ISSN: 2393-8048
International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.
SJIF Impact Factor = 8.35, January-June 2026, Submitted in January 2026

Data-Driven Personalization and Deceptive Advertising: Emerging Governance Questions in India

Parteek Goel, Research Scholar, Dept. of Law, NIILM University, Kaithal (Haryana)
Dr. Sevanand, Supervisor, Dept. of Law, NIILM University, Kaithal (Haryana)

Abstract

Digital advertising in India has been reinvented structurally. The advertiser used to send out a standard message to a mass audience, but today he uses artificial intelligence and precise personal data profiles to provide customized messages, prices and claims to each consumer. When this capability of personalization is abused — to exploit emotional vulnerability, to withhold unflattering information, or to display different prices to different users for the same commodities — it creates a fresh and legally underexplored category of harm: data-driven deceptive advertising. This research study gives a rigorous doctrinal and policy examination of the problem in the Indian legal setting. It goes beyond the mapping of the existing statutory framework (covered in prior scholarship) to an original taxonomy of personalised deception techniques, a critical assessment of the structural architecture of governance failure, the proposal of a five-pillar reform model and a comparative penalty analysis across the five major jurisdictions. The report contends that India needs to shift its legislative reform from a complaint-reactive paradigm to a structural-preventive model, centered on algorithmic accountability, advertising transparency and consumer sovereignty.

Keywords: algorithmic targeting, personalised deception, DPDPA 2023, Consumer Protection Act, dark patterns, digital advertising governance.

1. The Problem of Personalised Deception: An Introduction

Classical consumer protection law is based on a basic assumption: that the seller makes a representation and the customer analyzes it. It may be incorrect or deceptive but at least it is publicly verifiable – the same statement is made to all buyers and regulators can see and judge it. This premise is profoundly subverted by data-driven advertising. Today, the seller is not making any representations to any purchasers whatsoever. Instead, an algorithm develops a tailored representation of each buyer, according to what that individual is most likely to be persuaded by – or least likely to challenge – at that moment in time. There is nothing wrong in itself with such individualisation of advertising messages. There are valid reasons for personalisation – a consumer who has looked for diabetic food can actually benefit from seeing relevant adverts. The legal and ethical issue is where personalisation is used not to serve the consumer's interests, but to exploit information asymmetries against them – where the algorithm knows something about the consumer's vulnerabilities, anxieties or limited information that the consumer does not know the algorithm knows, and uses that knowledge to construct a misleading or manipulative message.

Until now, Indian research has dealt with this subject at the level of mapping statutory provisions. The doctrinal gap that this paper addresses is a more fundamental one: the question of whether India's normative framework, its underlying legal logic, is able to conceptualise and condemn personalised deception as a distinct category of wrongdoing or whether existing law can only address it as an accidental overlap of data protection and consumer protection violations. The argument of the paper is that the present Indian law treats the symptoms and not the disease. The law of consent under the DPDPA only talks about the first stage of data collection, but does not talk about the downstream harm of utilizing legitimately consented data to deceive. The Consumer Protection Act's misleading advertising regulation deals with the content of ads, but it was built for mass-broadcast messaging and lacks conceptual or procedural tools for dealing with ads that are invisible to all but their target. This creates a structural governance deficit which has profound legal and social implications.

2. A New Taxonomy of Personalised Deception Techniques

In the scholarly and regulatory literature, misleading advertising is treated as a homogeneous group. This study argues that in the context of data-driven customisation, deceptive practices need to be taxonomised by method, as different approaches involve different legal norms, different evidential obstacles and different regulatory responses. Based on an examination of regulatory action, consumer complaints, and academic literature and platform disclosures in the Indian digital advertising ecosystem, Table 1 presents an innovative taxonomy.

