Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Transparency and Explainability of Algorithms from a Consumer Law Perspective

Shibanee Acharya[1], Prof. (Dr) Binay Kumar Das[2], Ashish Kumar Mishra[3] Omkar Acharya[4]

[1]Department Research Fellow, PG Department of Law, Fakir Mohan University, Balasore, Odisha, India
[2]Dean, PG Department of Law, Fakir Mohan University, Balasore, Odisha, India
[3]Advocate, Orissa High Court
[4]LL.M. Student, PG Department of Law, Fakir Mohan University, Balasore, Odisha, India

Abstract

The growing use of algorithmic and artificial intelligence–driven systems in digital markets has significantly reshaped consumer transactions, influencing product recommendations, pricing, advertising, and access to services. While these technologies enhance efficiency and personalization, their opaque functioning creates serious challenges for consumer protection. Algorithmic "black box" decision-making deepens information asymmetry, restricts consumer autonomy, and raises concerns regarding fairness, accountability, and trust in digital marketplaces. This paper examines the principles of transparency and explainability of algorithms from a consumer law perspective, with specific reference to the Indian legal framework. It analyses the adequacy of the Consumer Protection Act, 2019 and e-commerce regulations in addressing algorithmic unfair trade practices, misleading digital conduct, and automated decision-making. The study also explores the interface between consumer protection and data protection law, particularly the Digital Personal Data Protection Act, 2023, in regulating profiling and data-driven consumer manipulation. Adopting a doctrinal and comparative approach, the paper draws insights from international developments, including the EU's General Data Protection Regulation and proposed AI regulatory framework. It argues that formal disclosure alone is insufficient and advocates for meaningful, consumer-centric explainability. The paper concludes by recommending legal and policy reforms to strengthen algorithmic accountability while balancing innovation and consumer rights.

Keywords- Algorithm, artificial, digital, consumer, policy, marketplace, Trade

1. Introduction

The rapid integration of algorithmic decision-making into consumer markets has transformed how products, services, and opportunities are offered and accessed. Algorithms now influence everything from pricing and credit scoring to targeted advertising and dispute resolution, raising significant questions about fairness, accountability, and consumer autonomy.[1] As these systems become more complex and opaque,

[1] Grochowski, M., et al., (2021). Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Premises. *Critical Analysis of Law*. https://doi.org/10.33137/cal.v8i1.36279.

the principles of transparency and explainability have emerged as central concerns in both legal and ethical debates.

Transparency refers to the ability of consumers and regulators to access meaningful information about how algorithmic decisions are made, while explainability focuses on making these processes understandable to non-experts.[2] The European Union, through instruments like the General Data Protection Regulation (GDPR), has established transparency and the "right to explanation" as foundational rights for individuals affected by automated decisions.[3] However, practical implementation remains challenging due to technical barriers (such as the "black box" nature of many machine learning models), trade-offs with intellectual property, and the limited technical literacy of most consumers.

1.1 Background and Emergence of Algorithmic Decision-Making

Algorithmic decision-making has rapidly evolved from simple rule-based systems to complex artificial intelligence (AI) and machine learning models that now permeate consumer markets, public services, and business operations. The roots of algorithmic decision-making trace back to early computational methods in the mid-20th century, with significant acceleration following the advent of electronic computers in 1946 and the subsequent digitalization of data processing.[4] By the 1990s, the rise of the internet and the datafication of online behaviour enabled algorithms to process vast amounts of user-generated data, leading to the development of automated marketing, recommendation systems, and search engines.[5]

In recent years, the proliferation of big data and advances in machine learning have enabled algorithms to make increasingly sophisticated predictions and decisions, often surpassing human capabilities in speed and scale. These systems are now integral to consumer-facing applications such as credit scoring, personalized advertising, dynamic pricing, and even public sector services like social welfare and employment support. The emergence of generative AI has further expanded the scope, allowing for not only predictive but also creative and adaptive decision-making processes. While algorithmic decision-making offers benefits such as efficiency, personalization, and cost reduction, it also raises significant concerns about transparency, fairness, privacy, and accountability. The shift from human to automated decisions has triggered debates about consumer trust, regulatory adequacy, and the ethical implications of delegating critical choices to opaque systems.[6]

Algorithmic decision-making is now central to consumer markets, shaping everything from advertising and pricing to credit and product recommendations. This shift brings both opportunities for efficiency and

[2] Lepri, B., et al., (2017). Fair, Transparent, and Accountable Algorithmic Decision-making Processes. *Philosophy & Technology*, 31, 611 - 627.
[3] De Laat, P. (2017). Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?. *Philosophy & Technology*, 31, 525 - 541.
[3] Gryz, J., & Rojszczak, M. (2021). Black box algorithms and the rights of individuals: no easy solution to the "explainability" problem. *Internet Policy Rev.*, 10. https://doi.org/10.14763/2021.2.1564.
[4] Airoldi, M., & Rokka, J. (2022). Algorithmic consumer culture. *Consumption Markets & Culture*, 25, 411 - 428. https://doi.org/10.1080/10253866.2022.2084726.
[5] Kotras, B. (2020). Mass personalization: Predictive marketing algorithms and the reshaping of consumer knowledge. *Big Data & Society*, 7. https://doi.org/10.1177/2053951720951581.
[6] Schmitt, B. (2024). Consumer Information Processing and Decision-Making: Origins, Findings, Applications, and Future Directions. *Journal of Consumer Research*. https://doi.org/10.1093/jcr/ucae008.

