
AI-DRIVEN CONSUMER HARM

Chahak Jain, BA LLB (Hons.), Manipal University Jaipur

ABSTRACT

The framework for consumer protection in India is fundamentally unfit to deal with the problems presented by artificial intelligence technology. There is a lack of transparency about algorithms¹, which gives rise to a major problem of accountability. Consumers have no awareness about how certain decisions, such as price setting, among others, were made by AI. Not only does the absence of knowledge of the decision-making process make it difficult for consumers to contest any decision, but it also makes it difficult for regulatory agencies, as they have no knowledge of the decision-making process.

No less important is the fragmented character of the regulatory regime². Harm created through the use of AI does not fit into the spheres of consumer, data, or competition regulation. Instead, it overlaps with these areas. The lack of a holistic approach leads to the overlap of competencies and regulation loopholes that impede addressing systemic threats. Ultimately, such a state of affairs leads to the deterioration of the legal system's ability to address technological threats.

Lastly, the regulation is normatively outmoded. It still operates under the assumption that consumers make decisions rationally³, while, in reality, they are subject to manipulation. Unless the regulation addresses systemic rather than individual concerns, it will fail to be relevant in modern digital markets.

¹ Frank Pasquale, *The Black Box Society* (Harvard Univ. Press 2015)

² Anu Bradford, *The Brussels Effect* (Oxford Univ. Press 2020).

³ Oren Bar-Gill, *Seduction by Contract* (Oxford Univ. Press 2012).

INTRODUCTION

Lawrence Lessig famously stated that "code is law"⁴ because he emphasizes the ability of digital architectures to regulate human behavior more than traditional systems do. His observations are most important and most concerning, in relation to artificial intelligence (AI)-based consumer markets, which have gone from being thought of as a neutral tool aimed at improving efficiency to now using AI's transformative power to define the structure of consumer actions by determining and projecting consumer behavior.

In today's digital marketplace, there are no longer free and informed choices for consumers; rather, they exist in an environment governed by algorithms and where their decisions are made obscurely through algorithmic systems' implicit routing and were created to maximize engagement and profit⁵. The AI in today's digital marketplace acts as an invisible intermediary between advertisers and consumers and employs tactics to influence the choice of both groups without consumers even being aware of how they are being affected or manipulated.

In this essay, I argue that the development of consumer harm associated with Artificial Intelligence will change the way that markets function, and that consumer protection laws in India currently cannot provide the protections necessary for harm associated with AI to be addressed properly. The Consumer Protection Act of 2019⁶ and the Digital Personal Data Protection Act of 2023⁷ are based on outdated views of what rational behaviour is, how transparent information is, and the way that we can specifically identify harm. AI creates consumer harm that is less easily identifiable, systemic, and has multiple actors who contribute to the harm.

Drawing on theories relating to regulation and comparative regulation, this paper argues that to protect consumers in the algorithmic era, we need to move towards algorithmic accountability, develop regulations prior to AI being made available for use, and implement substantial fairness in all acts related to AI. If we do not make these changes to the law, then we will lose control of the normative value framework governing technology and how technology will govern consumers through the choices they make.

⁴ Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

⁵ Shoshana Zuboff, *The Age of Surveillance Capitalism* (Public Affairs 2019).

⁶ Consumer Protection Act, No. 35 of 2019, India Code (2019).

⁷ Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

How Consumer Markets are Changing: Switching from Free Choice to Free to Be Controlled

The foundation of all consumer protection laws is grounded in the idea that each person has control over his/her desires, whereby he/she can choose what to purchase using rational thought based upon relevant information before the purchase. With AI changing the way in which people make their choices, this foundational concept will no longer exist.

AI does more than just provide an outcome that the consumer wants. The AI Systems create their own preferences for the consumer based on how often customers have purchased an item, what items are available, and how they were given access to that item. The design and the method in which a platform presents its items is called “choice architecture,”⁸ and this is what can turn a traditional market into a market where consumers can be influenced in how they make a purchase decision.

Authors Cass Sunstein and Richard Thaler have conducted significant research that shows that small “nudges” can have a large impact on a consumer's decision-making; however, as it pertains to AI, the nudges are based on how the technology is devised and how that technology guides consumers in making a purchase. Therefore, this creates a way of saying that the consumer is being paternalistically guided by the AI Algorithms that are created to be helpful to the consumer. Dynamic pricing complicates the situation even more. Through big data⁹, AI networks are able to set unique prices for every customer based on how much they are willing to spend. Price discrimination is not illegal by itself; however, pricing algorithms being used to determine prices create issues of equity and transparency.

Under these circumstances, the consumer is no longer making independent decisions, but rather is being treated as a data subject living in a predictive system, causing many questions regarding the legitimacy of market results.

Data's Limitations and the Illusion of Consenting to Data Practices

The use of consent as a regulatory principle is becoming more common, but as the way we use data/AI has evolved, the standard of using consent as a method for validating our use of data/AI

⁸ Cass R. Sunstein & Richard H. Thaler, *Nudge* (Yale Univ. Press 2008).

⁹ OECD, *Personalized Pricing in the Digital Era* (2018).

has become less effective.

