on previous exposure[92]. by online companies like Apple, Facebook, Google, and Amazon, yet we have no idea how this information is being utilized. Their policy for algorithms is an ideal representation of a black box.

An artificial intelligence program that is a "black box" will make decisions and predictions just like individuals do, but it won't be able to explain why it makes them[93]. The AI may think in terms of patterns that are invisible to humans, so comprehending it might be similar to comprehending a separate highly intelligent species with completely different senses and perception abilities. This implies that not much can be deduced about the intentions or behaviour of the people who developed or used the AI.

Since an AI's actions or decisions might not reveal anything about the intentions of its creator or user, intent tests that focus on an individual's intent to achieve an illegal result become unsatisfiable; intent tests that examine the reasoning behind an AI's decision or prediction become unsatisfiable; and because intent tests frequently act as a gatekeeper, restricting the range of claims, they might completely stop some claims or legal challenges from being made when AI is involved[94].

Concerns about market dominance and competition in the digital sphere are greatly heightened by the black box algorithm problem. These algorithms give platforms a competitive advantage over their rivals because of their opaque working methods. The opaque nature of these algorithms' workings not only makes it hard for rivals to imitate or compete with them, but it also raises the bar for new players to enter the market[95].
Black box algorithms allow platforms to collect a great deal of user data, frequently without explicit permission or awareness from the user. They can improve their services and recommendations thanks to this immoral data collection, which feeds into a vicious loop of addictive user engagement.

[89] *Ibid.*
[90] Weimin Ouyang, *Research on the Role of Algorithm Transparency in Algorithm Accountability, Shanghai University of Political Science and Law*, Advances in Social Science, Education and Humanities Research, volume 385 (ICEEMR 2019)
[91] Vidovic, M. M.-C., Görnitz, N., Müller, K.-R., Rätsch, G., & Kloft, M. *Opening the Black Box: Revealing Interpretable Sequence Motifs in Kernel-Based Learning Algorithms. In Machine Learning and Knowledge Discovery in Databases*, Springer International Publishing.(2015) https://doi.o rg/10.1007/978-3-319-23525-7_9
[92] *Ibid*
[93] Gryz, J. & Rojszczak, *M., Black box algorithms and the rights of individuals: no easy solution to the "explainability" problem*, Internet Policy Review, 10(2).(2021) https://doi.org/10.14763/2021.2.1564
[94] Yavar Bathaee, *the artificial intelligence black box and the failure of intent and causation*, Harvard Journal of Law & Technology Volume 31, Number 2 Spring (2018).
[95] *Supra note 13*

ILE COMPETITION AND COMPANY LAW JOURNAL
VOLUME 3 AND ISSUE I OF 2025
APIS – 3920-0028 | ISSN - 2583-8385
Published by
Institute of Legal Education
https://iledu.in

Users might find themselves attracted back into these platforms on a regular basis, frequently without fully understanding how their data is being used or the possible repercussions of their interactions. As a consequence, platforms with access to black box algorithms may create and preserve dominance in the market. They have a distinct advantage over competitors who could find it difficult to compete in the market because the platforms with black box algorithms have capacity to monopolize user attention and data. Moreover, worries about privacy and user autonomy are made worse by the dominance attained by unethical data methods.

CHAPTER -3 REGULATION ALGORITHM TRANSPARENCY UNDER GENERAL DATA PROTECTION REGULATION AND PERSONAL DATA PROTECTION BILL

Regarding algorithmic transparency, government agencies have implemented a variety of laws and rules to control the sound evolution of platform algorithms. Additionally, collaborative efforts have been made to advance the governance of Internet platform algorithms, pointing the way towards a global framework for diverse algorithm governance patterns. As a result, the governance of algorithms has reached a new level. Nonetheless, it is clear that governance and development are not aligned given the grave consequences of today's data breaches.

Of all the governance models and rules established, GDPR is most recognised for taking a novel approach to transparency by introducing the right to explanation. One of the objectives of the GDPR was to modify EU laws to accommodate contemporary data processing techniques like big data and cloud computing. As a result, the EU legislature expanded already-existing laws, such as those pertaining to the right to information and automated decision-making, and added a number of new ones, such as the much-discussed right to data portability.