personalization, and challenges around fairness, privacy, and consumer empowerment.[7] Algorithms influence consumer choices, market segmentation, and pricing, often operating with limited consumer awareness or understanding. Their widespread use can lead to both enhanced consumer experiences and risks such as manipulation, discrimination, and loss of autonomy. Regulatory frameworks, especially in the EU, are evolving to address these impacts.[8]

1.2 Objectives of the Study

1. Assess the Effectiveness of Legal Frameworks- Evaluate how current consumer protection laws (e.g., GDPR, EU AI Act) address transparency and explainability requirements for algorithmic systems, and identify gaps or ambiguities in these regulations.
2. Examine the Impact on Consumer Rights and Empowerment- Investigate how transparency and explainability influence consumer understanding, trust, and ability to make informed decisions, as well as their capacity to contest or object to automated decisions.[9]
3. Identify Barriers and Trade-offs- Analyze technical, legal, and business obstacles to implementing meaningful transparency and explainability, including trade-offs with innovation, intellectual property, and algorithmic performance.
4. Develop Best Practices and Policy Recommendations- Propose actionable guidelines for regulators and industry to enhance transparency and explainability in a way that is accessible to lay consumers, supports accountability, and balances competing interests .
5. Explore Multidisciplinary and Comparative Approaches- Encourage cross-national and interdisciplinary research to understand how different jurisdictions and sectors operationalize transparency and explainability, and to identify effective models for consumer protection.

1.3 Research Problem

The central research problem concerns the inadequacy and complexity of current legal frameworks in ensuring meaningful transparency and explainability of algorithmic decision-making for consumers. As algorithms increasingly shape consumer experiences and rights, the opacity of these systems stemming from both technical design and intentional concealment creates significant risks of exploitation, manipulation, and unfair treatment in consumer markets.[10] Key Dimensions of the Research Problem are as follows-

[7] Grochowski, M., et al., (2021). Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Premises. *Critical Analysis of Law*.
[8] Helberger, N., et al., (2020). Macro and Exogenous Factors in Computational Advertising: Key Issues and New Research Directions. *Journal of Advertising*, 49, 377 - 393.
[9] A'yun, A., & Setyaningsih, W. (2025). Consumer Empowerment Through Ethical AI: Strategies for Transparent and Trustworthy Personalized Marketing. *Journal of Marketing Breakthroughs*. https://doi.org/10.70764/gdpu-jmb.2025.1(1)-01.
[10] Bordt, S., et al., (2022). Post-Hoc Explanations Fail to Achieve their Purpose in Adversarial Contexts. *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*. https://doi.org/10.1145/3531146.3533153.

- Algorithms often function as "black boxes," making it difficult for consumers to understand how decisions affecting them are made. This opacity can be intrinsic (due to technical complexity) or relational (due to lack of accessible information for users).
- Existing laws, such as the EU's GDPR and proposed AI Act, introduce rights to explanation and transparency obligations. However, these are often vague, limited in scope, or difficult to enforce, especially given the technical and legal challenges of providing meaningful explanations to lay consumers.
- There is a mismatch between the information provided and consumers' ability to understand and act on it, raising questions about the effectiveness of transparency as a tool for consumer empowerment and market fairness.
- Demands for transparency may conflict with business interests (e.g., trade secrets), increase compliance costs, or even create a false sense of understanding among consumers, leading to misplaced trust in algorithmic decisions.

1.4 Rationale of the study

This research is necessary to address the power imbalance between consumers and algorithmic service providers, ensure fair treatment, and inform the development of legal standards that genuinely protect consumer rights in the age of automated decision-making 156151617. The study aims to clarify what constitutes effective transparency and explainability, identify barriers to their implementation, and propose legal and technical solutions that balance innovation with consumer protection.

2. REVIEW OF LITERATURE

Research across law, marketing, finance and information systems converges on the idea that opaque, data-driven systems create structural vulnerabilities for consumers and strain existing consumer-law tools.

- **Di Porto, F. (2020)[11]-** Legal analyses of AI-based products and services highlight regulatory gaps: unclear liability of AI providers, weak data protection, and absence of effective mechanisms for consumers to challenge or correct automated decisions. Limited access to algorithmic transparency leaves consumers in a structurally weaker position, reinforcing vulnerability in digital markets. A distinctive contribution from disclosure-regulation scholarship is the idea of algorithmic disclosure design: using machine-learning tools and regulatory sandboxes to test and optimize legally mandated consumer disclosures (e.g., “Best Available/Best Ever Disclosures”), aiming for adaptive, audience-specific and proportionate information duties.
- **Wang, R., et.al (2022)[12]-** Transparency is framed as a multifaceted concept involving disclosure of data use, interpretability of system logic, and accountability for outcomes, rather than mere access to technical details. Explainable AI (XAI) adds a technical layer, aiming to make black-box models interpretable enough for affected users, regulators, and courts to understand and contest

[11] Di Porto, F. (2020). From Bads to Beds. Algorithmic Disclosure Regulation. Social Science Research Network. https://doi.org/10.2139/ssrn.3633847.
[12] Wang, R., et al., (2022). Transparency in persuasive technology, immersive technology, and online marketing: Facilitating users' informed decision making and practical implications. *Comput. Hum. Behav.*, 139, 107545. https://doi.org/10.1016/j.chb.2022.107545.

decisions. Legal scholarship stresses that in high-accountability domains (law, finance, health), opacity clashes with requirements of due process, reason-giving and reviewability.