Table 1: Taxonomy of Data-Driven Deceptive Personalisation Techniques in India

Technique	Data Used	How Deception Occurs	Indian Platform Example
Dynamic Pricing Deception	Purchase history, location, device type, browsing time	Different prices shown to different users for identical products; higher prices to loyal or time-pressed users	E-commerce platforms showing higher hotel rates to users on iPhones
False Urgency Amplification	Past purchase impulse rate, session duration, cart abandonment data	Countdown timers and 'Only 2 left' messages personalised to users known to respond to scarcity cues	Online ticketing and fashion retail apps targeting repeat visitors
Targeted Health Exploitation	Search queries, app usage (fitness, symptom checkers), insurance data	Ads for unverified remedies or predatory health insurance shown to users flagged as health-anxious	Digital lending apps targeting users who searched for medical finance
Selective Disclosure	Credit score, income inference, demographic segment	Key terms (interest rates, penalties) hidden from low-income users; premium users receive transparent pricing	BNPL and fintech apps showing simplified terms to first-time users
Emotional State Targeting	Posting time, content sentiment, location (hospital, gym), social interactions	Ads for alcohol, gambling, or junk food served when user sentiment is detected as negative or stressed	Social media platforms monetising grief or anxiety windows
Personalised Fake Reviews	Product category interest, review-reading behaviour	Algorithmically curated review pages showing 5-star reviews to likely buyers and hiding negative ones	E-commerce review manipulation on major Indian platforms

Source: Author's compilation based on ASCI complaint records, CCI market study on e-commerce (2020), FTC enforcement reports, and academic literature on dark patterns (2019–2024).

Three aspects of this taxonomy are noteworthy. First, dynamic pricing deception and selective disclosure are difficult to challenge under traditional misrepresentation laws because consumers are shown accurate information but unaware that others may receive better terms. Second, emotional-state targeting and targeted health exploitation employ lawfully gathered personal data in ways that data protection rules do not, creating a gap between data collection and advertising-related harm. Third, tailored false reviews raise problems regarding platform responsibility and regulatory accountability in digital advertising due to algorithmic collusion, as platforms recommend deceptive information without producing it.

3. Structural Architecture of the Governance Failure

3.1 The Indian Legal Framework: A Matrix Analysis

In India, there are six regulatory instruments that impact data-driven deceptive advertising to varied degrees. Table 2 compares each instrument by administering body, relevant provision, coverage of personalised advertising, enforcement power and key gap.

Table 2: Indian Legal Framework Matrix — Coverage of Data-Driven Deceptive Advertising

Law / Rule	Body	Key Provision	Personalised Ads	Enforcement	Key Gap
Consumer Protection Act, 2019	CCPA	Misleading ads, penalties	Partial	Up to ₹50 lakh	No audit power
DPDPA, 2023	Data Protection Board	Consent, child data rights	Indirect	Up to ₹250 crore	No specific opt-out for personalised ads
IT Act, 2000 & IT Rules, 2021	MeitY	Due diligence obligations	No	Takedown/blocking orders	No ad-targeting rules
Competition Act, 2002	CCI	Abuse of dominance	Indirect	Up to 10% turnover	Slow enforcement
ASCI Code	ASCI	Misleading claims, influencer rules	Limited	Ad withdrawal recommendations	No legal force
CCPA Dark Pattern Guidelines, 2023	CCPA	Prohibits dark patterns	Partial	CPA penalties	Ignores data profiling

Personalised Ads?' refers to whether the instrument specifically addresses the use of personal data profiles to customise advertising content or targeting. 'Partial' coverage means the instrument applies to advertising generally but lacks provisions specific to personalisation or algorithmic targeting.

What the matrix reveals is a pattern more disturbing than legislative quiet. India does not just lack a law on tailored deception – it has six separate legal instruments that each addresses a part of the problem, managed by various authorities, with different enforcement cultures, and with no coordinating mechanism. A consumer deceived by a personalised predatory loan ad would need to file complaints with the CCPA (misleading ad), the Data Protection Board (consent violation), perhaps the RBI (mis-selling of financial products), and perhaps the CCI (market dominance) — and would probably get inconsistent or contradictory responses from each.

3.2 The Three Structural Deficits

Apart from the fragmentation noted above, there are three fundamental structural weaknesses which explain why the present structure does not operate. The first is the reactive-complaint model the big Indian regulating bodies in this field work on complaints-received basis. No regulator has the stature or the resources to conduct proactive investigations of advertising algorithms. This is a fatal vulnerability because data-driven deceit, by its very nature, leaves no public trail. The misled consumer may not even realize they were tricked. And even if they do, they confront an insuperable knowledge asymmetry ire demonstrating algorithmic intent.