Every person has the right to know the extent of the data that is processed about them and the reason behind it, as per the EU data protection model. Additionally, the GDPR, 2016 states in Article 12(1)[96] that the data controller must give them this information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language." The right to privacy and the right to personal data protection are protected under EU law and are listed in the 2012 Catalogue of Fundamental Rights[97]. It should also be mentioned that while though these rights are intimately linked, they are separate rights in and of themselves. This implies, especially, that data protection regulations may be violated even in cases where privacy is unaffected[98], at least as far as EU law is concerned.

Without a question, one of the primary objectives of enacting laws specifically regarding data protection is to safeguard people's rights and freedoms in the digital age and guard them from current threats brought about by the quick advancement of technology and the internationalisation of contemporary IT services. In line with this objective, Article 22 of the GDPR establishes the right to be free from decisions that are made based on automated data processing and that have a substantial influence on an individual's life or legal status. The GDPR's predecessor, Directive 95/46, which was in effect for more than 20 years, also contained references to this legislation[99]. However, this clause has little practical impact because bulk algorithmic processing of personal data has only advanced significantly in the previous 20 years. The rise in profiling—including profiling for uses other than promoting goods and services—has altered the landscape. It is important to note that the right of an individual to an explanation of an

[96] Article 12(1), General Data Protection Regulation
[97] CFR, 2012
[98] Ansgar Koene, 'A governance framework for algorithmic accountability and transparency', European Parliament (2019)

[99] Bryan Casey, Ashkon Farhangi, Roland Vogl, *Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, *Berkeley Technology Law Journal*, Vol 34:133, pp 143-188, (2019).

automated decision is not expressly stated in Article 22 of the GDPR. Rather, it lays forth the broad idea that a person has the right to object to automated decision-making[100].

By adding the requirement to provide "meaningful information" on the reasoning behind automated decision-making in Article 15(1)(h) of the GDPR, the EU legislature expanded the information obligation placed on data controllers to include the "significance and the envisaged consequences of such processing for the data subject." and even while the phrase "right to explanation" does not directly appear in the rule's wording, it is this regulation that is the basis of the term[101].

Similar to the accountability concept outlined in the GDPR, this principle of accountability required data controllers to be accountable for adhering to measures that give effect to data protection standards. The PDP Bill 2019 reflects this idea, stating that the data fiduciary is in charge of adhering to legal requirements. Furthermore, in order to prove compliance with the PDP Bill's requirements, particular duties to keep and distribute documents and carry out recurring audits support this general obligation. Under this law, the proposed Data Protection Authority of India is responsible for monitoring compliance and has the authority to publish rules of practice that will help data fiduciaries fulfil their duties. Crucially, algorithmic accountability is not a topic that the PDP Bill 2019 specifically addresses. Key data protection principles are outlined in Article 5(1) of the GDPR and serve as a guide for data processing companies' operations. In accordance with the GDPR, personal data must be processed "lawfully, fairly, and transparently with respect to the data subject.[102]"

Based on the fairness principle outlined in the Srikrishna Report, the PDP Bill 2019 places purpose constraints on data processing corporations. According to Clause 5 of the PDP Bill 2019, data fiduciaries must: (a) process personal data fairly and reasonably; (b) use it for purposes approved by the data principal and for which the data principal may reasonably expect it to be used, taking into account the purpose, the context, and the circumstances of the data's collection. Nevertheless, the fairness of algorithms[103] is not specifically taken into account in the initial text of PDP Bill 2019. In an effort to overcome this gap, the JPC Report mandates that data fiduciaries reveal the algorithmic fairness of personal data in order to guard against algorithmic abuse.

The PDP Bill 2019 which is yet to come into force has transparency as a central topic for data protection. A privacy-by-design policy must be prepared and published by each data fiduciary, among other general transparency requirements. Furthermore, the PDP Bill 2019 places particular disclosure requirements on data fiduciaries to advise data principals about the types of personal data processed, their rights, the reason for processing the data, and any unusual reasons for processing that could put the data subject at serious risk of harm[104].

Part of the rationale behind the JPC Report's[105] advice to data principals about the fairness of algorithms or data processing techniques was the necessity of guaranteeing the transparency of the algorithms that digital organisations employ to process personal data.