- **Richmond, K., et.al (2023)[13]-** Meta-surveys of XAI highlight persistent challenges: lack of standardized explanation metrics, tensions between trade secrets and transparency, risks of "explanation theatre" (cosmetic transparency without real accountability), and difficulty aligning technical XAI outputs with legal standards of reason-giving and fairness.
- **Olateju, O., et.al (2024)[14]-** User-centric XAI reviews identify four key dimensions of explanations i.e format, completeness, accuracy, currency and show that explanations can enhance perceived trust, transparency, understandability, usability, and fairness, though effects vary by context and design. Empirical survey work finds that implementing XAI is positively associated with perceived transparency, trust in AI systems, and ethical use of customer data, especially when combined with information-governance standards and user education.
- **Shemshaki, M. (2024)[15]-** In AI-driven marketing and personalization, literature documents systematic transparency deficits about profiling, targeting criteria and algorithmic changes, which undermine trust and informed consent. Studies of persuasive and online marketing show that "black-box" recommendation and targeting systems expose consumers to manipulation and behavioural steering while providing little meaningful information about how content or offers are curated.
- **Sarkar, M. (2024)[16]-** XAI in e-commerce is proposed as a way to give consumers understandable reasons for recommendations, fraud flags, or dynamic prices; explanations tend to increase user trust and satisfaction, but current methods struggle with scalability, bias, and tailoring explanations to lay audiences and regulators simultaneously. Reviews of ethical and digital marketing emphasize that transparency about data use, targeting logic and influencer or platform practices is becoming a core component of "ethical" or "responsible" AI use toward consumers.
- **Tahvildari, M. (2025)[17]-** In financial services, regulators explicitly demand a high level of transparency and traceability for AI systems used in credit, risk management, trading and robo-advisory. Systematic reviews show growing use of post-hoc XAI tools (e.g., feature importance, local explanations) to satisfy transparency and audit requirements while preserving complex models. Generative-AI-enabled robo-advisors heighten these concerns: explainability and hybrid AI-human oversight are identified as key to consumer trust, regulatory compliance, and mitigation of algorithm aversion.

[13] Richmond, K., et al., (2023). Explainable AI and Law: An Evidential Survey. *Digit. Soc.*, 3, 1.
[14] Olateju, O., et al., (2024). Exploring the Concept of Explainable AI and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data. *Journal of Engineering Research and Reports*.
[15] Shemshaki, M. (2024). Exploring the Ethical Implications of AI-Powered Personalization in Digital Marketing. *Data Intelligence*. https://doi.org/10.3724/2096-7004.di.2024.0055.
[16] Sarkar, M. (2024). Explainable AI In E-Commerce: Enhancing Trust and Transparency In AI-Driven Decisions. *Innovatech Engineering Journal*. https://doi.org/10.70937/itej.v2i01.53.
[17] Tahvildari, M. (2025). Integrating generative AI in Robo-Advisory: A systematic review of opportunities, challenges, and strategic solutions. *Multidisciplinary Reviews*. https://doi.org/10.31893/multirev.2025379.

3. ALGORITHMS AND ALGORITHMIC PERSONALISATION IN CONSUMER DECISION-MAKING

Algorithms underpin how digital platforms process data and shape what consumers see, click, and buy online. In e-commerce and digital marketing, increasingly sophisticated AI models tailor content to individual users, influencing attention, preferences, and purchase decisions.

Algorithms are described as finite, structured procedures that transform inputs into outputs via stepwise instructions, independent of any specific programming language. Core properties include abstraction, control structure, finiteness, and an effective mechanism for achieving a goal. Introductory computer science highlights search algorithms, data compression, hashing, and repetition algorithms as foundational types.[18] In data science, algorithms are evaluated less on truth/falsehood and more on efficiency and performance within larger systems. Machine learning algorithms (supervised, unsupervised, reinforcement learning) learn patterns from data to optimize a performance criterion automatically, and neural networks can even be trained to execute classical algorithms on complex inputs.

3.1 Algorithmic Personalisation in Digital Marketing and E-Commerce

Personalisation typically combines user data (browsing, clicks, purchases), item attributes, and context (time, device, location) to rank products or ads. Common mechanisms:

- Collaborative filtering: recommends items liked by similar users.
- Content-based filtering: matches item features to a user's profile.
- Hybrid and multimodal models: integrate text, images, behaviour, and context for richer relevance.
- Deep learning & deep interest networks: capture complex user interests over long histories.
- Reinforcement learning / DRL: adapts recommendations and bidding in real time based on feedback (clicks, conversions).

