# Legal Implications of Using of AI in Marketing Assets in India

## Executive Summary

This report provides a comprehensive legal analysis for client regarding the strategic deployment of Artificial Intelligence (AI) in its marketing assets within India. It identifies the prevailing legal frameworks, assesses potential future risks, and offers actionable recommendations for ensuring compliance and fostering responsible AI adoption.

India's legal landscape concerning AI is currently in an evolving state, primarily relying on existing statutes that were not specifically designed to address the intricate complexities of AI. While the Digital Personal Data Protection Act, 2023 (DPDP Act), marks a significant stride in data privacy, notable gaps persist, particularly regarding the explicit legal status of AI-generated content authorship and clear liability frameworks for AI-driven errors. Non-binding guidelines and frameworks from governmental bodies like NITI Aayog and the Ministry of Electronics and Information Technology (MeitY), alongside industry associations such as NASSCOM and the Advertising Standards Council of India (ASCI), are instrumental in shaping current industry best practices and providing foresight into future regulatory directions.

To navigate this dynamic legal environment effectively, we must adopt a proactive, ethical, and transparent approach to AI in marketing. This necessitates implementing robust data governance protocols, ensuring clear disclosure of AI involvement in marketing assets, actively mitigating algorithmic biases, diligently managing intellectual property rights, and establishing effective grievance redressal mechanisms. Continuous monitoring of the rapidly evolving regulatory landscape, including the impending Digital India Act, is paramount to ensure sustained legal compliance and maintain public trust.

## Content

# 1. Introduction: AI in Marketing and the Indian Legal Context

## AI's Transformative Role in Marketing

Artificial Intelligence is profoundly reshaping the marketing domain, offering unprecedented capabilities for efficiency, personalization, and innovation. AI tools are increasingly employed to automate the creation of diverse marketing content, encompassing text, images, articles, and various other promotional collaterals.[1] Beyond content generation, AI enhances customer engagement through sophisticated applications such as chatbots, self-service solutions, and intelligent AI assistants.[1] A particularly impactful application lies in the realm of hyper-personalized campaigns, where AI's analytical prowess, capable of processing vast datasets, enables highly targeted messaging. A compelling illustration of this is Cadbury's innovative Diwali campaign in 2021, which effectively utilized deepfake technology to feature Shah Rukh Khan delivering geo-targeted messages, thereby supporting local businesses at scale.[2] This demonstrates how AI can foster more meaningful connections with consumers while also driving commercial objectives.

## The Indian Digital Landscape

India is currently undergoing a remarkable digital revolution, characterized by an accelerating rate of internet adoption. Projections indicate that the country will host an astonishing 900 million internet users by 2025, with approximately 10 million new users joining the digital ecosystem each month.[4] This exponential expansion of digital engagement underscores a critical and urgent need for robust data protection measures and comprehensive regulatory frameworks. As more aspects of daily life and commerce shift online, the imperative to safeguard individual rights and ensure fair practices become increasingly pronounced.

## Current Regulatory State

The legal framework for AI in India is still in its formative stages. It primarily relies on existing, broader legal frameworks rather than dedicated AI-specific legislation.[5] This approach reflects a recognized imperative to strike a delicate balance: protecting societal interests, including those of individuals and communities, without unduly stifling the rapid research and innovation occurring within the AI field.[8] This dynamic environment presents both opportunities and challenges for corporations like Clients, requiring careful navigation of legal ambiguities and proactive adherence to evolving standards.

## The Challenge of Regulatory Responsiveness to Technological Advancement

The current legal and regulatory landscape in India faces a significant challenge stemming from the rapid pace of technological advancement in AI. Existing Indian laws, such as the Information Technology Act, 2000, and the Copyright Act, 1957, were enacted long before the advent of modern AI's complex capabilities.[5] Consequently, these statutes inherently lack explicit provisions to address the unique legal and ethical complexities posed by AI, leaving many critical questions unresolved.[9] The continuous "dramatic progress" [12] and "rapid advancements" [10] in AI technology mean that legal clarity frequently lags behind the capabilities of these systems. This creates an environment where inherent compliance risk is elevated due to persistent regulatory uncertainty.

For client, this situation means that relying solely on explicit legal prohibitions for compliance is insufficient. Instead, a proactive approach is necessary, anticipating future regulations and adhering to evolving ethical guidelines and industry best practices. This strategy is crucial for mitigating the risk of retrospective liability, avoiding potential reputational damage, and preventing consumer backlash. Furthermore, in this interim period, self-regulatory bodies and industry-led initiatives play a disproportionately important role in defining acceptable conduct and establishing de facto standards for responsible AI deployment.

## 2. Prevailing Legal and Regulatory Frameworks Impacting AI Marketing in India

### 2.1 Digital Personal Data Protection Act, 2023 (DPDP Act)

The Digital Personal Data Protection Act, 2023, enacted on August 11, 2023, represents India's first comprehensive statute dedicated to data privacy. Its core purpose is to safeguard individuals' personal information within an increasingly digital environment and to significantly bolster user privacy across the nation.[4]

#### Key Provisions & Applicability

The DPDP Act governs the collection, processing, and storage of digital personal data within India. Importantly, its applicability extends extraterritorially, covering entities that handle the data of individuals located within India, regardless of where the processing occurs.[4] A fundamental provision of the Act is the requirement for explicit consent from individuals before their personal data can be collected or processed. This consent is dynamic, meaning it can be withdrawn at any time, compelling companies to establish easily accessible mechanisms to facilitate such withdrawals.[4] For marketers, this necessitates a re-engineering of communication strategies to ensure transparency regarding data use and to secure consent through a foundation of trust.[4] The Act broadly defines personal data to include any information that can identify an individual, such as a combination of a photograph and a company name.[4] Furthermore, Clause 8 of the Act outlines the obligations of "data fiduciaries," which include marketers and businesses, in handling personal data. Clauses 11, 12, 13, and 14 enumerate the rights of users concerning their personal data, encompassing rights to access, correction, erasure, and grievance redressal.[4] The DPDP Act also mandates robust data governance practices, including data minimization, and requires regular audits and monitoring of AI models to detect biases, inefficiencies, or security vulnerabilities.[4]

## AI-Specific Gaps

Despite its comprehensive nature, the DPDP Act does not explicitly address all AI-related privacy risks. For instance, it lacks specific provisions for automated decision-making or algorithmic transparency. While the Act emphasizes principles such as consent, purpose limitation, and data minimization, these may not be entirely sufficient to address the intricate and evolving challenges posed by AI-driven privacy concerns.[5]

## Implementation Status

The DPDP Act is anticipated to be fully implementable by the end of 2024. The newly established Data Protection Board of India will be responsible for overseeing compliance and addressing complaints, functioning with powers akin to a civil court.[4] Draft rules for the Act were released in January 2025 for public consultation, further detailing its implementation.[14]

## The Evolving Nature of Consent for AI Applications

The DPDP Act firmly establishes explicit consent as a foundational requirement for data processing.[4] However, AI-driven marketing, particularly hyper-personalization, inherently relies on extensive data collection and granular profiling of individuals.[5] While the Act mandates consent, it explicitly acknowledges that it does not comprehensively cover AI-related privacy risks, such as automated decision-making or algorithmic transparency.[5] This suggests that obtaining initial consent for general data collection might not adequately encompass all subsequent, evolving AI-driven uses or inferences, especially if the AI's capabilities or applications change over time. The provision for easily accessible mechanisms to withdraw consent [4] becomes critically important for AI systems that continuously learn and adapt, necessitating a dynamic approach to consent management.