While PDP is in place for algorithm transparency, the Section 4[106] of the Competition Act, 2002 provides for prohibition of abuse of dominant position, the sub clause (c) emphasises that indulging in practice or practices resulting in

[100] Wachter, S., Mittelstadt, B., & Floridi, L. *Why a right to explanation of automated decision making does not exist in the general data protection regulation.* International Data Privacy Law, 7(2), 76–99. (2017) https://doi.org/10.1093/idpl/ipx005
[101] *Supra note 20*
[102] Margaret Mitchell, 'Model cards for model reporting', Proceedings of the conference on fairness, accountability, and transparency (2019) https://arxiv.org/pdf/1810.03993.pdf
[103] *Supra note 22*
[104] Jai Vipra and Dhruv Somayajula, *Ensuring Coherence between Personal Data Protection and Algorithmic Accountability: The Role of Fairness, Accountability and Transparency*, Vidhi Centre for Legal Policy(2022).
[105] The Joint Parliamentary Committee (***JPC***) on the Personal Data Protection Bill, 2019
[106] Competition Act,2002

ILE COMPETITION AND COMPANY LAW JOURNAL
VOLUME 3 AND ISSUE I OF 2025
APIS – 3920-0028 | ISSN - 2583-8385
Published by
Institute of Legal Education
https://iledu.in

denial of market access [in any manner]; would amount to the enterprise being in dominant position. For the same a punishment can, be up to 10% of the normal turnover for the last three preceding financial years of endless supply of such people or ventures[107]. And the preamble of the act emphasises the objective of the act is "to promote and sustain competition in markets, to protect the interests of consumers".

The Competition Act poses difficulties when algorithms are used to sway customer decisions, particularly when they are used to push recommendations that are designed in a way to be addictive. Due to the uncertainty around the definition of a market, it is challenging to determine the pertinent market that these algorithms affect. Since all of the markets might be viewed as one, it is challenging to determine which platforms are dominant in the market by using standard indicators. It becomes difficult to prove anti-competitive behaviour in the absence of thorough knowledge of algorithmic operations.

CHAPTER -4 ALGORITHMIC TRANSPARENCY AS A REMEDY

The most widely accepted solution to stop algorithm abuse is algorithm transparency. It is thought that greater transparency about the inner workings of these algorithms will provide users with knowledge and regulators with oversight powers. When users possess knowledge about how algorithms function, they may make more educated choices regarding their digital interactions, and regulators can more effectively evaluate and rectify any potential biases or discriminatory practices.

Nonetheless, this ostensibly simple solution poses noteworthy obstacles for the platforms themselves. Algorithms are essential to platforms' competitiveness and value proposition; they are not only tools. These algorithms, which represent priceless intellectual property and trade secrets, are frequently the result of substantial research and investment. Overly openness runs the risk of disclosing this exclusive technology, making it easier for rivals to copy or even surpass them[108]. This weakens incentives for further innovation in algorithmic technology as well as the original platform's competitive edge. While excessive algorithm transparency can lower the cost for government departments to understand algorithms and raise user understanding of them, platforms view algorithm technology as a core competitive advantage, and excessive disclosure encourages competitors to copy and imitate their work, leak trade secrets, and stifle technological innovation within their own businesses[109]. This might also destroy confidentiality.

Moreover, consumers and regulators might not always get the results they want from excessive transparency. Even with complete transparency, many algorithms are hard to grasp due to their extreme complexity, which might result in misconceptions or misinterpretations[110]. Furthermore, disclosing specific algorithmic details could unintentionally reveal security weaknesses or vulnerabilities that could be used by bad actors, endangering the security of users' devices as well as that of platforms.

As previously mentioned, individuals may find themselves drawn back to these platforms on a regular basis, often without fully realising the implications of their activities or how their data is being utilised. Even in cases when algorithmic openness—such as that provided by the GDPR—is present, it is critical to recognise that these algorithms are frequently incomprehensible to humans, making the transparency pointless in

[107] Google INC & Ors. v. Competition Commission of India (2022).

[108] De-Laat, P. B. *"Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?"* Philosophy & Technology (31:4), pp. 525-541 (2018).

[109] Ananny, M., & Crawford, K. 2018. *"Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability"*, new media & society, 20(3), 973989.

[110] Zhao, R., Benbasat, I., and Cavusoglu, H. *"Do users always want to know more? Investigating the relationship between system transparency and users' trust in advice-giving systems,"* in *ECIS 2019 Proceedings* (2019).

ILE COMPETITION AND COMPANY LAW JOURNAL
VOLUME 3 AND ISSUE I OF 2025
APIS – 3920-0028 | ISSN - 2583-8385
Published by
Institute of Legal Education
https://iledu.in

light of the possibility that users may remain ignorant of them[111].