Algorithms classify users by engagement and value (e.g., Customer Merit index using clickstream paths, time, revisit frequency) to target high-value customers with tailored campaigns. Clustering and graph neural networks further refine segments by demographics and behavior, boosting recommendation satisfaction and accuracy.[19]

In emerging markets, personalization must handle limited connectivity, low-end devices, and sparse data. Strategies include lightweight models, offline capability, tiered architectures, and transfer learning to maintain relevance while respecting resource constraints. Despite limitations, AI personalisation in these markets can increase conversion by ~30% and extend retention by several months.[20]

[18] Daulay, P., & Yahfizham, Y. (2023). Penerapan Algoritma Pemrograman dalam Pembelajaran Ilmu Komputer. *Jurnal Arjuna : Publikasi Ilmu Pendidikan, Bahasa dan Matematika*. https://doi.org/10.61132/arjuna.v1i6.297.
[19] Ye, A., & Yang, J. (2025). Optimisation of e-commerce personalised recommendation algorithms driven by neural network models. *Journal of Combinatorial Mathematics and Combinatorial Computing*.
[20] Khy, T. (2025). AI-Powered Personalization in E-Commerce: Enhancing Customer Engagement and Retention Through AI-Driven Recommendation Systems in Emerging Markets Tykea Khy. *International Journal of Advanced Research in Science, Communication and Technology*.

Critical algorithm studies note that in popular discourse "the algorithm" often appears as an opaque system governing disempowered users, masking the social choices embedded in design. Algorithmic personalisation raises privacy, transparency, and bias concerns; marketers acknowledge risks of over-personalisation, privacy invasion, and ad fatigue, emphasizing the need for transparency, user control, and careful frequency capping.[21] Calls for ethical AI frameworks stress fairness, explainability, and avoiding displacement of responsibility onto algorithms alone.

3.2 Algorithmic Transparency, Explainability, and Trust

Transparency is often treated as a way to "see inside" systems, but research shows it is multidimensional and graded, not all-or-nothing. Dimensions include: algorithm/code, data, goals, system performance, organizational context, and user literacy. Creel distinguishes functional (algorithmic), structural (code/model), and run transparency (hardware/data execution) as different "varieties" that can be increased separately. Other work proposes three levels: algorithmic, interaction, and social transparency, stressing that user-facing interfaces and institutional practices matter as much as code disclosure. Ethically, transparency is an instrumental value enabling knowledge and accountability, subject to trade-offs with duties like security or privacy, and can be graded and role-dependent.[22]

3.3 Black Box Algorithms, Accountability, and Information Asymmetry

Black box algorithms are epistemically opaque to humans due to high-dimensional optimization, secrecy, and expertise gaps. This creates:

- Accountability deficits: relying only on disclosure or code access is insufficient to govern complex, evolving systems; accountability should be reconceived as ongoing interaction, audit, and "observability" of system behaviour over time.
- Gaslighting risks: platforms can use their epistemic authority to dismiss user experiences (e.g., "shadow banning is not a thing"), undermining credible critique.
- In high-stakes domains (medicine, security, work), opacity complicates responsibility, bias detection, and workers' or patients' ability to contest decisions.

3.4 Ethical and Human Rights Foundations

Transparency is framed as a prima facie ethical duty, grounded in values of knowledge, beneficence, and justice; it can be outweighed but not erased, and may be qualified to specific stakeholders when full disclosure would cause harm or undermine legitimate interests. Design-level transparency ("design publicity") links algorithms to goals, performance metrics, and fairness criteria, enabling procedural justification of systems even when internal mechanics stay inscrutable. Consumer and citizen trust depends on:

- Perceived reliability and safety of outputs.

[21] Pan, S. (2025). Effectiveness of Personalized Advertising in E-commerce Platforms. *Interdisciplinary Humanities and Communication Studies*.
[22] Hayes, P. (2020). An ethical intuitionist account of transparency of algorithms and its gradations. *Business Research*. https://doi.org/10.1007/s40685-020-00138-6.

- Accessible, role-appropriate explanations and interaction-level transparency.[23]
- Mitigation of fairness concerns and perceived information asymmetry; when only organizations understand and control the system, users face domination and loss of autonomy (e.g., at work, in security, on platforms).

4. CONSUMER PROTECTION LAW AND ALGORITHMIC PRACTICES IN INDIA

The CPA 2019 and E-Commerce Rules 2020 give a broad toolkit that can be applied to algorithm-driven practices, even though they do not always name algorithms explicitly.

CPA 2019 modernises the 1986 regime by:

- Recognising e-commerce and digital products expressly.
- Creating the Central Consumer Protection Authority (CCPA) with regulatory and enforcement powers.
- Introducing product liability, unfair contracts, stricter rules on misleading advertisements, and online-friendly redressal (e-filing, mediation cells).[24]

The Act applies to online marketplaces, aggregators and platforms providing technologies that enable advertising and sale of goods and services. CPA 2019 widens the notion of unfair trade practices, including misrepresentation, misleading information, and unfair contract terms.[25] In the e-commerce context, this can cover algorithmic dark patterns that manipulate choice, or conceal material information. Biased rankings or personalised offers that mislead about price, availability or comparative value. Scholars emphasise that the digital shift has produced new forms of unfair and unethical business, especially in e-commerce, requiring more active regulation and enforcement.