A second structural weakness is the absence of evidential instruments. To demonstrate that an advertising algorithm was being abused, a regulator would need to examine the training data, the goals of the optimisation, the logic of the audience segmentation, and a sample of what various consumers were given. There is currently no mechanism in Indian law to force such disclosure by authorities. The DPDPA's data fiduciary duties concern security and permission, not the content or targeting logic of advertising systems.

Failure three is lack of a plaintiff representing the public interest. In the United States, the FTC is able to bring suit on behalf of consumers without any specific complainant. In the EU, digital rights groups can file complaints over data protection. Such a process does not exist in India. Consumer organisations can access the CCPA, but in the absence of the algorithmic evidence

outlined above, they cannot bring legally sufficient complaints. The statute effectively privatizes the burden of proof of a public harm.

4. Comparative Regulatory Models: What India Can Learn

Since 2018, the international regulatory landscape for data-driven advertising has evolved significantly. Five jurisdictions provide various models, with different logics of institution building, each with distinctive lessons for India. A systematic comparison is given in Table 3.

Table 3: Comparative Regulatory Models — Digital Advertising Governance across Five Jurisdictions

Jurisdiction	Key Legislation	Advertising-Specific Rights	Enforcement Highlight	Lesson for India
European Union	GDPR (2018); Digital Services Act (2024); Digital Markets Act (2023)	Art. 21 GDPR: right to object to profiling for direct marketing; DSA Art. 26: ad transparency repository; prohibition on targeting minors and sensitive data	Meta fined €390 million (2023) for using contract basis instead of consent for behavioural ads	Adopt a right to object to personalised ads; mandate ad repositories; ban sensitive-data targeting
United Kingdom	UK GDPR; Data Protection Act 2018; Online Safety Act 2023	ICO Adtech Guidance (2019): RTB deemed systemically non-compliant; CMA remedies for Google Privacy Sandbox	ICO issued enforcement notices to Experian and other data brokers for illegal profiling (2020–2022)	Empower data protection authority to investigate adtech ecosystem proactively, not just reactively
United States	FTC Act S.5; COPPA; CCPA (California 2020); Colorado Privacy Act 2021	CCPA: right to opt out of sale/sharing of personal data; COPPA: no targeted ads to under-13s; FTC proposed rules on commercial surveillance (2022)	FTC action against BetterHelp (2023): $7.8 million settlement for sharing health data with advertisers without consent	Introduce a federal-style opt-out right; protect children absolutely; strengthen health-data advertising restrictions
Brazil	Lei Geral de Proteção de Dados (LGPD), 2020; Consumer Defence Code	Art. 20 LGPD: right to review automated decisions; Art. 18: right to deletion; PROCON enforcement on digital deception	ANPD (data protection authority) issued first enforcement actions in 2023 on consent violations in digital marketing	Useful peer — similar developing economy context; shows DPDPA can be extended to cover automated ad decisions
China	Personal Information Protection Law (PIPL) 2021; Algorithmic Recommendation Regulations 2022	Art. 24 PIPL: right to opt out of personalised recommendations; Algorithmic Regs: must label personalised ads; cannot raise prices	CAC ordered Didi and other apps to cease illegal data collection and personalised pricing in 2022	India should adopt explicit anti-price-discrimination rules and mandatory labelling of personalised advertisements

Jurisdiction	Key Legislation	Advertising-Specific Rights	Enforcement Highlight	Lesson for India
		based on personal profiling		

Sources: GDPR Art. 21, 22; EU Digital Services Act Art. 26, 39; UK ICO Adtech Report (2019); FTC v. BetterHelp Consent Order (2023); LGPD Art. 18, 20; PIPL Art. 24; CAC Algorithmic Recommendation Regulations 2022.

From this comparative analysis a number of cross-cutting observations arise. First, all jurisdictions that have made real progress have done so with an express right to opt out of personalised advertising – not a generic data protection right, but a specific, easy-to-exercise one aimed at the advertising use case. This right is not part of India's DPDPA. Second, the most effective enforcement actions have been brought by cross-cutting regulators – agencies like the FTC that can handle both the data infringement and the consumer harm in a single case. India's segregated regulatory framework hinders this.

