



**JUNE 2024  
EDITION**

---

# MONTHLY NEWSLETTER

**LEXTECH: CENTRE FOR  
LAW, ENTREPRENEURSHIP  
AND INNOVATION**



दादये विद्वतो धर्म



# CONTENTS

1. Technology, Media  
and Telecommunications

2. FinTech

3. Artificial Intelligence  
& Data Privacy

4. Online Gaming

# TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS



## SECTION 1



# SELF-DECLARATION CERTIFICATES: MANDATORY FOR THE FOOD AND HEALTH SECTORS

## NEWS

The Supreme Court in the case of *Indian Medical Association vs. Union of India and Ors.* had passed an order mandating all advertisers to submit a self-declaration certificate before publishing any advertisement on television, radio, print, or digital media. In pursuance of this order, the Ministry of Information and Broadcasting released an advisory stating that the certificates are to be submitted only by health and food sector advertisements. Proof of this must be provided to the respective broadcaster or platform and no advertisements will be allowed without this certificate. The order was issued in response to concerns about misleading advertisements.

## LEGAL TALK

The Order requires the Self-Declaration to certify compliance with the Guidelines for Prevention of Misleading Advertisements and Endorsements, 2022, issued under the Consumer Protection Act. It requires advertisers to submit a brief description, full script, URL or PDF of the advertisement, proposed broadcast date, authorization letter, and CBFC certificate if applicable. Advertisers and advertising agencies issuing advertisements for products and services related to health and food sectors are now required to upload an annual certificate on the Broadcast Seva Portal for TV/Radio Advertisements and on the Press Council of India's Portal for print/internet advertisements.

The concerns in the Order stem primarily from health-related issues, as it enforces the fundamental right to health. The Bench has repeatedly emphasised consumer health as the central issue. However, the Self-Declaration requirement does not ensure that advertisements are free of misleading claims since the submitted documents are not verified by a regulator. Ensuring that non-compliant advertisements are taken down as this approach also aligns with the existing mechanism under Section 79 of the IT Act and Section 21 of the Consumer Protection Act, which addresses the takedown of misleading advertisements.

## THE WAY FORWARD

This order is crucial for addressing health concerns and protecting consumers from misleading advertisements. By requiring annual self-declaration certificates, it reduces the compliance burden for each advertisement while ensuring advertiser accountability. However, there is no review mechanism for these certificates, as the portal does not verify the documents. The initiative lacks depth due to the absence of a regulatory body to review the certificates. A possible solution is to establish a dedicated regulatory body tasked with reviewing and verifying the self-declaration certificates. This body could conduct random audits and inspections to ensure compliance. Implementing penalties for non-compliance and promoting transparency through public disclosure of verified certificates can further enhance the effectiveness of this initiative.





## ENFORCING THE TELECOMMUNICATIONS ACT, 2023

### NEWS

The Ministry of Communications via a notification has enforced several sections of the Telecommunications Act, 2023 (“the Act”) starting from 26th June, 2024. The sections on definitions, the right of way framework, powers to notify standards and provision on regulatory sandbox have now been notified.

### LEGAL TALK

Section 20 of the Telecom Act, 2023, encompasses extensive powers for the Union government, including the ability to temporarily possess, suspend, intercept, or detain any telecommunication service, intercept, detain, disclose, or suspend any message or class of messages, direct the suspension of any telecommunication service or class of telecommunication, and notify encryption and data processing standards, all justified on grounds of public emergency (including disaster management) or public safety. These provisions reinforce the colonial-era powers of the Union government, raising concerns about potential misuse, particularly if the Act's scope extends to internet services, potentially leading to draconian outcomes.

Furthermore, Section 22(3), in conjunction with Section 2(f), empowers the Union government to designate 'critical telecommunication infrastructure' and implement protective measures for such networks and services. These measures include the collection, analysis, and dissemination of traffic data, defined as "any data generated, transmitted, received, or stored in telecommunication networks, including data relating to the type, routing, duration, or time of a telecommunication." This special categorization and the accompanying government powers to establish standards and issue directives for these measures did not exist in the Telegraph Act of 1885.