CPA 2019 and later guidelines create a robust regime against false/misleading advertisements:

- CCPA can order discontinuation/modification and impose penalties and recall.
- The 2022 Guidelines on Misleading Advertisements apply across media, including online and influencer ads, and hold manufacturers, advertisers and endorsers responsible.

In algorithmic settings this extends to micro-targeted ads that exaggerate performance, hide risks, or selectively show information. Programmatic campaigns that systematically target vulnerable groups with deceptive claims, which research links to erosion of consumer trust and market fairness.[26]

[23] Heuillet, A., et al., (2020). Explainability in Deep Reinforcement Learning. *Knowl. Based Syst.*, 214, 106685. https://doi.org/10.1016/j.knosys.2020.106685.
[24] Ramcharan, K., & Bujad, C. (2023). Expanding Horizons Consumer Rights Under Consumer Protection Act, 2019. *International Journal For Multidisciplinary Research*.
[25] Chawla, N., & Kumar, B. (2021). E-Commerce and Consumer Protection in India: The Emerging Trend. Journal of Business Ethics, 180, 581 - 604.
[26] P, S. (2025). From Puffery to Penalty: Legal Control of Misleading Advertisements in India. *International Journal of Advanced Research in Science, Communication and Technology*.

CPA 2019 introduces product liability against manufacturers, product service providers and product sellers, applying also to online transactions and digital products.

- E-commerce platforms must ensure that products/services match what is advertised, disclose seller identity, and have mechanisms against fraud.
- Defects in digital services (e.g., non-performance of promised online services, unsafe or fraudulent platforms) can amount to deficiency of service and trigger liability.[27] Algorithmic malfunctions that lead to financial loss or unsafe outcomes may thus be framed as defective service or product liability, though detailed case law is still emerging.

Central Consumer Protection Authority (CCPA) is the central regulator for systemic issues, with powers to inquire into consumer rights violations, unfair trade practices, misleading advertisements (including in e-commerce), Order recall of unsafe goods/services, discontinue unfair practices, impose fines, and initiate class actions and issue guidelines (e.g., for misleading advertisements, endorsements) applicable to digital and algorithmic marketing.[28]

The Consumer Protection (E-Commerce) Rules 2020 complement CPA 2019 by imposing on e-commerce entities:

- Mandatory disclosures (seller identity, address, grievance officer, return/refund, payment and security).
- A functioning grievance redress mechanism with defined timelines.
- Duties to prevent unfair trade practices, ensure that advertisements are consistent with actual characteristics of goods/services, and to not manipulate prices or discriminate unjustifiably.

Empirical work on Indian e-commerce consumers shows that effective customer care, clear information, and trustworthy redress are central to building trust in online markets, and that the new framework is regarded as strong on paper but dependent on enforcement and awareness.[29]

Algorithmic consumer decisions rely on intensive personal data collection and profiling, raising issues of consent, autonomy, and how data protection and consumer law interact. Recent work around GDPR and India's Digital Personal Data Protection Act (DPDPA) 2023 frames these debates around transparency, explainability, and limits on profiling. Consumer data increasingly drive profiling, personalization, dynamic pricing, and credit scoring, often through opaque machine-learning systems. Data can be used not only to match products but to exploit biases and vulnerabilities in decision-making. AI "autonomy" in recommendations has non-linear effects on purchase decisions and perceived self-efficacy.[30]

[27] Sao, T. (2025). An Analysis of the Indian Consumer Protection Act, 2019. *International Journal For Multidisciplinary Research*. https://doi.org/10.36948/ijfmr.2025.v07i01.38093.
[28] Solanki, K., & Singh, N. (2025). The Consumer Protection Act, 2019 : A Shield against False / Misleading Advertisements. *International Journal For Multidisciplinary Research*. https://doi.org/10.36948/ijfmr.2025.v07i03.48787.
[29] Chawla, N., & Kumar, B. (2021). E-Commerce and Consumer Protection in India: The Emerging Trend. *Journal of Business Ethics*, 180, 581 - 604.
[30] Husairi, M., & Rossi, P. (2024). Delegation of purchasing tasks to AI: The role of perceived choice and decision autonomy. *Decis. Support Syst.*, 179, 114166.

Core principles in EU GDPR and many comparative regimes are lawfulness/fairness, purpose limitation, data minimisation, storage limitation, integrity/confidentiality, and accountability.[31] Purpose limitation is often reduced to a procedural exercise and does not by itself prevent large-scale profiling, though it forces early reflection and risk management. Consent quality is a persistent weakness, especially in complex, real-time bidding and mobile payment ecosystems.

India's DPDPA 2023 is framed as a tool to rebuild consumer trust and regulate data processing in line with global standards, including consent, security, and transparency duties.[32] EU debates around GDPR's Article 22 and the "right to explanation" highlight technical and legal limits of explainability for black-box models, yet emphasize that opacity cannot justify abandoning safeguards around automated decision-making and profiling.