Third, the China experience is particularly illuminating for India, given their differing political settings, as the Algorithmic Recommendation Regulations of 2022 in China are the world's first specialized legislative framework for personalised recommendation systems including advertising. The need that tailored advertisements be identified as such and that users be given an easy way to turn off personalised recommendations are technically basic criteria with enormous consumer protection significance. There is no legislative intricacy in India to move both ways.

Brazil's experience as a developing economy with similar digital market structures — high mobile internet penetration, big unbanked population, rapid fintech growth — is also immediately relevant. Brazil's LGPD, enacted in 2020, demonstrates that a developing economy may operationalize important data protection protections within a few years of adoption. India's DPDPA, adopted in 2023 but not yet fully operationalised, is reaching a similar turning moment.

5. A Five-Pillar Governance Reform Model for India

The governance reform model for India proposed in this study has five pillars. The pillars are based on the taxonomy of harms outlined in Section 2, the governance analysis in Section 3, and the comparative lessons of Section 4. The model attempts to solve the three structural inadequacies noted – the reactive-complaint paradigm, the absence of evidence tools, and the absence of a public interest plaintiff. At the same time it attempts to be compatible with India's constitutional framework, and its developmental economic backdrop. The detailed architecture of reform is illustrated in Table 4.

Table 4: Proposed Five-Pillar Governance Reform Framework for Data-Driven Advertising in India

Reform Pillar	Specific Proposal	Legislative Vehicle	Responsible Body	Timeline
Transparency Obligation	All platforms with >5 million Indian users must maintain a public Ad Library disclosing advertiser identity, targeting criteria (by category, not individual), reach, and expenditure	Amendment to IT Rules, 2021 (new Rule 3A)	MeitY + CCPA joint enforcement	Short term (0–12 months)
Opt-Out Right	Amend DPDPA Rules to create an explicit, free-of-charge right to opt out of behavioural advertising. Platforms must offer	DPDPA Rules under S.40 (rules by central government)	Data Protection Board	Short-medium term (6–18 months)

Reform Pillar	Specific Proposal	Legislative Vehicle	Responsible Body	Timeline
	equal-quality contextual advertising as default alternative			
Sensitive Data Ban	Prohibit use of health, financial vulnerability, caste, religion, and mental health data for advertising targeting. Platforms must maintain and audit negative data lists	New Clause in DPDPA or standalone Digital Advertising Standards Act	Data Protection Board + sector regulators	Medium term (12–24 months)
Algorithmic Accountability	Platforms earning >Rs. 500 crore annually from Indian advertising must conduct annual Algorithmic Impact Assessments (AIAs) covering discrimination risks, vulnerability exploitation, and accuracy of profiling	Digital Advertising Standards Act or IT Rules amendment	Independent AIA Auditor Registry (MeitY-recognised)	Medium term (18–30 months)
Children's Protection	Absolute ban on behavioural advertising targeting users under 18; platforms must implement age verification for advertising systems, not just account creation	DPDPA S.9 + CCPA S.10 strengthened guidelines	CCPA + NCPCR joint oversight	Immediate (0–6 months)
Dedicated Regulator	Establish a Digital Markets and Advertising Authority (DMAA) as a statutory body combining consumer, competition, and data protection functions for digital advertising. Coordinate with CCPA, CCI, and Data Protection Board	New Digital Markets and Advertising Act (recommended)	DMAA — new body under Ministry of Consumer Affairs	Long term (24–48 months)

The proposed Digital Markets and Advertising Authority (DMAA) is modelled on aspects of the UK's Digital Markets Unit within the CMA and the EU's coordination structure between the European Data Protection Board and national Digital Services Coordinators under the DSA. Timeline estimates are indicative and assume standard legislative drafting and parliamentary scheduling.

A brief theological explanation is due for each pillar of the proposed framework. The transparency requirement under Pillar 1 is based on the fundamental right to the information which has been held by the Supreme Court to be derived from Article 19(1)(a) of the Constitution. The requirement for platforms to reveal aggregate advertising targeting criteria in a publicly accessible repository is not a publication of individual user data and so does not interfere with the right to privacy under Article 21. It is a reasonable restriction in the authority of regulation of the state under Article 19(6).