The Act, not only retains several provisions that centralise power and control with the Executive but also introduces new ones. Notably, Section 20 closely mirrors Section 5 of the Indian Telegraph Act of 1885. The Act, intended to reform these colonial provisions, fails to introduce meaningful oversight, accountability mechanisms, or procedural safeguards in the country's surveillance and internet shutdown framework.

### THE WAY FORWARD

While the Act aims to enhance regulatory frameworks and infrastructure, it raises significant concerns regarding privacy, encryption, by providing the government extensive powers to decipher messages. The parallels with the colonial Indian Telegraph Act highlight the need for careful scrutiny and balanced implementation. Moving forward, it is imperative for the government to establish clear, transparent rules and ensure robust safeguards to protect citizens' rights. Ongoing dialogue with stakeholders and the incorporation of checks and balances will be crucial to address the ambiguities and potential overreach inherent in the Act. A plausible solution is to create an unbiased law commission that reviews the reforms required in the telecom industry. This shall do away with the colonial laws and bring in reforms as per industry requirements.

# FinTech



## SECTION 2



# RESERVE BANK OF INDIA ('RBI') ISSUES DRAFT FRAMEWORK FOR ELECTRONIC TRADING PLATFORMS ('ETPS')

## NEWS

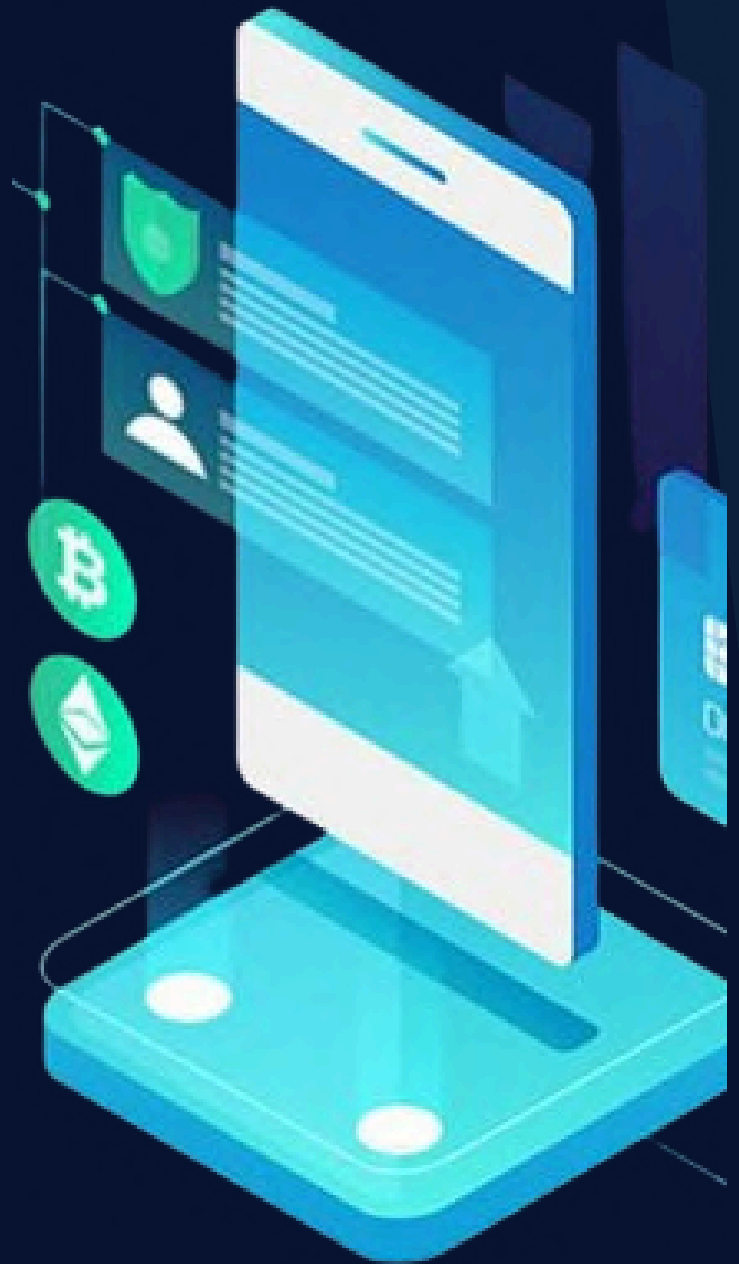
Recently, RBI released its draft Master Direction- RBI (Electronic Trading Platforms) Directions 2024. RBI has introduced the directions for authorization of ETPs with the aim to facilitate access to offshore ETPs offering permitted INR products.