Consumer and data protection laws are increasingly seen as complementary "data consumer law": consumer law can attack unfair or non-transparent data practices, while data protection principles constrain profiling and manipulation. Both aim to protect autonomy and prevent exploitation in data-driven markets.[33]

5. COMPARATIVE AND INTERNATIONAL LEGAL FRAMEWORKS

Art. 5 (lawfulness, fairness, transparency) and Art. 12–14 (transparent information) impose duties to inform consumers about automated processing. Art. 22 GDPR restricts decisions "based solely on automated processing" with legal or similar significant effects, giving consumers i.e the right not to be subject to such decisions, the right to human intervention, to express views, and to contest. Recital 71 and Art. 15(1)(h) support a right to "meaningful information about the logic involved", which is often interpreted as a form of explainability, though EU case law and guidance (EDPB, WP29) tend to limit this to high-level explanations, not full source code.

Consumer Law Overlay (UCPD, Consumer Rights Directive, Omnibus Directive)

The Unfair Commercial Practices Directive (UCPD) tackles algorithmic dark patterns misleading omission of how ranking, personalisation or nudging works may constitute misleading practice. The Consumer Rights Directive and Omnibus Directive require transparency about ranking criteria on online marketplaces, "personalised pricing" based on automated decision-making, and review manipulation. These norms indirectly incentivise algorithmic transparency by forcing disclosure of key parameters affecting consumer choice.

EU AI Act and High-Risk/Consumer-Facing Systems

The AI Act (politically agreed) introduces risk-based obligations like High-risk AI (credit scoring, employment, essential services) must ensure transparency, human oversight, documentation, and risk

[31] De Lucca, N., et al., (2023). Brazilian General Data Protection Law (LGPD) and California Consumer Privacy Act (CCPA). *Brazilian Journal of Law, Technology and Innovation*. https://doi.org/10.59224/bjlti.v1i1.38-57.
[32] Mishra, A. (2024). Balancing Innovation and Privacy: The Role of AI Governance in Shaping Data Protection Jurisprudence under the Digital Personal Data Protection Act, 2023. *Revista Electronica De Veterinaria*. https://doi.org/10.69980/redvet.v25i1.1813.
[33] Helberger, N., et al., (2017). The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law. *ArXiv*, abs/2510.13466.

management and Limited-risk AI (chatbots, emotion recognition in some contexts) must disclose that consumers are interacting with an AI system.

For consumers, explainability enters mainly through requirements to provide concise, clear, meaningful information on system capabilities, limitations, and intended use; obligations on providers to keep technical documentation that can later support regulatory and judicial scrutiny. Trade secrets vs. effective consumer redress remains unresolved; enforcement will likely depend heavily on Data Protection Authorities and market surveillance authorities.

United States: Sectoral Approach and FTC Oversight

- Fragmented Sectoral Model- No comprehensive federal data protection law; instead, sector-specific statutes (e.g., FCRA, ECOA, HIPAA, COPPA) regulate algorithmic uses in credit, employment, health, children's data. Consumer protection is anchored in Section 5 FTC Act (unfair or deceptive acts or practices), supplemented by state privacy laws (CCPA/CPRA in California, Virginia, Colorado, etc.).
- FTC's Role in Algorithmic Transparency- FTC treats lack of transparency or misuse of algorithms as deception (misleading statements about AI/ML, opaque data uses) or unfairness (causing substantial injury not reasonably avoidable by consumers). Key themes in FTC guidance and enforcement includes "Truth, fairness, and equity in your use of AI" – urging explainability, bias testing, and data minimisation. Actions ordering deletion of both illegally obtained data and algorithms trained on such data (e.g., Everalbum, Cambridge Analytica). Focus on "dark patterns" and manipulative personalisation in digital interfaces. There is no explicit statutory "right to explanation", but agencies and courts can demand disclosures during investigation/litigation.
- CCPA/CPRA introduce rights to know, access, delete, opt-out of "sale/sharing" and some automated decision-making, potentially expanding transparency about profiling. FCRA already grants a strong form of explainability in credit scoring (adverse action notices, reasons for denial or higher interest), functioning as a targeted transparency right in a high-risk context.

United Kingdom: CMA and Algorithmic Accountability

Retains GDPR principles via UK GDPR and Data Protection Act 2018, including Art. 22 equivalents on automated decisions. Consumer protection frameworks (Consumer Protection from Unfair Trading Regulations, Consumer Rights Act) apply to misleading algorithmic practices and unfair contract terms in digital services.

The Competition and Markets Authority (CMA) has taken a leading role on algorithms. Reports on "Online platforms and digital advertising", "Algorithms How they can reduce competition and harm consumers" highlight risks from personalised pricing, ranking bias, and dark patterns. Emphasis on ex ante transparency, auditing of pricing and recommendation algorithms, and pro-competitive data practices. The forthcoming DMCC Bill strengthens powers to address harmful choice architecture and non-transparent personalisation in digital markets. The UK's approach links algorithmic accountability to competition law and consumer law, not just privacy, widening the toolkit for intervention.

The Information Commissioner's Office (ICO) guidance on AI and data protection stresses explainable AI, model documentation, Data Protection Impact Assessments, and user-facing explanations. Joint work

(CMA–ICO–Ofcom–FCA) explores cross-regulator coordination on digital algorithms, signalling a multi-regulator accountability ecosystem.