In the modern ecosystem of Data and AI, informed consent is almost impossible¹⁰ because both the complexity of the usage of data and the lack of clarity in privacy policies do not allow consumers to provide informed consent. Consumers are agreeing to the terms of use without necessarily knowing or understanding how their data will be used, disclosed, or analyzed. The issue finds its roots within the Constitution of India in *Puttaswamy vs Union of India*¹¹. In the landmark ruling, the Supreme Court identified information privacy as an important component of personal autonomy. The judgment also highlights the importance of meaningful and informed consent, thereby raising doubts about uninformed or general consent processes prevailing within the digital economy.

The actual or potential harm caused by data/AI processes is not created from the collection of data, but from the way that data is used to create assumptions and manipulate the way people behave.

According to Shoshana Zuboff, one of the defining characteristics of today's digital economy is the development of "surveillance capitalism." In this context, people's personal data is turned into a commodity that is used to predict and influence how people behave. Consent is then used as a way of legitimizing the use of someone's data rather than being a way of protecting the consumer. One such act is the Digital Personal Data Protection Act (2023) in India that has been framed by the Government of India. Nevertheless, the act focuses only on one major aspect of the regulation of data usage, that is, consent, while ignoring another vital issue relating to algorithmic power over consumers. Although consumers may give consent for the use of their data, they are still at risk of being harmed when their data is processed and/or used by Algorithms.

Therefore, as regulators continue to develop regulatory frameworks for data, the focus of regulators must shift from how data is collected to how data is used. It is important to recognize that the actual or potential harm created by data/AI usage does not occur because data has been collected, but rather from the decisions made by Algorithms using the collected data.

¹⁰ Solove, Daniel J., *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013).

¹¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

Opacity, Prejudice, and the Rise of Unseen Harm

The emergence of AI provides a new type of harm that is both widespread and incredibly hard to find. AI-induced harm, as opposed to typical consumer harm that is generally visible and traceable, has an opaque, probabilistically-based, and multifaceted aspect to it.

Many AI platforms are "black boxes," which leaves consumers unable to learn how the platform arrived at their decision, whether it relates to lending, purchasing, or pricing; this lack of transparency creates issues with both accountability and the possibility of obtaining a remedy in relation to those decisions. The second layer that impacts the existence of this new type of harm is algorithmic bias¹². AI's use of historical data to train algorithms results in algorithms replicating and even enhancing pre-existing disparities between different demographics. For example, some pricing algorithms disadvantage select demographics, while other algorithms used by recommendation engines perpetuate certain stereotypes.

The reality is that these new forms of harm can be produced without any sort of intentional wrongdoing on the part of either the creators of the algorithm or the individual actors who are impacted by that algorithm. Harm arises as a product of data, coding, and context; developing laws that address this type of harm presents a critical dilemma for the legal community - to develop laws that prevent the infliction of injury when that injury is not easily identifiable as either visible or intentional, but will have profound consequences.

Liability Crisis with AI

Artificial intelligence threatens to disrupt long-held beliefs about legal responsibility. Traditional liability systems are based on clear causation and identifiable actors, whereas AI systems utilize a form of complicated agent-based interaction, where there are often multiple parties involved¹³ in the process, such as developers, deployers, and data providers.

When there is an incident that results in harm, it often becomes difficult to determine who or what is responsible. Is the programmer of the algorithm ultimately liable? Or is there an obligation on behalf of the manufacturer who implemented the algorithm in their product? Or could it be that the data that was used to train the machine or inform its decisions is where legal

¹² Barocas & Selbst, *Big Data's Disparate Impact*, 104 Calif. L. Rev. 671 (2016).

¹³ Marchant & Lindor, *The Coming Collision Between Autonomous Vehicles and the Liability System*, 52 Santa Clara L. Rev. 1321 (2012).

liability lies? Each time this type of scenario arises, it is difficult to provide a precise answer, leaving a vacuum of regulatory control.

The Consumer Protection Act (2019) in India fails to adequately address the issues presented in this complex reality of liability associated with the use of AI technologies. The Act presupposes a certain level of intention and control on behalf of the parties involved in an unfair trade practice, an assumption that AI technologies cannot satisfy due to the diffuse nature of their operation.

When liability is diffused among multiple parties, there are fewer incentives for companies to accept their own liability, resulting in companies often externalizing the risk associated with using AI technologies in the marketplace. As long as there are no defined legal standards for the use of algorithm-based applications, AI technologies will continue to operate in an environment where there is no regulated responsibility.

India's consumer protection system has a number of structural deficiencies.

The challenges presented by AI are not simply an extension of existing consumer risks but reveal fundamental weaknesses within India's current consumer protection architecture. These structural deficiencies are built into the design, orientation, and assumptions of the existing legal framework.