## LEGAL TALK

ETPs refer to any electronic system other than a recognized stock exchange which enables the trading of eligible instruments such as securities, money market instruments, foreign exchange instruments, derivatives, or other instruments of like nature as may be specified by RBI. Some of the important directions are:

### (i) Eligibility Criteria for authorization of ETPs

An entity seeking authorisation as an ETP operator must conform to all applicable laws and regulations, including the FEMA, 1999. Additionally, the entity must maintain a minimum net worth of Rs.5 crore and must continue to maintain a minimum net worth as prescribed at all times. Shareholding by non-residents, if any, must conform to all applicable laws and regulations, including the FEMA, 1999. Further, the entity seeking authorisation as an ETP operator or its key managerial personnel must have at least three years of experience in operating trading infrastructure in financial markets. In addition to this, the entity must obtain and maintain robust technology infrastructure with a high degree of reliability, availability, scalability and security in respect of its systems, data and network, appropriate to support its operations and manage the associated risks.



The directions are designed to ensure compliance with legal frameworks, to uphold operational standards and ensure financial stability in the market. Mandating experience minimises operational risks while robust technology requirements aim to enhance system reliability.

#### (ii) Grant of authorization to operate ETP and cancellation of Authorization

According to the directions RBI can seek for any additional information from the applicants which it finds relevant. The decision of RBI to grant, reject or cancel the authorization to operate ETP will be final. RBI has the power to cancel the authorization issued to an entity if it is satisfied that the ETP operator:

- Violates any statutory provision or rules issued by the RBI.
- Violates any terms and conditions issued by the RBI while granting authorization
- The continuance of authorization is prejudicial to public interest or financial system of the country

These directions grant RBI extensive oversight over ETP operators. Granting RBI the authority to request additional information enhances transparency and allows thorough assessment of applicant suitability. These measures aim to deter misconduct and uphold investor confidence by holding ETP operators accountable.

In addition to these guidelines, ETP operators must also undertake due diligence at the time of onboarding of all the members, and must put in place a comprehensive risk management framework. Additionally, they must implement surveillance systems and controls to ensure fair and orderly trading to maintain market integrity and must maintain transparency.

## THE WAY FORWARD

These directions signify a proactive approach by the RBI to regulate ETPs, ensuring they contribute positively to the financial markets while minimising risks and safeguarding stakeholders. Compliance with these directives is expected to elevate operational standards across ETPs. Additionally, prior to issuing these directions, RBI had flagged certain unauthorised entities offering forex trading facilitates with promises of exorbitant returns. With these directions under which authorization of an ETP operator is mandatory, these malpractices will reduce fostering market integrity, transparency and investor confidence.

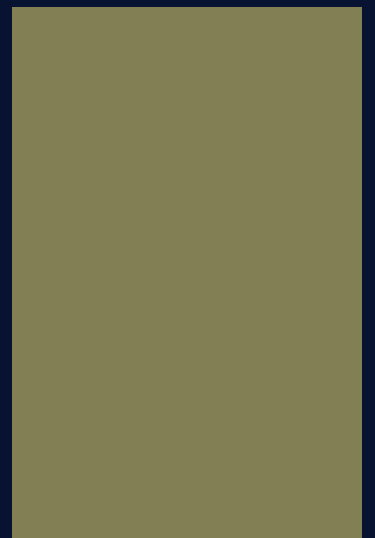




# ARTIFICIAL INTELLIGENCE & DATA PRIVACY



SECTION 3





# GOOGLE INTRODUCES A NEW SCAM CALL DETECTION FEATURE

## NEWS

Google's AI-powered assistant, Gemini Nano, is currently testing a new feature to detect scam calls using AI. With this feature, Android devices can alert users during a call if they detect conversation patterns typically linked to scams. However, the legality of this feature has been controversial.