The Pillar 2 opt-out right is patterned on the GDPR's Article 21 right to object to processing for direct marketing, and modified to the Indian consent regime. The main legal ground for processing data is already consent under the DPDPA. The proposed rule would merely provide that consent to data processing does not in general include consent to behavioural advertising expressly, and that separate, freely given consent is necessary for that purpose – keeping with the DPDPA's requirement that consent be specific and informed.

The Pillar 3 sensitive data restriction targets what this report calls the 'consent laundering' problem — the process of taking data originally acquired for one reason (health app usage, financial transactions) and utilizing it to develop advertising profiles that apply the insights gleaned from that data. Even if every link in this chain is consensual in the technical sense, the cumulative effect is not something reasonable customers would have contemplated or consented to. The right legal reaction is a specialized ban on the use of sensitive categories of data for advertising targeting – akin to Article 9 GDPR but expanded to the advertising use case.

6. Penalty Architecture: Deterrence, Proportionality, and the Indian Deficit

A governance system is only as good as its enforcement teeth." One of the biggest problems with the current approach in India is that the fines are inadequate compared to the revenues that platforms are making from the identical advertising tactics that are being banned. Table 5 compares penalty regimes across major jurisdictions, scaled to actual enforcement outcomes.

Table 5: Comparative Penalty Analysis — Data-Driven Advertising Violations across Jurisdictions

Jurisdiction	Law	Maximum Penalty	Basis	Notable Enforcement Action
European Union	GDPR	€20 million or 4% global turnover	Higher of two	Meta: €1.2 billion (2023); Google: €150 million (2022) for cookie consent
United Kingdom	UK GDPR / DPA 2018	£17.5 million or 4% global turnover	Higher of two	Clearview AI: £7.5 million (2022); British Airways: £20 million (2020)
United States	FTC Act S.5	$51,744 per violation per day (civil penalty)	Per violation	Facebook: $5 billion (2019); Google: $170 million COPPA (2019)
China	PIPL + Cyberspace regulations	Up to RMB 50 million or 5% of prior year revenue	Higher of two	Didi: RMB 8.026 billion (2022) for illegal data collection
India (Current)	DPDPA, 2023	Up to Rs. 250 crore (~$30 million)	Per category of violation	No major enforcement action yet — Data Protection Board not yet operational (as of 2024)
India (Proposed)	Enhanced DPDPA + Digital Advertising Act	Rs. 500 crore or 3% of India revenue for ad violations	Higher of two (recommended)	(Proposed) Mandatory corrective advertising + platform suspension for repeat offenders

Sources: GDPR Art. 83; UK DPA 2018 S.157; FTC Act S.5(m); PIPL Art. 66; DPDPA 2023 Schedule. Exchange rates approximate as of 2024. All figures refer to maximum statutory penalties; actual penalties imposed may be lower.

Comparative data in Table 5 demonstrates a large deterrence disparity in India. Google's India ad revenue reached Rs. 10,000 crore by 2022. Even with full penalties, the DPDPA's maximum penalty of Rs. 250 crore is 2.5% of that revenue and less than 1% of the company's global advertising sales. In law and economics, the penalty must be larger than the expected gain from the violation times the inverse of the chance of detection to discourage. This is much below the

threshold. The fact that the DPDPA Data Protection Board has not yet begun functioning exacerbates this issue. Punishment clauses are speculative unless enforced. The Indian DMA proposed in the reform framework above should be able to levy penalties proportionate to Indian advertising revenue, not as a punishment, to ensure that big platforms face real financial consequences for deceiving Indian consumers. Two further penalty modifications are worth examining. First, India should oblige platforms that distributed fraudulent tailored advertising to provide remedial messaging to the same audience categories. A monetary penalties, which goes to the government rather than the deceived consumer, is less effective and financially significant, thus the platform has strong incentives to avoid it. Second, the regulator should be able to halt a platform's advertising operations in India for repeated or intentional violations, which will be more commercially damaging than any punishment and has been used in China with proven deterrence.

7. Constitutional Foundations and Judicial Avenues

Any reform in governance in India has to be ultimately based on the constitutional framework. Fortunately, the Constitution of India provides strong theological moorings for controlling data-driven misleading advertisements. In Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1, a nine-Judge court held that the right to privacy is a basic right under Articles 14, 19 and 21. In the majority ruling, a basic characteristic of privacy was described as the right of an individual to control information about themselves, informational autonomy.