For client, this means designing consent mechanisms that extend beyond mere data collection. Consent should ideally cover the *types of AI processing* and *automated*

*decisions* that will be made using that data in marketing contexts. This requires a dynamic consent architecture that can anticipate future AI applications or provide consumers with granular control over how their data fuels AI. Furthermore, implementing comprehensive transparency measures and clear data disclosure policies [5] is crucial for effectively communicating AI's data processing activities to users, thereby securing and maintaining valid and informed consent, and mitigating risks of invasive tracking.[5]

### 2.2 Information Technology Act, 2000 and Rules (including IT Rules, 2021)

The Information Technology Act, 2000 (IT Act), serves as India's foundational legislation for regulating computer technology, combating cybercrime, and governing electronic commerce.[5] It provides legal recognition to electronic records and digital signatures, which has been instrumental in facilitating the growth of e-commerce in the country.[16] The Act criminalizes various cybercrimes, including hacking, spamming, identity theft, and phishing.[16] It also includes provisions enabling individuals to seek compensation in cases of damage or misuse of their personal data by unauthorized parties, and it mandates companies to obtain consent for collecting or using personal information.[16]

#### IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Introduced under the IT Act, these rules broadly define "intermediaries" as online service providers who process or provide services related to digital content on behalf of others.[17] They establish new categories: Social Media Intermediaries (SMI) and Significant Social Media Intermediaries (SSMI), with SSMIs subject to additional compliance obligations.[17] All intermediaries are mandated to provide a grievance redressal mechanism for user complaints.[18] The rules impose specific obligations on online publishers of news and current affairs content and curated audio-visual content. These include content classification, age-restricted ratings (U, U/A 7+, 13+, 16+, A), viewer discretion advisories, and the appointment of India-based Grievance Officers.[17] Notably, Rule 4(4) specifically mandates large platforms to audit their algorithmic tools for fairness, bias, and privacy risks.[19] Furthermore, Section 69A of the IT Act empowers

the government to block public access to content under specified conditions [15], and the IT Rules 2021 impose obligations on intermediaries to take down unlawful content, including AI-generated material.[19]

### AI-Specific Gaps

Despite its broad scope and subsequent amendments, the IT Act lacks specific provisions explicitly tailored for AI. This limits its efficacy in comprehensively addressing privacy issues and other unique challenges arising from AI applications.[5] While the IT Rules 2021 introduce obligations for intermediaries concerning algorithmic audits and unlawful content, they do not fully encompass the unique complexities of AI's autonomous and generative capabilities.[19]

### Evolving Intermediary Liability and AI Content

The IT Rules 2021 define intermediaries and impose obligations, including the requirement to take down unlawful content.[17] A significant development is the proposed Digital India Act, which aims to remove "safe harbour" immunity for online intermediaries concerning purposeful misinformation or other content violations from third parties.[20] This signifies a clear legislative intent to shift accountability more directly onto platforms for moderating and removing disallowed content. This shift is particularly relevant given AI's increasing capacity to generate sophisticated misinformation and deepfakes.[7C]

If client utilizes AI to generate marketing content that is subsequently disseminated via online intermediaries, such as social media platforms, the responsibility for ensuring that such content is lawful, truthful, and non-misleading will increasingly fall on *both* brand (as the advertiser/creator) and the intermediary. The future Digital India Act is poised to strengthen this accountability, potentially making brand more directly liable for the AI-generated content it places on platforms, even if the platform itself has moderation duties. This evolving liability landscape necessitates the implementation of robust internal vetting processes for all AI-generated marketing assets before their public deployment.

## 2.3 Consumer Protection Act, 2019 and E-Commerce Rules, 2020

The Consumer Protection Act, 2019 (CPA), along with the Consumer Protection (E-Commerce) Rules, 2020, establishes a modernized and robust regulatory framework aimed at safeguarding consumer rights in the digital domain.[22] This legislation addresses new forms of exploitation that have emerged with digital commerce, including data breaches, misleading advertisements, and unfair trade practices.[22]

### Key Provisions

The Central Consumer Protection Authority (CCPA), established under the CPA, is empowered to investigate violations, initiate class-action suits, and take swift action against unfair trade practices.[22] Under Section 21 of the CPA, the CCPA specifically targets misleading advertisements, a common feature in digital marketing, and can impose penalties or ban deceptive promotions.[1] Advertisers, brands, publishers, and endorsers may be held liable for legal violations in AI-generated advertisements.[1] Notably, endorsers who promote illegal advertisements without due diligence can face significant penalties, including fines up to Rs 10 lakh, which may extend to Rs 50 lakh for repeat offenses.[23] Section 2(47) of the CPA, 2019, explicitly defines and prohibits unfair trade practices, including false claims about the quality, quantity, or standard of goods and services.[22] The Guidelines for Prevention of Misleading Advertisements and Endorsements, issued under the CPA, further outline criteria for permissible advertisements and restrictions on misleading claims.[1] The E-Commerce Rules, 2020, specifically Rule 6(1), prohibit the publication or facilitation of false or misleading reviews by online platforms.[22] These rules also detail obligations for e-commerce entities, mandatory disclosures, and advertising standards.[22]

A significant area of focus for the CCPA is "Dark Patterns." The Authority issued the "Guidelines for Prevention and Regulation of Dark Patterns, 2023," which explicitly prohibit deceptive design interfaces (UI/UX) that mislead consumers or manipulate their decision-making.[24] The guidelines identify specific dark patterns such as "False Urgency" (falsely implying scarcity), "Basket Sneaking" (adding items without consent), "Confirm Shaming" (using guilt to nudge purchases), and "Drip Pricing" (not revealing

full price upfront).[26] E-commerce platforms are advised to conduct self-audits to identify and resolve such dark patterns.[24]

Regarding algorithmic bias, the CPA 2019 and E-Commerce Rules 2020 are applicable to AI-enabled services.[19] Algorithmic bias can manifest in discriminatory advertising and limit diversity in AI-generated content.[7] The Ministry of Consumer Affairs is actively investigating underlying algorithms and data-driven pricing strategies that may lead to discriminatory pricing practices by e-commerce companies.[25]

**AI as a Facilitator of Deceptive Practices and Misleading Advertisements**

AI's advanced capabilities, particularly its ability to analyze vast amounts of data, enable highly personalized shopping experiences and dynamic pricing strategies.[3] However, this power can be leveraged for manipulation and persuasion through subtle nudges or the exploitation of consumer vulnerabilities.[7] The CCPA's "Dark Patterns" guidelines [24] explicitly target such deceptive design interfaces. Furthermore, the CPA strictly regulates misleading advertisements.[1] If client uses AI for highly personalized marketing, there is a substantial risk of inadvertently crossing the line into deceptive practices or "dark patterns," even if the initial intent is not malicious.

This means client must not only ensure the factual accuracy and legality of its AI-generated marketing content but also critically evaluate the *method* of delivery and targeting employed by AI systems. This necessitates auditing AI systems for manipulative design elements, assessing their potential for "nudging" consumers into unintended actions, and ensuring that dynamic pricing models do not lead to discriminatory outcomes that violate consumer rights.[25] Compliance with these guidelines is crucial to avoid CCPA action, potential penalties, and to maintain consumer trust.