## THE LEGAL TALK

Under Section 20(2) of the Telecommunications Act 2023 (“Act”), the government or an officer specially authorised by the government can take control of services or networks and authorise the interception or disclosure of messages for safety reasons. This provision poses a serious threat to the core feature of end-to-end encrypted platforms—the assurance that messages, in any format, can only be viewed by the sender and the intended recipient(s), including the service provider. Despite safeguards intended to prevent misuse of this rule, such as the requirement that, interception directions be provided for **specific** grounds and be subject to review by a committee under Rule 419A(2) of the Indian Telegraph Rules, 1951 (“**Telegraph Rules**”) (implemented through Section 61 of the Act), the fundamental principle of encryption is still at risk.

The Act, like its predecessors, does not define “interception.” In the absence of a clear definition, guidance can be taken from the IT Act, which grants similar interception powers for information processed on computer resources. Section 2(l) of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, issued under the IT Act, defines “intercept” as ‘the aural or other acquisition of the contents of any information through any means, including an interception device, so as to make some or all of the contents of the information available to a person other than the sender or recipient or intended recipient of that communication.’ If this definition is interpreted broadly, it could encompass Google's Gemini Nano and its new scam call detection feature. However, under Section 20(2) of the Act, *only* the government is empowered to perform such interception, even in the interest of safety. This suggests that Google's initiative to include this feature may be unlawful from the outset. Moreover, the safeguards established under the Telegraph Rules underscore the seriousness and sensitivity of such actions. The lack of these formal procedures in Google's implementation further complicates its legality. Without adherence to these stringent requirements, any interception—even if well-intentioned for scam prevention—risks being deemed unauthorised and illegal.

## THE WAY FORWARD

Assuming the feature passes initial legal scrutiny, several other potential harms must still be considered. Gemini Nano will have access to users' conversations and location data. Users would be sharing their personal data without specifically consenting to it. Google's actions could unleash a Pandora's box, prompting authoritarian governments and other agencies to acquire this technology for unlawful surveillance. Despite this potential for misuse, the significant benefits of the feature should not be overlooked. Cybercrime statistics are alarmingly high. The new scam call detection feature, which analyses voice and speech patterns locally, could greatly benefit users who are unaware of cyber fraud. Scams often follow similar patterns, and AI can effectively analyse these patterns to identify potential threats. If the analysis is conducted in real-time, it eliminates the need for Google to collect and store data on its servers, thus reducing privacy risks. Transparency is crucial for companies developing such technologies. They must prioritise informing users about the data being collected, how it will be processed, and whether it will be shared. Ensuring users are fully aware of these details can help mitigate concerns about privacy and misuse

 **Likely scam**

**Banks will never ask you to move  
your money to keep it safe.**

**Dismiss & continue**

**End call**



# Meta AI



## META HALTS ROLLOUT OF NEW AI TOOLS IN EUROPE

### NEWS

Meta has decided to pause plans to roll out AI tools in Europe following a recent direction from the Irish Data Protection Commission.