Firstly, Indian Consumer protection laws are reactive in nature¹⁴, while the damage caused by AI is proximate to nature and systemic. For instance, the Consumer Protection Act 2019 is intended to remedy particular cases where there is clear and concrete damage that could be attributed to the use of defective goods, deceptive advertising, and unfair business practices; but the AI systems are not separate cases of damage. Instead, they continuously produce outputs from inputs in a chain reaction of impacts on the consumer's behavior. In this respect, harm from AI systems will often be cumulative rather than immediate. For example, an algorithm may assist consumers in making decisions by nudging them in the right direction; however, it may not create an immediate and specific injury, but rather will distort the consumer's choice and freedom over time.

There is a severe deficit of institutional and technical capacity within regulatory bodies because

¹⁴ Brownsword, Roger, *Law, Technology and Society* (Routledge 2019).

regulation requires both legal authority and an understanding of and the tools to audit AI systems. Regulatory institutions in India, such as those related to consumer protection, do not have sufficient technological expertise on staff or the proper tools to perform audits of algorithmic systems. The operation of AI involves complex models, large volumes of data, and dynamic learning mechanisms that are not well understood via traditional legal analysis. Without interdisciplinary expertise, the regulators are in a structurally inferior position to corporations that have large amounts of technological infrastructure and proprietary know-how. As a result of this imbalance, there is regulatory asymmetry, meaning there is ineffective enforcement not due to intent, but because of capacity issues. So, even if the legal provisions are drafted well, they are unlikely to be enforced in practice.

When companies do not have to provide clear information about their algorithms, it is difficult to hold them liable for their actions. The lack of transparency makes it impossible to enforce consumers' rights. This lack of transparency hides the algorithms from scrutiny. Transparency should not only be defined as technical disclosures or statements of the Company's algorithm policy; the Company also needs to provide the consumer with a meaningful explanation. The consumer must be provided with easy-to-understand information regarding the algorithm utilized, which allows a consumer to either understand how a Company's algorithm has made a decision on a consumer or, if appropriate, contest a Company's algorithm decision. Without transparency and explanations for algorithm decisions, legal rights are almost theoretical and not enforceable.

Lastly, the present framework is outdated from the normative perspective insofar as it operates under the assumption that AI has changed everything about consumer behaviour and the nature of markets and transactions. Traditional consumer protection theory rests upon the principle of consumers' rational and informed choice, while the markets that rely on AI operate under the conditions of informational asymmetries, consumer manipulation, and prediction, thus making the traditional consumer an obsolete concept. As long as the basic legal principles do not undergo fundamental reconsideration, the law will prove insufficient.

Comparative Insights: Proactive Governance of AI

There is much to learn from the development of regulations around the world. One of the leaders in regulating AI governance is the EU, which adopted a risk-based approach¹⁵ to the

¹⁵ Proposal for a Regulation on Artificial Intelligence (Artificial Intelligence Act), COM/2021/206 final.

regulation of AI applications. Categorizing AI systems according to their impacts, it makes them accountable and focuses on prevention.

Transparency, accountability, and oversight of humans over machines are some essential components of the proactive approach towards AI regulation. AI applications in industries considered to be high risk will go through strict regulatory measures, such as audits. At the same time, discussions about AI regulation in India have only recently begun. If there is no sufficient regulation, there is a high probability of developing negative practices.

"Those who control data control the future," says Yuval Noah Harari¹⁶. The lack of proper regulations makes it possible to control consumers and the future of democracy.

Towards an Algorithmic Accountability Regime

To effectively counter the adverse consequences of AI on consumers, a shift in focus is necessary.

Firstly, algorithmic accountability¹⁷ has to be at the forefront of any legal framework. It must be ensured that those using AI technologies cannot absolve themselves from legal responsibility.

Secondly, the concept of transparency has to move beyond mere lip service. There should be a provision for consumers to receive comprehensive and substantive explanations regarding decision-making processes, especially in high-impact situations.

Thirdly, it is crucial to introduce an algorithmic audit¹⁸ mechanism. This will help detect possible problems, monitor compliance, and restore confidence.

Fourthly, there should be a risk-based strategy. It should be focused on those areas where AI usage affects consumers the most.

Lastly, consumer protection policies have to be placed into a larger context of digital rights.

¹⁶ Yuval Noah Harari, *21 Lessons for the 21st Century* (2018).

¹⁷ Selbst et al., *Fairness and Abstraction in Sociotechnical Systems*, 2019 FAT* Conf.

¹⁸ Kroll et al., *Accountable Algorithms*, 165 U. Pa. L. Rev. 633 (2017).

Conclusion

Harm to consumers arising from the use of AI poses a significant threat to the principles of consumer protection. Such harm goes against the underlying concepts of freedom, autonomy, and accountability¹⁹, thus highlighting the inadequacies of the current framework. This essay demonstrates how India's legal framework falls short of meeting the contemporary needs and challenges associated with such harm. Absent a move towards regulation and transparency, consumers will continue to be victims in an environment that grows more and more complex due to advancements in technology.

The issue of regulating technologies requires that lawmakers find ways of asserting human agency in the face of powerful algorithms and ensure that the markets remain fair to all parties involved. Ultimately, whether AI can be regulated or not becomes irrelevant; what remains to be seen is if consumer protection laws can adapt fast enough to changing times.

¹⁹ Amartya Sen, *Development as Freedom* (Oxford Univ. Press 1999).