## 2.4 Intellectual Property Laws (Copyright Act, 1957 & Trademarks Act, 1999)

### Copyright Act, 1957

The Copyright Act, 1957, is the primary legislation governing copyright protection in India, extending legal protection to original literary, dramatic, musical, and artistic works, as well as cinematographic films and sound recordings.[1]

**Authorship & Ownership Ambiguity for AI-Generated Content:** The Act was framed with the fundamental premise that human beings were the sole creators of original work.[9] Section 17 of the Act stipulates that the author of a work is its first owner. However, AI currently lacks legal status in India and therefore cannot be considered an 'author' or 'owner' of the works it creates.[1] For "computer-generated works," authorship is assigned to the person who

*causes* the work to be produced.[9] This provision, originally drafted in the context of conventional automation, is increasingly proving inadequate in the age of advanced AI, leading to significant legal uncertainty when AI produces work with minimal human involvement.[9] Indian courts consistently emphasize that originality requires the application of "skill and judgment" and a "creative effort by a human author".[10] Consequently, purely AI-generated works, particularly those with "no evident contribution on the human side," are unlikely to be protected under copyright law in India.[9]

**AI Training Data Infringement:** The unauthorized use of copyrighted works to train AI models is a major and highly contentious legal issue, with ongoing legal cases in India, such as *ANI Media (P) Ltd. v. Open AI Inc.* in the Delhi High Court.[2] The Department for Promotion of Industry and Internal Trade (DPIIT) clarified in mid-2024 that AI developers must generally obtain authorization from copyright holders to use their content for training purposes. The DPIIT explicitly rejected any blanket "fair use" defense under Section 52 of the Copyright Act, 1957, for commercial-scale AI training.[29]

## Trademarks Act, 1999

Under the Trade Marks Act of 1999 and common law principles, a mark or visual symbol that can be graphically represented and distinguishes goods and services can be protected as a trademark.[1]

**AI-Generated Trademarks:** Indian law currently does not expressly recognize non-human creators.[31] Trademark law fundamentally hinges on a natural or juristic person being the proprietor of a mark. When AI plays a central role in the creation of a mark, the question of ownership becomes legally complex. In the absence of statutory recognition of AI as a legal person, the AI itself cannot be named as the proprietor. Instead, the person or entity who commissioned, programmed, or prompted the AI to generate the trademark would typically be considered the rightful applicant.[31] AI branding tools can inadvertently generate marks that closely resemble or are too similar to existing registered trademarks, thereby heightening the risk of confusion or deception.[31] Therefore, conducting comprehensive trademark searches is critical to avoid conflicts.[31] Clear contractual ownership of AI-generated content with AI platform providers is also crucial to avoid disputes.[31]

## The Dual Nature of IP Risk: Input and Output

When brand utilizes AI in its marketing efforts, it faces distinct yet interconnected intellectual property risks on two fronts. The first is **Inbound IP Risk**, concerning the training data. The data used to train the AI model, whether internally generated or sourced from third parties, may include copyrighted material. The ongoing *ANI v. OpenAI* case [11] and the DPIIT clarification [29] strongly indicate that unauthorized use of copyrighted content for commercial AI training constitutes infringement, as "fair dealing" exceptions are limited.[29] This means Clients must ensure that any AI tools it uses or develops have been trained on legally acquired and licensed data, or that the use falls squarely within a recognized statutory exception.

The second is **Outbound IP Risk**, pertaining to the AI-generated marketing assets themselves. If these assets lack sufficient human creativity or significant human input, they may not qualify for copyright protection under Indian law.[9] This directly compromises client's ability to assert exclusive rights over its marketing materials,

including licensing or commercializing them, or defending against unauthorized use. Conversely, if AI-generated outputs too closely resemble existing copyrighted works (even without direct copying from training data), they could lead to copyright infringement claims.[32] Additionally, there is a risk of "passing off" if AI-generated works cause consumer confusion about their source or official affiliation.[32]

Therefore, client needs a robust, two-pronged IP strategy that addresses both the provenance of AI training data and the originality and non-infringing nature of the AI-generated marketing outputs. This implies diligent due diligence on AI tools and their underlying data, clear contractual terms with AI vendors regarding IP ownership and indemnification, and robust internal creative oversight to ensure sufficient human "skill and judgment" is applied to AI outputs to secure copyrightability. Furthermore, performing standard IP clearance (trademark and copyright searches) for all AI-generated assets before public use is essential.

### 2.5 Constitutional Principles and Fundamental Rights

While India currently lacks specific, comprehensive AI legislation, the fundamental rights enshrined in the Indian Constitution serve as overarching principles that implicitly govern AI development and deployment.

#### Right to Privacy (Article 21)

The Supreme Court of India recognized privacy as a fundamental right under Article 21 of the Constitution in 2017.[4] The Digital Personal Data Protection Act, 2023, is a significant legislative step towards strengthening and operationalizing this fundamental right in the digital age.[4]

#### Right to Equality (Article 14) and Freedom of Expression (Article 19)

Algorithmic bias, which has the potential to perpetuate and even amplify existing

societal biases, poses a direct threat to the right to equality under Article 14.[7] Such biases can lead to discriminatory outcomes in various applications, including marketing. Furthermore, by limiting diversity in content or creating discriminatory narratives, algorithmic bias can also impact freedom of expression under Article 19.[34]

**Constitutional Underpinnings of AI Governance**

The fundamental rights enshrined in the Indian Constitution—namely the right to privacy (Article 21), the right to equality (Article 14), and freedom of expression (Article 19)—serve as overarching principles that implicitly govern AI development and deployment. The ongoing discourse on algorithmic bias, for instance, is explicitly linked to upholding the "Golden Triangle" principles of the Indian Constitution.[34] The consistent push for "Responsible AI" by government bodies like NITI Aayog [8] and industry bodies like NASSCOM [8] is explicitly rooted in these constitutional values.

This means that even in the absence of explicit AI legislation, client's AI marketing practices are implicitly subject to constitutional scrutiny. Technical compliance with existing statutes might not be sufficient; practices must also fundamentally align with broader ethical principles of fairness, non-discrimination, and respect for privacy to avoid potential legal challenges based on fundamental rights. This reinforces the critical need for brand to adopt ethical AI standards and implement robust bias mitigation techniques [5] as a core part of its AI strategy, extending beyond mere statutory compliance.