### LEGAL TALK

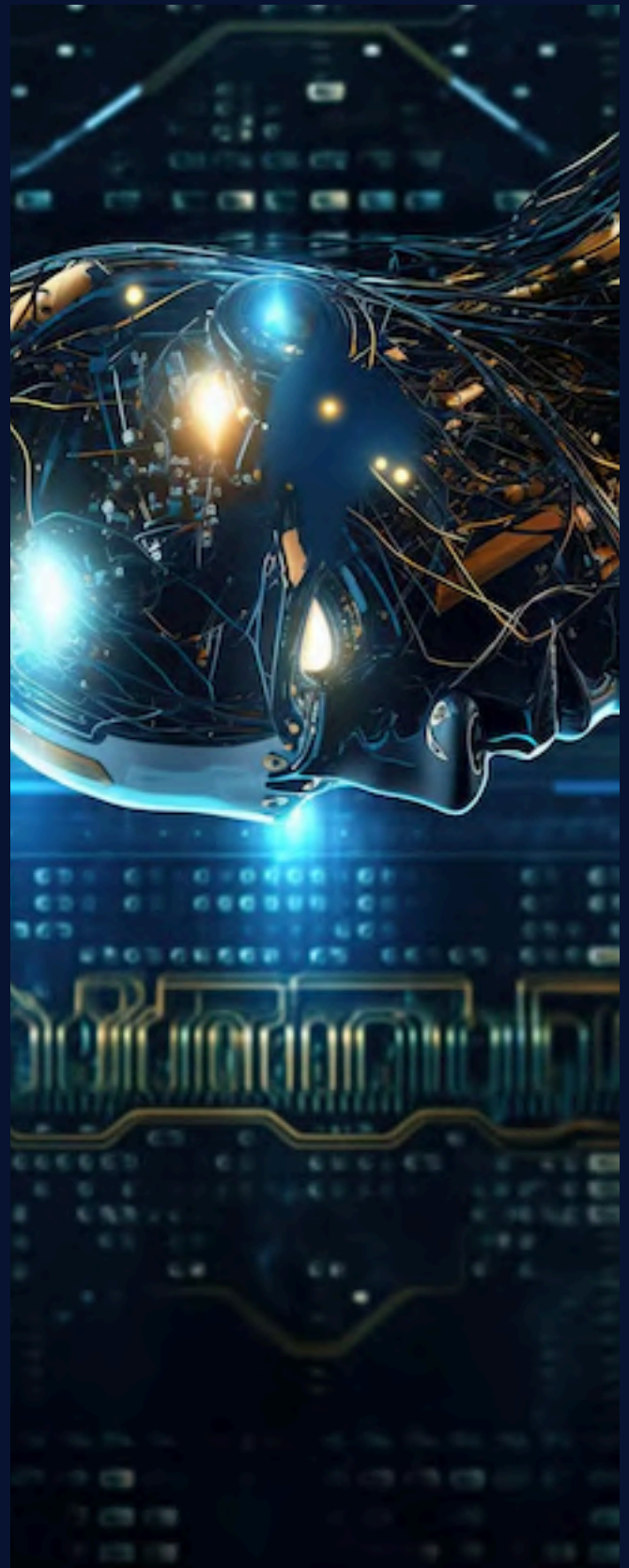
In its initial notification, Meta asserted that it was adopting a more transparent approach to training its large language models by following the example set by Google and OpenAI, utilising publicly available data. However, the scope of how this data will be used—both for current and future AI technologies—remains undefined. Despite their claims of transparency, Meta has failed to inform users about the specific technologies their data will support. The term "AI technology" is broad and lacks clear legal boundaries, which could lead to applications that infringe on individual rights. Under Articles 5(1) and 14 of the General Data Protection Regulation ("GDPR"), data must be processed for specified, explicit, and legitimate purposes. Additionally, data subjects have the right to be informed, meaning companies must maintain transparency and explicitly state why they are collecting data. Meta's current approach falls short of these requirements. While they have disclosed that the data will be used to train AI models, they have not provided sufficient details about the specific purposes these models will serve. Without clear information, users cannot fully understand or consent to how their data will be used, rendering the consent obtained as not truly informed.

Additionally, Meta's newly updated privacy policy has introduced further complications. The policy states that by agreeing to it, users permit the use of any personal data—whether on public or private accounts, stored on Meta systems or external sources, and including third-party data—for any purpose involving "AI technology." Furthermore, this data can be shared with any third party. The inclusion of data from third parties and sources outside Meta's direct ecosystem means that users have little to no control over what data is collected and how it is utilised, increasing the risk of data breaches and misuse.

To inform users about this new practice, Meta sent notifications to Europeans, accompanied by an objection form allowing individuals to opt out of having their data used for training AI models. If users submit the objection form before the training begins, their data will not be included in the current or future training rounds. However, this approach is inherently problematic because it treats the failure to object as implicit consent. The main issue here is the difference between opting in and opting out.