Strict accountability for harm caused by AI or regulation of the level of transparency AI must demonstrate are two potential (though ultimately ineffective) answers to these issues. Both approaches have flaws, are lacking, and most likely won't work as powerful tools to control AI.

A detailed regulation framework governing AI transparency will probably put an end to new AI technology firms since they would have to pay exorbitant fees for regulatory compliance and deal with restrictions on their ability to create new products. Furthermore, there is no assurance that specific machine learning and AI programmes will be created with greater transparency. Unregulated algorithms, on the other hand, result in a concentrated market structure, protecting a small number of rivals with significant hurdles to entry, which creates an environment that is very favourable to coordination.

A dilemma arises regarding the proper course of action to address the impact of algorithms on consumer decisions: while strict regulation of algorithms may place a heavy financial burden on new entrants, making it extremely difficult for them to comply with such policies and enter the market, minimal transparency regarding algorithms may keep regulators and users in the dark about how they operate, potentially exacerbating the issues related to algorithmic manipulation. Finding the right balance between transparency and regulation is essential to effectively addressing these concerns while maintaining fair competition and consumer protection in the digital landscape.

CHAPTER-5 PROPOSING GUIDELNES FOR REGULATING ALGORITHM

It will become more difficult to decide between "strict governance" and "innovation and development" if the platform algorithm misuse is not curbed in a timely manner. Platforms must provide pertinent algorithm information, but the amount of information must be carefully examined in order to prevent both too little and too much disclosure that could violate platform trade secrets or hinder the effective control of algorithm misuse. The primary concern at this point is not "whether the algorithm is transparent," but rather "the degree of transparency of the algorithm."[112] This is demonstrated by the government, which is the leading authority on algorithm governance and is promoting algorithm transparency through pertinent laws, policies, and industry regulations.

Adding a sliding scale to the intent and causation requirements that takes into account the degree of Algorithm transparency and human oversight would be a preferable approach. However, when AI acts on its own, responsibility should depend on how transparent the AI is, what limitations its designers or users have set on it, and how closely its behaviour is observed. As AI systems grow more autonomous, questions regarding how much human influence influences their decisions and actions arise. Furthermore, it becomes more challenging to establish intent and causality when dealing with AI systems due to their ambiguity.

According to the suggested changes to the intent and causation test, a sliding scale method based on the degree of AI transparency and human oversight should be included[113]. This means that when AI systems become more autonomous, responsibility should be evaluated according to elements like the AI's decision-making process' transparency, the limitations placed on it by its designers or users, and the degree of care used to observe its behaviour.

When it comes to algorithm transparency, the intention and causation test has a lot to offer. It

[111] Krishnan, M., Against Interpretability: A Critical Examination of the Interpretability Problem in Machine Learning. Philosophy & Technology, (2019)

[112] N. Diakopoulos, *"Accountability in Algorithmic Decision Making,"* Communications of the ACM, Vol 59, No. 2. pp. 56-62. (2016)

[113] Zúñiga, N, *Does more transparency improve accountability?,* U4 Anti-Corruption Helpdesk (2019).

offers clarity in establishing accountability and responsibility by assessing the motivations underlying algorithmic actions as well as the causal connections to the harm that results[114]. This paradigm facilitates targeted accountability measures by clearly defining the roles of different stakeholders engaged in algorithm creation, implementation, and oversight. Additionally, it encourages developers and operators to divulge information about their algorithms in order to reduce liability risks, hence promoting greater openness in algorithmic operations. All of these advantages work together to ensure accountability in algorithmic decision-making processes and to encourage the ethical and responsible usage of algorithms.

CHAPTER-6 CONCLUSION

In conclusion, algorithm transparency presents a promising solution to algorithm misuse, but its application needs to be carefully considered to prevent unforeseen effects. Achieving openness while maintaining platforms' competitive edge and fostering innovation calls for sophisticated strategies that take into account the interests of all parties involved. In order to protect the integrity of proprietary technology, promote transparency where it is appropriate, and encourage ongoing innovation in the digital ecosystem, regulatory frameworks should strive to achieve this delicate balance. Along with the transparency provisions it is suggested that the intent and causation test be applied as a supervisory approach.