## 3. Key Legal Risks and Challenges of AI in Marketing

### 3.1 Data Privacy and Automated Decision-Making Risks

AI applications inherently rely on massive datasets for training, leading to large-scale collection of personal data. This creates significant privacy risks and the potential for misuse.[5] AI enables granular data profiling, where individuals can be categorized based on their online activities. While this is beneficial for targeted marketing, it may also result in invasive tracking and privacy invasions.[5]

AI models frequently make decisions based on user data, which can potentially impact individuals' lives, for example, in contexts like job offers or loan approvals. The lack of transparency in these automated decisions raises significant ethical and legal concerns.[5] The DPDP Act mandates explicit consent for data processing.[4] However, the dynamic and evolving nature of AI makes obtaining and managing truly informed consent for all potential future uses of data, especially for complex AI-driven processes, a significant challenge.[5] Furthermore, the misuse or negligent handling of personal data collected by AI systems can lead to severe privacy breaches and identity theft.[7]

#### The Opaque Nature of AI Decisions and the Need for Explainability

AI models frequently make decisions based on user data, which can profoundly impact individuals. However, without transparency, these automated decisions may harm individuals, raising ethical and legal concerns.[5] This highlights the "black box" problem, where the internal workings and decision-making logic of AI systems are often opaque. While the DPDP Act emphasizes consent, it does not explicitly cover AI-related privacy risks, such as automated decision-making or algorithmic transparency.[5] Nevertheless, NITI Aayog's responsible AI principles explicitly include "Transparency and

explainability" [8], and NASSCOM's guidelines advocate for publicly disclosing data and algorithm sources.[13]

For Clients, when utilizing AI for targeted marketing or automated customer interactions (e.g., chatbots, personalized offers), the risk extends beyond *what* the AI does to *how* it arrives at its decisions. If an AI system makes a decision—such as segmenting a customer for a specific promotion or denying a service—that leads to consumer harm, discrimination, or a perception of unfairness, and Clients cannot explain the underlying rationale, it could face legal challenges under consumer protection or data privacy laws, even if not explicitly covered by AI-specific legislation. This necessitates investing in Explainable AI (XAI) capabilities and maintaining detailed records of AI model logic, data inputs, and decision pathways to ensure accountability and build trust with consumers.

### 3.2 Algorithmic Bias and Discrimination

AI models can inherently exhibit biases, which are often hidden within the algorithms themselves. [33] These biases typically stem from the data used to train the AI, which may reflect "past discriminatory practices or societal biases".[5] This can inadvertently reinforce or amplify existing biases, leading to unfair treatment of certain individuals or groups.[5]

#### Manifestations in Marketing

Algorithmic discrimination can arise from biased agents, such as training data reflecting underrepresentation of certain demographic groups, or from biased feature selection, where proxy variables like ZIP codes are used for race, or web browsing history inadvertently excludes certain demographics.[33] In marketing, this can lead to discriminatory advertising, limited diversity in AI-generated content, or the perpetuation of harmful stereotypes.[7] Current Indian laws, including the Information Technology Act 2000 and the Digital Personal Data Protection Act 2023, are noted to fall short of adequately addressing algorithmic accountability.[34]

## Government Focus

The issue of algorithmic bias is a prominent concern at the highest levels of government. Prime Minister Modi has advocated for a global framework and domestic legislation in India to counteract algorithmic bias.[34] The Ministry of Electronics and Information Technology (MeitY) has also published a governance framework for AI that explicitly includes "fairness" as a key principle.[19]

## Reputational Harm as a Precursor to Legal Action

While specific, comprehensive laws directly addressing algorithmic bias are currently lacking in India [34], the perpetuation of stereotypes and discriminatory advertising by AI [7] directly results in unfair treatment of certain individuals or groups.[5] This directly implicates fundamental constitutional principles such as the right to equality (Article 14).[34] Even in the absence of explicit legal penalties for bias

*per se* in current statutes, a major corporate entity like Clients faces significant and immediate reputational damage, public outcry, and consumer backlash if its AI marketing practices are perceived as biased or discriminatory. The Advertising Standards Council of India (ASCI), a self-regulatory body, actively promotes ethical advertising [23] and has issued reports focusing on responsible AI integration.[38] This indicates that industry self-regulation and consumer advocacy may act as an early warning system or an initial enforcement mechanism for such issues, potentially leading to public censure or calls for withdrawal of advertisements.

Therefore, Clients must implement robust bias mitigation techniques and conduct regular, independent audits of its AI models [4] not merely as a future-proofing measure for legal compliance, but as a critical component of brand reputation management and maintaining consumer trust. This commitment to ethical AI standards [5] should be integrated into the entire AI lifecycle, from data selection and model training to deployment and continuous monitoring, to proactively identify and address potential biases.

### 3.3 Misleading Content, Deepfakes, and Consumer Deception

Generative AI tools offer advanced capabilities for automating the creation of original content, including text, images, articles, and various marketing collaterals.[1] This includes the production of highly realistic but fake videos or audio recordings known as deepfakes.[7]

#### Risks

AI-generated content, particularly deepfakes, poses significant risks. It can be used to spread misinformation and propaganda at a harmful scale.[7] Highly realistic deepfakes can deceive consumers, influence public opinion, or damage reputations.[7]

#### Current Legal Recourse

The **Consumer Protection Act, 2019 (CPA)**, explicitly prohibits misleading advertisements (Section 21) [1] and empowers the Central Consumer Protection Authority (CCPA) to investigate and take action against such violations.[1] Advertisers, brands, publishers, and endorsers may be held liable for legal violations in AI-generated advertisements.[1] Penalties can be imposed on endorsers who promote illegal advertisements without due diligence.[23]

The **Information Technology Act, 2000 (IT Act)**, while not AI-specific, offers existing provisions that can be applied. Section 66D penalizes cheating by impersonation using a computer resource, potentially applicable to deepfakes used for fraudulent impersonation. Section 66E addresses privacy violations, which could be relevant if deepfakes are used to share private content. Sections 67, 67A, and 67B prohibit and punish the publication or transmission of obscene or sexually explicit material. Section 69A empowers the government to block public access to content.[15]

**Defamation laws** can be invoked if deepfakes are used to spread misinformation or damage an individual's reputation.[21] Under the

**Copyright Act, 1957**, copyright holders can initiate legal proceedings if copyrighted material is used without permission to create deepfakes.[21] Furthermore, Indian courts have affirmed the

**personality rights** of celebrities, providing protection against the unauthorized creation of AI-generated content that uses their audio or visual likeness.[2]

### Regulatory Push for Transparency

The Ministry of Electronics and Information Technology (MeitY) has advised on the use of technology like watermarking and labeling to prevent, detect, and track harmful AI outcomes, including malicious synthetic media like deepfakes.[21] The Advertising Standards Council of India (ASCI)'s influencer guidelines require mandatory disclosure labels (e.g., #ad, #collab) for promotional content, and explicitly define and include "Virtual Influencers," requiring them to disclose that they are not real human beings.[41] ASCI recommends disclosure when AI features prominently in an ad and is unlikely to be obvious to consumers.[12]

### The Erosion of Trust and the Imperative of Disclosure

The proliferation of deepfakes and misinformation generated by AI [7] directly erodes consumer trust in digital content. While existing laws offer some recourse, they are often inadequate in addressing rapidly unfolding threats.[15] The consistent emphasis from MeitY [21] and ASCI [12] on mandatory labeling and disclosure of AI-generated content, especially deepfakes, indicates a proactive regulatory stance aimed at mitigating this growing trust deficit. This is fundamentally about ensuring "digital literacy and awareness" so individuals can make "informed choices".[1]

For Clients, this means adopting a stringent internal policy for labeling all AI-generated marketing assets, particularly those involving synthetic media (e.g., AI-generated voices, faces, or text that could be mistaken for human-created or real content). This is not merely a compliance measure to avoid legal penalties for misleading advertisements but a critical strategy for proactively building and maintaining

consumer trust in an increasingly AI-saturated media landscape. Failure to disclose AI involvement could lead to significant consumer backlash, complaints to regulatory bodies like CCPA or ASCI, and potentially serve as evidence of deception, even if the content itself is not explicitly "misleading" in a traditional sense.