The use of data-driven customized deception is a clear infringement of informational autonomy. When a platform leverages a consumer's personal data profile to tailor a message to exploit their specific psychological vulnerabilities, it undermines the consumer's ability to make free and informed choices – the very ability informational autonomy is meant to defend. While no statutory provision exists, a constitutional challenge to a platform's failure to disclose its advertising targeting reasoning could potentially prevail before Indian courts on Puttaswamy grounds.

Commercial companies that oppose advertising regulation sometimes claim Article 19(1)(g) – the right to carry on any trade or business. This right, however, is subject to reasonable restrictions under Article 19(6) in the interest of the general public. The Supreme Court has often recognized consumer protection as a legitimate public-interest ground for economic regulation. Using personal data to deceive consumers is not a valid exercise of commercial free speech; it is, in the Court's words from a related context, a fraud on the public that cannot cover behind free speech rights. The judicial path to accelerate reform is also interesting. A qualified consumer organisation, with suitable backing by technical experts, can file a public interest litigation in the Supreme Court or a High Court to direct the government to operationalise the Data Protection Board, issue rules on advertising opt-outs under the DPDPA, and develop an accountability framework for advertising algorithms. Litigation approach can be a supplement to legislative reform, particularly given the slow pace of parliamentary action on digital governance concerns.

8. Conclusion

This paper has argued that India's current approach to data-driven deceptive advertising is structurally inadequate – not primarily because specific legal provisions are lacking (though they are), but because the underlying regulatory logic is one of symptom management rather than structural governance. Laws and regulators act after harm has been done, after a customer has complained, and after evidence may be obtained through the normal course of legal process. None of these prerequisites are reliably met in the context of data-driven tailored deception. The five-pillar reform strategy presented here – transparency, opt-out rights, sensitive data ban, algorithmic impact assessments, and a separate digital markets authority – is intended to alter the regulatory logic from reactive to preventive. Each pillar is based on comparable experience, constitutionally defendable, and technically possible given the current

institutional infrastructure in India. None of them are about waiting till harm occurs, all of them are about creating the conditions in which harm is less likely to occur in the first place. The costs of inactivity are dire. The digital advertising market in India was valued at Rs. 35,809 crore in 2023 and is expected to cross Rs. 60,000 crore by 2027. As this market has grown, data and targeting power has increasingly concentrated in a few dominating platforms. Without institutional oversight, the expansion of digital advertising will be increasingly the growth of personalised exploitation – of the economically poor, the digitally inexperienced, the emotionally susceptible and the informationally disempowered. mThe Indian constitutional promise of a life of dignity — articulated through the fundamental rights to privacy, equality and free speech — carries into the digital marketplace. The key governance problem of India's digital decade is to give practical content to that promise, in the face of the most powerful commercial manipulation technologies yet produced. In this work we have tried to map out that difficulty and to offer a principled, practically based response. The task of getting it done lies ahead -- in Parliament, in regulatory offices, in courtrooms and in classrooms where tomorrow's attorneys and policy-makers are being trained.

Bibliography

A. Primary Sources: Legislation

1. The Consumer Protection Act, 2019 (Act 35 of 2019)
2. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023)
3. The Information Technology Act, 2000 (Act 21 of 2000)
4. The Competition Act, 2002 (Act 12 of 2003)
5. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
6. CCPA Guidelines for Prevention and Regulation of Dark Patterns, 2023
7. EU General Data Protection Regulation (Regulation 2016/679)
8. EU Digital Services Act (Regulation 2022/2065)
9. China Personal Information Protection Law (PIPL), 2021
10. China Algorithmic Recommendation Regulations (Provision on the Management of Algorithmic Recommendations, 2022)
11. Brazil Lei Geral de Proteção de Dados (LGPD), 2020

B. Primary Sources: Case Law and Enforcement Decisions

1. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1
2. Competition Commission of India, Market Study on E-Commerce in India: Final Report (CCI, 2020)
3. Data Protection Commission (Ireland), Decision against Meta Platforms Ireland Ltd., January 2023 (In re: Behavioural Advertising Legal Basis)
4. FTC v. BetterHelp, Inc., Consent Order, FTC File No. 2223028, March 2023
5. UK Information Commissioner's Office, Enforcement Notice: Experian Ltd, October 2020