OECD and UN Guidelines on Algorithmic Transparency

OECD AI Principles (2019) call for transparency and responsible disclosure to ensure people understand AI outcomes robustness, safety, and accountability throughout AI lifecycle. While non-binding, they shape national policies and soft law on explainability, impact assessments, and risk-based regulation. UN Guiding Principles on Business and Human Rights emphasise corporate responsibility to respect rights (privacy, non-discrimination, access to remedy) in digital technologies. UN Special Rapporteurs (on privacy, freedom of expression, racism) have linked opaque algorithms to human rights violations and called for transparency about logic, data sources, and impact, due diligence and human rights impact assessments, robust remedies for those harmed by automated systems. UNESCO's Recommendation on the Ethics of AI further reinforces explainability, contestability, and inclusiveness as normative benchmarks.

These soft law frameworks do not create direct individual rights but inform interpretation of domestic consumer and data protection law, set global "best practices" for transparency standards, guide regulators in emerging economies (including India) when designing AI/algorithmic policies.

Clarifying Transparency and Explanation Rights includes Incorporate explicit duties to disclose when decisions are automated, when prices/rankings are personalised, and what key parameters influence such outputs. It Consider a limited "right to meaningful explanation" for high-impact consumer decisions (credit, insurance, employment-linked services), modelled on GDPR Art. 22 + FCRA adverse action notices.

Embedding Algorithmic Transparency into Consumer Protection Act, 2019

Define algorithmic opacity and dark patterns as forms of unfair trade practices or misleading representation. Mandate that e-commerce platforms disclose includes primary ranking criteria, whether results are sponsored or personalised, whether prices/offers are targeted based on profiling. It Empower CCPA to issue algorithmic transparency guidelines and sector-specific codes of practice, similar to EU/UK guidance.

Using the Digital Personal Data Protection Act, 2023 together with CPA, 2019 DPDP Act handles lawful processing, consent, and data rights and CPA/CCPA address fairness of market conduct, dark patterns, and deception. It create formal cooperation mechanisms (MoUs, joint investigations) between the Data Protection Board and CCPA, learning from UK's multi-regulator approach.

Inspired by the AI Act, prioritise transparency duties for high-risk consumer contexts like essential services (credit, health-related apps, education, housing), scoring/rating systems, large platforms with gatekeeper power. For lower-risk uses, focus on clear labelling of AI systems and basic disclosures, reducing compliance burden while still promoting trust.

Strengthening Remedies and Access to Redress ensure consumers can know that a decision was automated, request reasons and key factors, seek human review, obtain compensation where algorithmic errors or bias cause loss. Procedural innovations include allow representative actions and public interest

litigation involving algorithmic harms, facilitate expert evidence and algorithmic audits in consumer forums, develop simplified ODR mechanisms for digital disputes.

6. CHALLENGES IN ENSURING ALGORITHMIC TRANSPARENCY

a) **Technical Complexity and Trade Secret Protection-** Modern AI systems (especially machine learning) are technically opaque even to experts, complicating meaningful explanation of "why" a decision occurred. Trade secrecy over models, data, and feature engineering adds "legal opacity" on top of technical opacity, particularly in competitive markets and government procurement.[34] Under the EU AI Act, high-risk AI providers must disclose training and design details, yet must also safeguard trade secrets; some AI-related information is not protectable as trade secrets, and access-to-information rules can override secrecy in specific contexts.

b) **Balancing Innovation with Consumer Rights-** There is a structural tension between commercial incentives for opacity and democratic values of transparency, fairness, and accountability. Economic modelling suggests welfare-maximising regulation may be quite stringent in some competition scenarios, while "light-touch" approaches are only optimal within a narrow band of foreign competition conditions. Over-regulation risks chilling beneficial innovation, but under-regulation allows opaque systems to erode privacy, equality, and safety.[35]

c) **Cost of Compliance for Businesses-** Internalising transparency and AI-related risk is framed as a core compliance function, with firms expected to absorb costs rather than externalise harms to third parties. Implementing transparency-by-design, documentation, audits, and governance structures entails organisational and financial burdens, especially for SMEs.[36] In some regulated environments (e.g., blockchain-based compliance or supply-chain transparency), evidence suggests that once systems are established, per-transaction compliance costs can become relatively low, though initial investment is high.

d) **Information Overload and Meaningful Transparency-** Legal frameworks such as the GDPR emphasise provision of information and explanation, but information-rich disclosures often fail to translate into genuine understanding or user empowerment. Context, audience, and performance of transparency (how, when, and to whom information is communicated) strongly condition whether transparency builds trust or is practically inert. Experiments show that transparency can even backfire: revealing that an algorithm is "too simple" reduces reliance on its advice, while perceived over-complexity does not necessarily harm trust.[37]

[34] Mylly, U. (2023). Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information. *IIC - International Review of Intellectual Property and Competition Law*, 54, 1013 - 1043.
[35] Larsson, S., & Heintz, F. (2020). Transparency in artificial intelligence. *Internet Policy Rev.*, 9. https://doi.org/10.14763/2020.2.1469.
[36] Awad, A., et al., (2025). Artificial intelligence in financial statement preparation: Enhancing accuracy, compliance, and corporate performance. *International Journal of Innovative Research and Scientific Studies*. https://doi.org/10.53894/ijirss.v8i2.5166.
[37] Lehmann, C., et al., (2022). The risk of algorithm transparency: How algorithm complexity drives the effects on the use of advice. *Production and Operations Management*, 31, 3419 - 3434.