### 3.4 Intellectual Property Infringement and Ownership Ambiguities

#### Training Data Infringement

The unauthorized use of copyrighted content for AI training is a major and contentious issue, with ongoing lawsuits in India, such as *ANI v. OpenAI*.[11] The Department for Promotion of Industry and Internal Trade (DPIIT) has explicitly clarified that AI developers must generally obtain licenses from copyright holders to use their work for training purposes, rejecting a blanket "fair use" defense under Section 52 of the Copyright Act for commercial-scale AI training.[29]

#### Authorship & Ownership of Outputs

Indian copyright law was framed on the premise of human creativity.[9] While Section 2(d)(vi) of the Copyright Act assigns authorship for "computer-generated works" to the person who causes the work to be created, this provision is increasingly inadequate for autonomous AI.[9] AI systems are not recognized as legal persons and, therefore, cannot own copyright.[28] Indian courts require "skill, judgment, and effort" and a "creative effort by a human author" for originality.[10] Purely AI-generated works with "very little human involvement" or "no evident contribution on the human side" are unlikely to be copyrightable.[9]

### Trademark Concerns

AI branding tools can inadvertently generate marks that closely resemble or are too similar to existing registered trademarks, thereby heightening the risk of confusion or deception.[31] Ownership of AI-generated trademarks is also ambiguous, with the person or entity who commissioned, programmed, or prompted the AI typically considered the rightful applicant.[31] Clear contractual ownership of AI-generated content with AI platform providers is crucial to avoid disputes.[31]

### The Two-Way Street of IP Risk

The intellectual property discussion reveals that client faces distinct yet interconnected IP risks when leveraging AI in marketing. The first is **Inbound IP Risk**, which relates to the training data. The data used to train the AI model, whether proprietary or sourced from third parties, may include copyrighted material. The ongoing *ANI v. OpenAI* lawsuit [11] and the DPIIT's clarification [29] demonstrate that unauthorized use of copyrighted content for commercial AI training is a live legal issue and likely constitutes infringement, as "fair dealing" exceptions are limited.[29] This means Clients must ensure that any AI tools it utilizes or develops have been trained on legally acquired and licensed data, or that the use falls squarely within a recognized exception.

The second is **Outbound IP Risk**, pertaining to the marketing assets produced by AI itself. If these assets lack "significant human input" or "meaningful creative decisions" [28], they may not qualify for copyright protection under Indian law.[9] This directly impacts Client's ability to exclusively own, license, commercialize, or defend against unauthorized use of its marketing materials. Conversely, if AI-generated outputs too closely resemble existing copyrighted works (even if not directly copied from training data), they could lead to copyright infringement claims.[32] Additionally, there is a "passing off" risk if AI-generated works cause consumer confusion about their source or official affiliation.[32]

Therefore, Clients' needs a comprehensive IP strategy that addresses both the provenance of AI training data and the originality and non-infringing nature of the AI-generated marketing outputs. This implies diligent due diligence on AI tools and their

underlying data, clear contractual terms with AI vendors regarding IP ownership and indemnification, and robust internal creative oversight to ensure sufficient human "skill and judgment" is applied to AI outputs to secure copyrightability. Furthermore, conducting thorough IP clearance (trademark and copyright searches) for all AI-generated assets before public use is essential.

### 3.5 Liability for AI System Errors and Harms

India currently lacks specific AI-specific legislation that clearly defines liability for AI system errors or harms.[44] There is also a lack of legal clarity on whether AI should be classified as a product or a service, which significantly impacts the applicability of existing liability frameworks.[44]

#### Existing Frameworks & Their Limitations

The **Consumer Protection Act, 2019 (CPA)**, includes product liability rules that apply to manufacturers or sellers for defective products causing harm.[44] However, the CPA's definition of "harm" primarily addresses physical injury and does not explicitly extend to "intangible objects" or "digital and data-related damages," leading to ambiguity in AI-related cases.[44] A promise of "extraordinary results/claims" in relation to an AI product or service that culminates in a "lack of credible information" may attract product or service liability under Sections 84, 85, and 86 of the CPA.[30] The

**tort of negligent misinformation** can be successfully invoked against entities that deploy AI to engage with (e.g., complaint redressal chatbots or AI assistants in marketing) if negligent misinformation is provided, on which the user relies and consequently suffers harm.[30] Furthermore, pricing algorithms, even when designed and implemented unilaterally by individual undertakings, can lead to anti-competitive effects resembling collusion due to increased transparency in digital markets.[45] In such scenarios, the undertaking is responsible for the conduct of the algorithm, treating it as an "extended hand" or a "mere tool".[45]

**Proposed Frameworks**

Legal literature suggests a pressing need for a revised legal framework in India that incorporates concepts like "digital harm" and clear liability allocation for AI.[44] Proposals include adopting a "risk-utility test" for AI defects and a "joint and several liability" approach to ensure fair compensation for victims.[44]

**The Shifting Paradigm of Liability from "User" to "Developer/Deployer"**

Traditional negligence frameworks often focus on the human user's actions. However, for AI, the responsibility for harm frequently shifts towards the creator or developer of the AI system, or the entity deploying it.[44] The concept of the algorithm as a "tool" in the hands of the undertaking [45] implies that Clients, as the deployer of AI in marketing, would be responsible for its conduct, much like it would be for an employee.[45] This indicates a move towards a "strict liability" or "product liability" approach for AI systems, particularly if they are deemed "defective in design" or operation.[44] The current ambiguity in defining "harm" under the CPA to include "digital and data-related damages" [44] is a critical gap that is actively being addressed in policy discussions.

Consequently, Clients cannot simply outsource AI development or deployment and absolve itself of liability. It must implement rigorous testing, validation, and continuous post-deployment monitoring of AI systems used in marketing to detect and mitigate errors, biases, or unintended harmful outcomes. This includes ensuring internal expertise to understand the AI system's limitations and potential risks and having clear indemnification clauses with AI vendors. The overarching focus should be on preventing "digital harm" and ensuring fair compensation for victims, even as the precise legal definitions and liability frameworks continue to evolve.

# 4. Evolving Regulatory Landscape and Future Outlook

## 4.1 The Proposed Digital India Act (DIA)

The proposed Digital India Act (DIA) represents a significant and ambitious legislative initiative aimed at replacing the outdated Information Technology Act, 2000. Its primary objective is to establish a comprehensive legal framework for India's digital economy, addressing modern challenges that the IT Act could not adequately cover.[6] The DIA seeks to ensure that the Indian internet is Open, Safe, Trusted, and Accountable.[6]

### Key Features

The DIA aims to create new regulations around emerging technologies, including 5G, IoT devices, cloud computing, metaverse, blockchain, and cryptocurrency, addressing associated security and privacy concerns.[20] It will reclassify online intermediaries into separate categories (e.g., cloud service providers, social media platforms, ISPs, metaverse, OTT providers) with specific regulations for each, moving away from a general label or size-based classification.[20] A critical feature is the proposed removal of "safe harbour" legal immunity for online intermediaries for purposeful misinformation or other content violations from third parties. This shifts the legal obligation onto platforms to moderate and remove disallowed content, making them accountable for content violations or cybercrimes on their websites.[20] The DIA is also expected to complement the Digital Personal Data Protection Act, 2023, by giving citizens more control over their personal data online.[20] Significantly, it is anticipated to include special provisions to regulate AI-generated content, specifically addressing deepfakes, misinformation, and biased algorithms.[47] The Act will also focus on online safety for children, including age-appropriate content, parental consent, and preventing online abuse targeting minors.[47] Furthermore, it will impose obligations on digital platforms for faster grievance redressal, requiring them to respond to user complaints and legal notices in a time-bound manner.[47] Finally, the DIA may introduce

a "Digital Bill of Rights" ensuring freedom of expression, protection against surveillance, and digital access as a public good.[47]

### Status

The DIA is currently in its drafting stage and is expected to be passed in 2025.[6] Public consultations on draft rules have been ongoing, indicating active development and stakeholder engagement.[14]

### Proactive Compliance for Anticipated Legislation

The Digital India Act is explicitly designed to address the "key limitations of the IT Act" [47], which notably include the absence of robust provisions for user privacy, deepfakes, and AI-generated misinformation.[47] The detailed features proposed for the DIA [20] directly target many of the current "key gaps in Indian law" concerning AI.[5] While the DIA is not yet enacted, its comprehensive proposals clearly signal the government's future regulatory direction and priorities.