The extensive usage of algorithms could lead to issues for all parties involved in the absence of regulation. These covert systems have the potential to influence people's decisions and privacy. Unfair treatment may result from this, particularly for some groups. In the business sector, large corporations may employ algorithms to stifle rivalry and make it difficult for smaller ones to thrive. Additionally, without guidelines to follow, businesses that use algorithms could encounter criticism if something goes wrong, harming their brand and putting them in legal hot water. Therefore, if algorithms are used without regulation, it could lead to a lot of issues for everyone.

The hypothesis is here by proved as positive.

REFERENCES

- Jai Vipra and Dhruv Somayajula, *Ensuring Coherence between Personal Data Protection and Algorithmic Accountability: The Role of Fairness, Accountability and Transparency*, Vidhi Centre for Legal Policy(2022).
- Gryz, J. & Rojszczak, *M., Black box algorithms and the rights of individuals: no easy solution to the "explainability" problem*, Internet Policy Review, 10(2).(2021) https://doi.org/10.14763/2021.2.1564
- Yavar Bathaee, *the artificial intelligence black box and the failure of intent and causation*, Harvard Journal of Law & Technology Volume 31, Number 2 Spring (2018)
- Weimin Ouyang, *Research on the Role of Algorithm Transparency in Algorithm Accountability, Shanghai University of Political Science and Law*, Advances in Social Science, Education and Humanities Research, volume 385 (ICEEMR 2019)
- De-Laat, P. B. *"Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?"* Philosophy & Technology (31:4), pp. 525-541 (2018).
- Zhao, R., Benbasat, I., and Cavusoglu, H. *"Do users always want to know more? Investigating the relationship between system transparency and users' trust in advice-giving systems,"* in *ECIS 2019 Proceedings* (2019).
- N. Diakopoulos, *"Accountability in Algorithmic Decision Making,"*

[114] Niklas Kossow, Svea Windwehr, Matthew Jenkins, *Algorithmic transparency and accountability*, Transparent international knowledge hub (2021)

Communications of the ACM, Vol 59, No. 2. pp. 56-62. (2016)

- Vidovic, M. M.-C., Görnitz, N., Müller, K.-R., Rätsch, G., & Kloft, M. *Opening the Black Box: Revealing Interpretable Sequence Motifs in Kernel-Based Learning Algorithms. In Machine Learning and Knowledge Discovery in Databases*, Springer International Publishing.(2015) https://doi.o rg/10.1007/978-3-319-23525-7_9
- Wachter, S., Mittelstadt, B., & Floridi, L. *Why a right to explanation of automated decision making does not exist in the general data protection regulation.* International Data Privacy Law, 7(2), 76–99. (2017) https://doi.org/10.1093/idpl/ipx005
- Krishnan, M., Against Interpretability: *A Critical Examination of the Interpretability Problem in Machine Learning.* Philosophy & Technology, (2019)
- Margaret Mitchell, *'Model cards for model reporting'*, Proceedings of the conference on fairness, accountability, and transparency (2019) https://arxiv.org/pdf/1810.03993.pdf
- Ansgar Koene, *'A governance framework for algorithmic accountability and transparency',* European Parliament (2019)
- Michal S. Gal, *Algorithms as Illegal Agreements*, *Berkeley Technology Law Journal,* vol 34:67, pp 67-118. (2019)
- Zúñiga, N, *Does more transparency improve accountability?,* U4 Anti-Corruption Helpdesk (2019).
- Niklas Kossow, Svea Windwehr, Matthew Jenkins, *Algorithmic transparency and accountability,* Transparent international knowledge hub (2021)
- Wachter, S., Mittelstadt, B., & Russell, C, *Counterfactual explanations without opening the black box: Automated decisions and the GDPR.* Harv. JL & Tech., 31, 841. (2017)
- Ananny, M., & Crawford, K. 2018. *"Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability",* new media & society, 20(3), 973989.
- Bryan Casey, Ashkon Farhangi, Roland Vogl, *Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, *Berkeley Technology Law Journal,* Vol 34:133, pp 143-188, (2019).
- Howard A. Shelanski *Information, Innovation, and Competition Policy for the Internet*,161 U.PA.L.REV. 1663(2013). https://scholarship.law.upenn.edu/penn_law_review/vol161/iss6/6
- Competition Act, 2002
- General Data Protection Regulation, 2016
- Privacy Data Protection bill, 2019
- K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.) AIR 2017 SC 4161