Opt-in consent means that a user's data cannot be used unless they explicitly agree to it. In contrast, opting out allows data to be used unless the user explicitly declines. This means that if users do not actively reject the data use, Meta can continue to use their data indefinitely. It places the responsibility on users to protect their privacy, rather than requiring Meta to obtain clear and explicit permission. Meta has also clarified that once users have failed to opt out, there is no option to do so later. The AI models will continue to be trained on this data, and due to the nature of generative AI, this data cannot be removed. This essentially deprives individuals of their right to erase their data, which is a direct violation of Article 17 of the GDPR.

The GDPR is more stringent and consumer-friendly compared to India's Digital Personal Data Protection Act ("DPDPA"). The DPDPA's scope is limited to personal data obtained through consent, excluding publicly available data. As a result, Meta can train its AI models on users' personal information available on its platform without needing explicit consent, and it does not provide Indian users with an opt-out option. In India, the option to opt out of third-party data usage hinges on Meta's approval of the user's request. This process involves navigating complicated forms and using very specific wording to gain Meta's approval, and even then, it is not guaranteed. Additionally, any data already used in training AI models is not erased. The rise of AI tools underscores a major loophole in the DPDPA—its exclusion of publicly available data from its purview. This loophole allows companies to use such data for any purpose they see fit, leading to significant privacy infringements.



## THE WAY FORWARD

It is well known that the world's largest companies are driving rapid advancements in AI technologies. The human race is eager to harness these innovations to their fullest potential, envisioning transformative changes across various sectors such as healthcare, education, and industry. Companies like Meta must find ways to innovate responsibly, ensuring that their AI technologies do not infringe on privacy rights. This means implementing robust safeguards, transparent data practices, and obtaining clear, informed consent from users.

# RECORD LABELS SUE AI MUSIC GENERATORS

## NEWS

Universal Music Group, Sony Music Entertainment, and Warner Music Group, aided by the Recording Industry Association of America, are suing Suno and Udio, two AI startups for copyright infringement.

## LEGAL TALK

Suno and Udio allow users to generate songs based on prompts, creating music in various genres with either user-provided or AI-generated lyrics. The labels accuse them of copyright infringement for training their AI models on music libraries, copying decades of popular recordings. The labels argue that AI can assist in creating innovative music with permission, but without regard for copyright, it harms artists, labels, and the industry, reducing music quality and cultural value. Generative AIs often scrape text from online sources, including copyrighted books and articles. Using this data without authorization can lead to copyright infringement claims because AI models rely on existing works to generate new content, potentially violating original creators' rights. Copyright law protects original works fixed in a tangible medium, but generative AI blurs these lines by creating derivative works that seem original.

Since there is no alternative method for training these models, to avoid liability, these companies must either prove their output as original or ensure their use of others' works falls under a legal exception. In the United States, the standard of originality, established in Feist Publications, Inc. v. Rural Telephone Service Co., requires a certain degree of creativity and novelty. For an AI-generated work to be considered original under US copyright law, it must exhibit more than trivial creativity. This means that the work should reflect some individual thought or inventiveness. However, AI models create new content by recombining existing data rather than by genuine creativity, making it difficult for their outputs to qualify as original works. This standard is relatively high, and AI-generated works typically do not meet it, pushing AI companies to seek protection under exceptions.

Copyright laws, including the US doctrine of fair use, permit certain uses of copyrighted works under specific conditions. In their defence, both companies have claimed fair use of the copyrighted music. Under Section 107 of the Copyright Act, fair use includes purposes like criticism, comment, teaching, scholarship, or research.



In Authors Guild v. Google, the court recognized Google's use of books for its Google Books service as transformative, meaning Google created a new and valuable product that did not compete with the existing market for books - giving fair use a new meaning. Generative AI companies argue similarly that their models transform training data into new forms rather than creating exact copies. However, claiming transformative use does not guarantee fair use. The justification must outweigh factors favouring the copyright owner. Unlike Google Books, generative AI products often compete directly with original works by labels and artists, weakening the fair use argument by impacting the market for the originals. India's standard for originality, established in Eastern Book Company v. D.B. Modak, is more flexible for AI-generated works than the US standard. In this case, Eastern Book Company ("EBC") added elements like paragraph numbers and headnotes to Supreme Court cases in their journal, SCC. When respondents copied these elements for their software, EBC sued for copyright infringement. The Indian Supreme Court found the American "modicum of creativity" too high. Instead, it adopted the Canadian test, which requires a work to result from the author's skill and judgement, beyond mere mechanical effort. The court ruled that EBC's added elements, requiring legal knowledge and judgement, were copyrightable. This decision means AI-generated works in India can meet the originality requirement if they show some skill and judgement, even if derived from existing knowledge. For Suno and Udio, this makes it easier to establish originality in India compared to the US. However, this lower threshold could undermine incentives for true creativity by allowing AI to repackage existing works without proper compensation to original creators.