Limitations of Existing Legal Frameworks

Current regimes (data protection, trade secrets, consumer and securities law) create fragmented and sometimes conflicting obligations: transparency duties sit uneasily alongside strong IP and secrecy protections. Technology-neutral instruments like the GDPR do not fully account for AI-specific challenges (multi-stakeholder contexts, lock-in, distributed harms, dark patterns), limiting their protective effect. Disclosure-based regimes often ignore the real informational needs of stakeholders in an AI-driven economy, leaving major gaps in accountability for algorithmic risks. Without stronger access-to-information tools, audit powers, and calibrated limits on secrecy, legal promises of algorithmic transparency risk remaining largely symbolic.[38]

7. POLICY RECOMMENDATIONS AND LEGAL REFORMS

Policy reforms should embed explicit, risk-based algorithmic transparency duties, backed by audits, integrated AI-consumer law, and sustained capacity-building.

- **Need for Explicit Algorithmic Transparency Obligations-** Multiple studies argue current privacy/consumer regimes are too generic; they call for clear, AI-specific duties of transparency, explainability and auditability (e.g., GDPR Arts 13–15, AI Act).[39] Proposals include mandatory impact/risk assessments, documentation of data and model logic, and user-facing explanations tailored to lay understanding.
- **Strengthening Consumer Consent and Choice-** Research on AI in health, finance and online services stresses informed, intelligible consent and real options to refuse/opt-out of automated decisions. Recommendations include layered notices, user-centric consent interfaces, and easy routes to human review and contestation.[40]
- **Enhancing Regulatory Oversight and Audits-** Systematic reviews call for regulator-mandated, continuous algorithm audits, not one-off tests, especially for high-risk systems. Proposals like dedicated AI supervisory units, standardized audit methodologies, and risk-based conformity assessments (as in the EU AI Act).[41]
- **Integrating Consumer Law with AI Governance-** Suggested reforms like update consumer law to cover automated unfair practices, mandate fairness and transparency in profiling and scoring, and link AI ethics codes to enforceable duties.
- **Capacity Building and Consumer Awareness-** Effective transparency depends on regulatory expertise and stakeholder education includes training for regulators, judges, developers, and consumer groups on fairness, accountability and transparency (FATE). Studies highlight consumer

[38] De Laat, P. (2022). Algorithmic decision-making employing profiling: will trade secrecy protection render the right to explanation toothless?. *Ethics and Information Technology*, 24.
[39] Radanliev, P. (2025). Privacy, ethics, transparency, and accountability in AI systems for wearable devices. *Frontiers in Digital Health*, 7. https://doi.org/10.3389/fdgth.2025.1431246.
[40] Froicu, E., et al., (2025). Artificial Intelligence and Decision-Making in Oncology: A Review of Ethical, Legal, and Informed Consent Challenges.. *Current oncology reports*. https://doi.org/10.1007/s11912-025-01698-8.
[41] Koshiyama, A.,et.al. (2024). Towards algorithm auditing: managing legal, ethical and technological risks of AI, ML and associated algorithms. *Royal Society Open Science*, 11.

education campaigns and public guidance on AI use and rights as essential to make legal protections usable in practice.[42]

8. Conclusion

Transparency and explainability of algorithms have emerged as foundational requirements for effective consumer protection in the digital marketplace. As algorithmic systems increasingly shape pricing, advertising, credit assessment, and access to goods and services, their opacity poses significant risks to consumer autonomy, fairness, and trust. From a consumer law perspective, the traditional principles of informed choice, fairness, and accountability cannot be meaningfully realized unless consumers are able to understand, at least in broad terms, how algorithmic decisions affecting them are made. While existing consumer protection frameworks implicitly support transparency through duties to disclose material information and prohibit unfair and deceptive practices, they are often ill-equipped to address the technical complexity and dynamic nature of algorithmic decision-making. Explainability therefore assumes a normative role: not to require full technical disclosure, but to ensure intelligible, contextual, and actionable explanations that enable consumers to challenge harmful outcomes and regulators to enforce compliance. A balanced approach is essential, one that reconciles consumer rights with legitimate concerns of innovation, trade secrets, and proportionality. Strengthening algorithmic transparency through sector-specific guidelines, ex ante impact assessments, and enhanced regulatory oversight can bridge this gap. Ultimately, embedding transparency and explainability within consumer law is not merely a technical or regulatory exercise; it is central to preserving consumer trust, market fairness, and the legitimacy of digital governance in an algorithm-driven economy.

9. ACKNOWLEDGEMENTS

The authors express sincere gratitude to Prof. (Dr) Santosh Kumar Tripathy, Vice-Chancellor, Fakir Mohan University, Balasore; Prof. (Dr) Bhaskar Behera, Chairman, PG Council, Fakir Mohan University, Balasore; Prof. (Dr) Amulya Kumar Acharya, Coordinator, PG. Department of Law, Fakir Mohan University, Balasore; the esteemed Judges, senior advocates and junior fellow advocates of Orissa High Court for their invaluable support.

[42] Uzougbo, N., et al., (2024). Legal accountability and ethical considerations of AI in financial services. *GSC Advanced Research and Reviews*. https://doi.org/10.30574/gscarr.2024.19.2.0171.