Therefore, Clients should not adopt a wait-and-see approach but should proactively align its AI marketing practices with the anticipated provisions of the Digital India Act. This includes strengthening internal content moderation processes, implementing robust fact-checking mechanisms for AI-generated content, and enhancing transparency and accountability measures beyond current minimums. Early adoption of these principles will facilitate a smoother transition once the DIA is enacted, demonstrate a commitment to responsible AI, and potentially influence future regulatory interpretations or enforcement approaches in a favorable manner.

## 4.2 Government and Industry Guidelines (NITI Aayog, MeitY, NASSCOM, ASCI)

In the absence of comprehensive AI-specific legislation, guidelines and frameworks from government bodies and industry associations play a crucial role in shaping responsible AI practices in India.

### NITI Aayog

As the apex public policy think tank of the Government of India, NITI Aayog has been instrumental in shaping India's AI strategy. It published the "National Strategy for Artificial Intelligence" in 2018 and subsequent "Responsible AI Approach Documents": Part 1: Principles for Responsible AI (2021), Part 2: Operationalizing Principles for Responsible AI (2021), and Part 3: Facial Recognition Technologies (2022).[6] These documents outline broad ethical principles for the design, development, and deployment of AI, including Safety & Reliability, Equality, Inclusivity & Non-discrimination, Privacy & Security, Transparency, Accountability, and Protection & Reinforcement of Positive Human Values.[8] The overarching aim is to strike a balance between protecting society and fostering innovation in AI.[8]

### MeitY (Ministry of Electronics and Information Technology)

MeitY published a governance framework in 2025, detailing eight key principles for AI: transparency, accountability, safety and reliability, privacy and security, fairness, human oversight, inclusive innovation, and technology-led governance.[19] A draft report by a MeitY subcommittee (November 2023) recommends establishing an inter-ministerial committee, a technical secretariat, and an AI incident database. It also encourages industry transparency commitments and investigating technologies like watermarking and labeling for malicious synthetic data.[40] The report acknowledges that existing laws apply to AI but notes a "glaring loophole" concerning publicly available data.[40]

### NASSCOM

The National Association of Software and Service Companies (NASSCOM) has actively contributed to the responsible AI discourse. It published a "Responsible AI Governance Framework" and "Responsible AI Guidelines for Generative AI" in June 2023.[8] These guidelines aim to promote and facilitate the responsible development and use of Generative AI solutions, balancing innovation with public safety concerns.[13] They emphasize demonstrating transparency and accountability through public disclosures about methodologies, model training datasets, and tools.[13] NASSCOM's "Developer's Playbook for Responsible AI in India" provides a voluntary framework for identifying and mitigating risks.[56]

**ASCI (Advertising Standards Council of India)**

As an independent, voluntary self-regulatory organization, ASCI aims to ensure advertisements in India are fair, honest, and truthful.[23] ASCI has released reports, such as "AdNext: The AI Edition," focusing on responsible AI integration, transparency, and accountability in advertising.[38] Its influencer guidelines require mandatory disclosure labels (e.g., #ad, #collab) for promotional content and explicitly define and include "Virtual Influencers," requiring them to disclose that they are not real human beings.[41] ASCI recommends disclosure when AI features prominently in an ad and is unlikely to be obvious to consumers.[12]

**The Imperative of Adhering to "Soft Law"**

These guidelines, while not legally binding in the same way as statutes, function as a form of "soft law." They set industry expectations, establish de facto standards for ethical conduct, and significantly influence the direction of future legislation. Adhering to them is essential for ethical conduct, proactive risk mitigation, and demonstrating corporate responsibility, especially in the current environment where explicit statutory law for AI is still developing.

Furthermore, India's active participation in international AI governance discussions, such as the G7's Hiroshima AI Process, the G20's New Delhi Leaders Declaration, and the 2023 AI Safety Summit in the UK, indicates a commitment to fostering safe, secure, and accountable digital ecosystems.[19] The Bureau of Indian Standards (BIS), through its LITD 30 technical committee, is also developing national AI standards aligned with

global benchmarks, covering areas such as trust, data quality, and risk management.[19] This global alignment further reinforces the importance of adhering to principles of responsible AI.

## 5. Conclusions and Recommendations

The integration of AI into marketing assets presents both significant opportunities and complex legal challenges for Clients in India. The current legal framework is fragmented, relying on existing laws that are not fully equipped to address AI's unique complexities. However, the rapidly evolving regulatory landscape, spearheaded by the proposed Digital India Act and various government and industry guidelines, signals a clear future direction towards greater accountability, transparency, and ethical considerations in AI deployment.

To proactively navigate these legal waters and uphold their reputation as a responsible corporate entity, Clients should implement the following strategic recommendations:

1. **Establish a Cross-Functional AI Governance Committee:** Form a dedicated committee comprising legal, marketing, IT, data privacy, and ethics experts. This committee should be tasked with overseeing the development, deployment, and monitoring of all AI systems used in marketing, ensuring alignment with legal requirements, ethical principles, and internal policies.
2. **Implement Robust Data Governance for AI:**
    - **Dynamic Consent Architecture:** Develop consent mechanisms that go beyond mere data collection, explicitly covering the types of AI processing and automated decisions that will be made using consumer data. Ensure easily accessible mechanisms for users to understand and withdraw consent at any time.
    - **Data Minimization & Quality:** Adopt strict data minimization practices, collecting only the personal data necessary for AI systems. Implement rigorous data quality and integrity checks to prevent biases stemming from flawed data input.
    - **Regular Audits:** Conduct periodic, independent audits of AI models to detect biases, inefficiencies, security vulnerabilities, and ensure compliance with DPDP Act principles.
3. **Prioritize Algorithmic Fairness and Bias Mitigation:**
    - **Bias Assessment & Mitigation:** Implement techniques to detect and mitigate biases in AI models throughout their lifecycle, from training data selection to output generation. This is crucial to prevent discriminatory advertising and ensure inclusive content.
    - **Explainable AI (XAI):** Invest in XAI capabilities to understand and explain the

decision-making logic of AI systems, particularly for targeted marketing or automated customer interactions. Maintain detailed records of AI model logic and data inputs to ensure accountability.