## THE WAY FORWARD

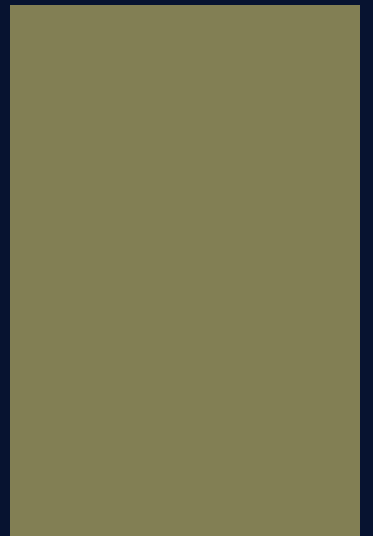
These lawsuits mark the most significant action against AI-generated music to date. The music community has embraced AI, collaborating with responsible developers to create sustainable AI tools that prioritise human creativity and put artists and songwriters in control. As AI-generated content proliferates, we must integrate it into our legal framework. We need to establish new standards of originality that consider AI's unique processes. Striking the right balance is crucial to ensure that both startups like Suno and Udio and artists benefit from these advancements.



# ONLINE GAMING



## SECTION 4





# TAMIL NADU ONLINE GAMING AUTHORITY (“TNOGA”) PROPOSES TO INTRODUCE TIME-BOUND RESTRICTIONS ON ONLINE GAMING

## NEWS

The TNOGA has proposed to enforce time-bound restrictions on online and real-money gaming. This comes after a significant increase in online gaming addiction. The proposed regulation is intended to mitigate the negative impact of excessive gaming on individuals and promote healthier gaming habits within the community.

## THE LEGAL TALK

Section 3 of the Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Act, 2022, establishes the TNOGA to ensure that online games are properly regulated and to advise the state government on issues relating to online gaming. Section 5 (2)(a) of the act empowers TNOGA to impose time-bound restrictions on online gaming.

The decision to impose time-bound restrictions is expected to have significant consequences, as gaming has evolved from merely a recreational activity into an economic one. Such provisions could impact the financial status of both gamers and online gaming platforms. While the move aims to combat gaming addiction, it can be easily circumvented by using multiple accounts or different devices. Moreover, the restriction might inadvertently lead to increased gaming frequency, as individuals may become more inclined to play daily, knowing there is a limited window of availability.

The proposed time-bound restrictions on online gaming in Tamil Nadu, while well-intended, present a multifaceted challenge that requires careful consideration. The effectiveness of such measures is indeed questionable and it would be wise to conduct a comprehensive analysis of the current gaming landscape and then implement any such regulations.

## THE WAY FORWARD

The TNGOA needs to carefully balance the potential benefits of reducing gaming addiction against the economic implications and practical challenges of enforcement. The authority can consider more nuanced approaches, such as age-based restrictions, educational initiatives about responsible gaming and collaborations with gaming companies to implement built-in tools for self-regulation. The outcomes in Tamil Nadu could serve as a valuable case study for other regions grappling with similar challenges in regulating the rapidly evolving world of online gaming.



# CONTRIBUTORS

## WRITERS

LAVANYA CHETWANI

ANJALI PANDE

TRISHNA AGRAWALLA

NAMAN OSTWAL

## EDITORS

NIKHIL JAVALI

HARSH MITTAL

SAGUN MODI

## DESIGNERS

SAMRIDHI BAJORIA

TRISHNA AGRAWALLA

**LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP  
AND INNOVATION**

**CONTACT US:**



INSTAGRAM



LINKEDIN



EMAIL