4. **Ensure Transparency and Disclosure in AI-Generated Content:**
    - **Mandatory Labeling:** Adopt a stringent internal policy for labeling all AI-generated marketing assets, especially synthetic media (e.g., AI-generated voices, faces, or text that could be mistaken for human-created or real content).
    - **ASCI Compliance:** Adhere strictly to ASCI's guidelines, including mandatory disclosure labels for promotional content and explicit disclosure for virtual influencers, particularly where AI features prominently and is not immediately obvious to consumers.
5. **Strengthen Intellectual Property Due Diligence:**
    - **AI Training Data Vetting:** Conduct thorough due diligence on all AI tools and their underlying training data to ensure that copyrighted material has been legally acquired and licensed, or that its use falls squarely within a recognized exception.
    - **Human Creativity & Ownership:** Implement internal creative oversight to ensure sufficient human "skill and judgment" is applied to AI outputs to secure copyrightability for Clients' marketing materials.
    - **IP Clearance:** Perform comprehensive intellectual property clearance (trademark and copyright searches) for all AI-generated assets before public use to mitigate infringement risks.
    - **Vendor Contracts:** Ensure clear contractual terms with AI vendors regarding IP ownership, indemnification for infringement, and data usage rights.
6. **Develop a Comprehensive AI Liability Framework:**
    - **Internal Protocols:** Establish clear internal protocols for detecting and responding to AI system errors or unintended harmful outcomes.
    - **Accountability Structures:** Define clear accountability structures within the organization for AI deployment and any resulting harms, acknowledging the shifting liability paradigm towards the deployer.
    - **Digital Harm Definition:** Advocate for and prepare for potential future legal frameworks that expand the definition of "harm" to include "digital and data-related damages."
7. **Continuous Regulatory Monitoring and Adaptation:**
    - **Stay Updated:** Actively monitor developments related to the proposed Digital India Act, as well as ongoing guidelines and recommendations from MeitY, NITI Aayog, NASSCOM, and ASCI.

- **Proactive Alignment:** Proactively align AI marketing practices with anticipated legislative provisions to ensure a smoother transition once new laws are enacted.

8. **Foster a Culture of Responsible AI:**
    - **Training & Awareness:** Provide regular training to marketing, legal, and technical teams on responsible AI principles, legal obligations, and ethical considerations.
    - **Ethical Guidelines:** Develop and disseminate internal ethical guidelines for AI use in marketing that align with national and international best practices.

By adopting these proactive and comprehensive measures, Clients can leverage the transformative power of AI in its marketing assets while effectively mitigating legal risks, fostering consumer trust, and demonstrating leadership in responsible AI innovation within the Indian market.

**Works cited**


1. GENERATIVE AI AND ADVERTISING - ASCI, accessed July 29, 2025, https://www.ascionline.in/wp-content/uploads/2023/07/KCO-ASCI-Gen-AI-paper-27-July-2023.pdf
2. How AI is shaping the future of advertising - ASCI, accessed July 29, 2025, https://www.ascionline.in/academy/wp-content/uploads/2025/03/ADNext-Report-digital.pdf
3. India's AI-Powered Consumer Revolution: E-Commerce, Digital Payments, and Smart Retail, accessed July 29, 2025, https://www.researchgate.net/publication/392544261_India's_AI-Powered_Consumer_Revolution_E-Commerce_Digital_Payments_and_Smart_Retail
4. Digital Personal Data Protection Act - Impact on Marketers in India | ValueFirst, accessed July 29, 2025, https://www.vfirst.com/post/digital-personal-data-protection-act---impact-on-marketers-in-india
5. AI and Data Privacy in India: Emerging Legal and Ethical Challenges, accessed July 29, 2025, https://www.cyberlawconsulting.com/ai_and_data_privacy_in_India.php
6. The Cyber Legislations Governing AI – India & EU - Seth Associates, accessed July 29, 2025, https://www.sethassociates.com/the-cyber-legislations-governing-ai-india-eu.html
7. India looking at AI regulations and how this could impact the advertising and marketing sector | by Suchana Sarkar | Medium, accessed July 29, 2025, https://medium.com/@suchana.sarkar/india-looking-at-ai-regulations-and-how-this-could-impact-the-advertising-and-marketing-sector-c1a3074d9fbb
8. Responsible AI Policy Study, accessed July 29, 2025, https://cerai.iitm.ac.in/projects/responsible-ai-policy/
9. India's Copyright Law and AI: Legal Implications of AI-Generated Content Bare Act Legal Manor, accessed July 29, 2025, https://legalmanor.com/indias-copyright-law-and-ai-legal-implications-of-ai-generated-content/
10. THE IMPACT OF AI ON COPYRIGHT AND INTELLECTUAL PROPERTY RIGHTS IN DIGITAL CONTENT - JETIR.org, accessed July 29, 2025, https://www.jetir.org/papers/JETIR2502352.pdf
11. What have courts ruled with respect to AI and copyright? | Explained - The Hindu, accessed July 29, 2025, https://www.thehindu.com/sci-tech/technology/what-have-courts-ruled-with-respect-to-ai-and-copyright-explained/article69839851.ece
12. Disclosure of AI in Advertising: Striking the Balance Between Creativity and Responsibility, accessed July 29, 2025, https://www.asa.org.uk/news/disclosure-of-ai-in-advertising-striking-the-balance-between-creativity-and-responsibility.html
13. Guidelines for Generative AI by NASSCOM, accessed July 29, 2025, https://www.nasscom.in/ai/img/GenAI-Guidelines-June2023.pdf

14. Parliamentary Committee raises concern with MeitY over DPDP Act implementation lag, accessed July 29, 2025, https://www.storyboard18.com/how-it-works/parliamentary-committee-raises-concern-with-meity-over-dpdp-act-implementation-lag-77105.htm
15. Bridging the Digital Divide: Lessons from the US Take It Down Act in India's Data Protection Landscape - JURIST - Features - Legal News & Commentary, accessed July 29, 2025, https://www.jurist.org/features/2025/06/16/bridging-the-digital-divide-lessons-from-the-us-take-it-down-act-in-indias-data-protection-landscape/
16. IT Act 2000: Objectives, Features, Amendments, Sections, Offences and Penalties, accessed July 29, 2025, https://cleartax.in/s/it-act-2000
17. India's New Digital Media Ethics Code | Amagi Blog, accessed July 29, 2025, https://www.amagi.com/blog/new-intermediary-guidelines-and-digital-media-ethics-code-for-india
18. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 - PRS India, accessed July 29, 2025, https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021
19. India joins global push for safe AI as domestic framework takes shape - Storyboard18, accessed July 29, 2025, https://www.storyboard18.com/how-it-works/india-joins-global-push-for-safe-ai-as-domestic-framework-takes-shape-77365.htm
20. What is the Digital India Act? India's Newest Digital Law | UpGuard, accessed July 29, 2025, https://www.upguard.com/blog/digital-india-act
21. Govt Report to Delhi HC Stresses Deepfake Content Disclosure & Labeling, accessed July 29, 2025, https://vajiramandravi.com/current-affairs/govt-report-to-delhi-hc-stresses-deepfake-content-disclosure-labeling/
22. The Role Of Consumer Protection Act In Regulating Digital Platforms And Online Market Places - IJCRT.org, accessed July 29, 2025, https://www.ijcrt.org/papers/IJCRT25A4745.pdf
23. Consumer Protection Authority's Collaboration With Advertising Council To Harmonize Advertising Laws - Naik Naik, accessed July 29, 2025, https://naiknaik.com/2024/04/08/consumer-protection-authoritys-collaboration-with-advertising-council-to-harmonize-advertising-laws/
24. Central Consumer Protection Authority issues advisory to E-Commerce Platforms for self-audit within 3 months to detect Dark Patterns and ensure its resolution - PIB, accessed July 29, 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2134765
25. GOVERNMENT OF INDIA MINISTRY OF CONSUMER AFFAIRS, FOOD AND PUBLIC DISTRIBUTION DEPARTMENT OF CONSUMER AFFAIRS RAJYA SABHA UNSTAR - Digital Sansad, accessed July 29, 2025, https://sansad.in/getFile/annex/267/AU197_h0baLV.pdf?source=pqars
26. Guidelines for Prevention and Regulation of Dark Patterns, 2023, accessed July 29,

2025, https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Draft%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns%202023.pdf
27. Guidelines for Prevention and Regulation of Dark Patterns, 2023 Authority - U/powers conferred by section 18 of the Consumer Pro, accessed July 29, 2025, https://www.nls.ac.in/wp-content/uploads/2021/04/Dark-Patterns.pdf
28. Copyright Protection for AI-Generated Works in India - LawBhoomi, accessed July 29, 2025, https://lawbhoomi.com/copyright-protection-for-ai-generated-works-in-india/
29. AI Copyright Law India: Ownership Explained - Maheshwari & Co., accessed July 29, 2025, https://www.maheshwariandco.com/blog/ai-copyright-law-india/
30. Developing AI within India's regulatory framework - Law.asia, accessed July 29, 2025, https://law.asia/ai-governance-copyright-india/
31. AI Generated Trademarks in India: Legal Issues - Maheshwari & Co., accessed July 29, 2025, https://www.maheshwariandco.com/blog/ai-generated-trademarks-in-india/
32. Navigating AI-Generated art and copyright law - Shardul Amarchand Mangaldas & Co, accessed July 29, 2025, https://www.amsshardul.com/insight/navigating-ai-generated-art-and-copyright-law/
33. Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices - Frontiers, accessed July 29, 2025, https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2024.1320277/full
34. Algorithms, Biases, and the Constitution: A Threat to the Golden Triangle? - DNLU-SLJ, accessed July 29, 2025, https://dnluslj.in/algorithms-biases-and-the-constitution-a-threat-to-the-golden-triangle/
35. AIFORALL - Approach Document for India Part 1 ... - NITI Aayog, accessed July 29, 2025, https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf
36. Responsible AI at nasscom, accessed July 29, 2025, https://nasscom.in/ai/responsibleai/
37. ASCI: The Advertising Standards Council Of India, accessed July 29, 2025, https://www.ascionline.in/
38. ASCI Report: Indian Advertising Industry Embraces AI - Passionate In Marketing, accessed July 29, 2025, https://www.passionateinmarketing.com/asci-report-indian-advertising-industry-embraces-ai/
39. AI-lluminating the future: How artificial intelligence is changing advertising in India, accessed July 29, 2025, https://brandequity.economictimes.indiatimes.com/news/research/ai-lluminating-the-future-how-artificial-intelligence-is-changing-advertising-in-india/119597599
40. MeitY's AI Regulation Report: Ambitious But No Concrete Solutions - The secretariat, accessed July 29, 2025, https://thesecretariat.in/article/meity-s-ai-

regulation-report-ambitious-but-no-concrete-solutions
41. ASCI's Guidelines For “Influencer Advertising” on Digital Media-w.e.f 14th June 2021, accessed July 29, 2025, https://www.anppartners.in/blog/ascis-guidelines-for-influencer-advertising-on-digital-media
42. Home - ASCI Social, accessed July 29, 2025, https://www.ascionline.in/social/
43. Smarter Research, Safer Practices: IFERP Publishes New Guidelines on the Ethics of AI Use in Academics | Medial, accessed July 29, 2025, https://medial.app/news/smarter-research-safer-practices-iferp-publishes-new-guidelines-on-the-ethics-of-ai-use-in-academics-7e869dfacb6ba
44. Addressing Product and Service Liability Concerns in Artificial Intelligence: An Indian Perspective - Law School Policy Review, accessed July 29, 2025, https://lawschoolpolicyreview.com/2025/02/12/addressing-product-and-service-liability-concerns-in-artificial-intelligence-an-indian-perspective/
45. Algorithmic Collusion: Corporate Accountability and the Application of Art. 101 TFEU, accessed July 29, 2025, https://www.europeanpapers.eu/en/europeanforum/algorithmic-collusion-corporate-accountability-application-art-101-tfeu
46. Digital India Act | ML and AI Wiki by AryaXAI, accessed July 29, 2025, https://www.aryaxai.com/wiki/digital-india-act
47. Digital India Act 2025 – Overview & Features - Delhi Law Academy, accessed July 29, 2025, https://www.delhilawacademy.com/digital-india-act/
48. National Strategy for Artificial Intelligence - NITI Aayog, accessed July 29, 2025, https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
49. Approach Document for India Part 1- Principles for Responsible AI | NITI Aayog, accessed July 29, 2025, https://www.niti.gov.in/node/326
50. NITI Aayog - Centre for Responsible AI, accessed July 29, 2025, https://cerai.iitm.ac.in/collaborators/niti-aayog/
51. Results for tag 'Principles for Responsible AI' (7) - INDIAai, accessed July 29, 2025, https://indiaai.gov.in/search?queryData=%7B%22searchText%22%3A%22%22,%22tagName%22%3A%22Principles%20for%20Responsible%20AI%22,%22collectionTypes%22%3A%5B%5D,%22is_brand%22%3Afalse,%22read_time%22%3A%22%22,%22author_name%22%3A%22%22,%22published_date%22%3A%22%22,%22sort_by%22%3A%22%22%7D
52. Responsible - AI - 05082020 - NITI Aayog | PDF - Scribd, accessed July 29, 2025, https://fr.scribd.com/document/535286859/Responsible-AI-05082020-NITI-Aayog
53. AIforAll: Approach Document for India (Part 1 – Principles for Responsible AI), accessed July 29, 2025, https://aisggovernanceresourcesapp.azurewebsites.net/documents/31
54. Principles for Responsible AI Innovation - UNICRI, accessed July 29, 2025, https://unicri.org/sites/default/files/2024-02/02_Principles_Resp_AI_Innovation_Feb24.pdf

55. NASSCOM responsible AI framework - Citizen Digital Foundation, accessed July 29, 2025, https://citizendigitalfoundation.org/resources/responsible-ai/nasscom-responsible-ai-framework/
56. Nasscom Responsible AI - Artificial Intelligence - Scribd, accessed July 29, 2025, https://www.scribd.com/document/801616229/Nasscom-Responsible-AI
57. The ASCI Code - Advertising Standards Council Of India, accessed July 29, 2025, https://www.ascionline.in/the-asci-code/
58. How AI is shaping the future of advertising - ASCI, accessed July 29, 2025, https://www.ascionline.in/wp-content/uploads/2025/03/ADNext-Report-digital.pdf
59. India emerges as global testbed for AI ads amid consumer openness: ASCI report, accessed July 29, 2025, https://bestmediainfo.com/insights/india-emerges-as-global-testbed-for-ai-ads-amid-consumer-openness-asci-report-8871783
60. ASCI launches report on industry adoption, consumer privacy, responsible integration of AI, accessed July 29, 2025, https://www.exchange4media.com/advertising-news/asci-launches-report-on-industry-adoption-consumer-privacy-responsible-integration-of-ai-142010.html
61. Indian Advertising Industry Embraces AI: ASCI Report - MediaNews4U, accessed July 29, 2025, https://www.medianews4u.com/indian-advertising-industry-embraces-ai-asci-report/