LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

DECEMBER 2025

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP, AND INNOVATION

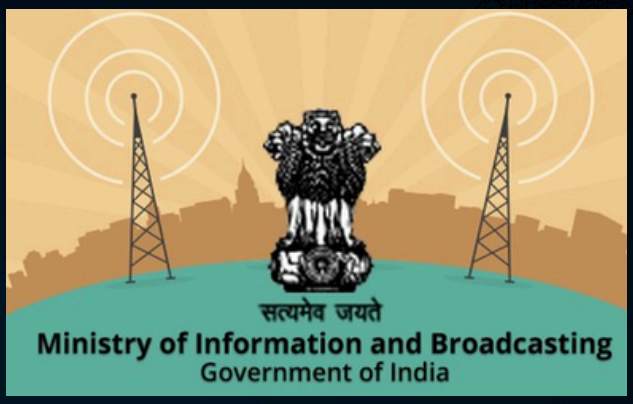
NATIONAL LAW UNIVERSITY ODISHA

CONTENTS

TECHNOLOGY, MEDIA, AND TELECOMMUNICATIONS

MIB PROPOSES AN EXPANDED DIGITAL MEDIA ETHICS CODE TO CURB ONLINE OBSCENITY

NEWS



The Ministry of Information and Broadcasting ("**MIB**") told the Supreme Court that it would **amend** The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**IT Rules, 2021**") to curb the sharing of "obscene content" online.

The Centre described this as a "**far-reaching revamp**" that would extend the code to social media users and digital news publishers. It also plans to define and ban "obscene digital content" online, citing Section 67 of the Information Technology Act, 2000.

ANALYSIS

The proposal was filed in the context of the recent Ranveer Allahabadia and CURE SMA Foundation of India cases on offensive online content. A March 2025 **order** had asked the government to frame guidelines on "morally offensive" programs in line with Article 19 limits. The MIB noted that the Bombay High Court had stayed their previous attempts to curb offensive speech in the form of Rule 9(1) and 9(3) of the IT Rules, 2021 as ultra vires, so these rules must be now "redrafted" to align with Article 19 protections.

Currently, the Code of Ethics is divided into two parts: the first for news, and the second for online curated content. The new plan proposes a four-part code. The first part would cover all digital content and will include an obscenity standard similar to the TV's Programme Code. Interestingly, it does not prohibit content promoting superstition or blind belief as found in the TV's Programme Code.

MIB PROPOSES AN EXPANDED DIGITAL MEDIA ETHICS CODE TO CURB ONLINE OBSCENITY

Continued...

The Code invokes Section 67, which criminalises online obscenity, and offers a definition based on existing law. Any content that is lascivious or appeals to prurient interest that tends to "deprave and corrupt" viewers would be deemed obscene. The MIB also noted that the famous Community Standard Test developed in the Aveek Sarkar v. State of West Bengal case should also be used to determine obscene content. Publishers would also have to rate content by age and lock or restrict adult material, much like the TV rating system.

The first part further continues to discuss a code to deal with AI-generated content and deepfakes. The second part largely retains the guidelines for online curated content but adds a section on accessibility.

The third and fourth part which shall deal with ser-generated content and news, are still under consideration by the MIB. Most digital publishers already follow self-regulation and have set up internal grievance bodies. However, civil society groups warn that any broad "programme code" for the internet must be carefully defined. Stakeholders are pushing for wide public consultation and precise wording, noting that vague censorship rules can have a chilling effect on legitimate speech.

UIDAI UPDATES AADHAAR AUTHENTICATION RULES

NEWS

TThe Unique Identification Authority of India (**"UIDAI**") notified the Aadhaar (Authentication and Offline Verification) Amendment Regulations, 2025 ("**Amendment**"). This Amendment aims to modernise offline Aadhar based verification processes while securing the privacy of users.

ANALYSIS

Currently, hotels and similar entities often request copies of customers' Aadhaar or take pictures of the same as proof of identity. This sensitive data is manually handled, without any transparency leading to a high possibility of misuse. To verify the credentials submitted, certain online entities would send requests to UDIAI servers which caused its overburdening.

These amendments introduce an Aadhaar Verifiable Credential ("**AVC**"), a digitally signed document generated by UDIAI against which identity checks will happen instead of the UDIAI servers like the DigiYatra process. This document will only contain information that the user consents to, like name, date of birth, photo, and last four digits of the Aadhaar number and will only be used as a method of authentication if the user consents to it.

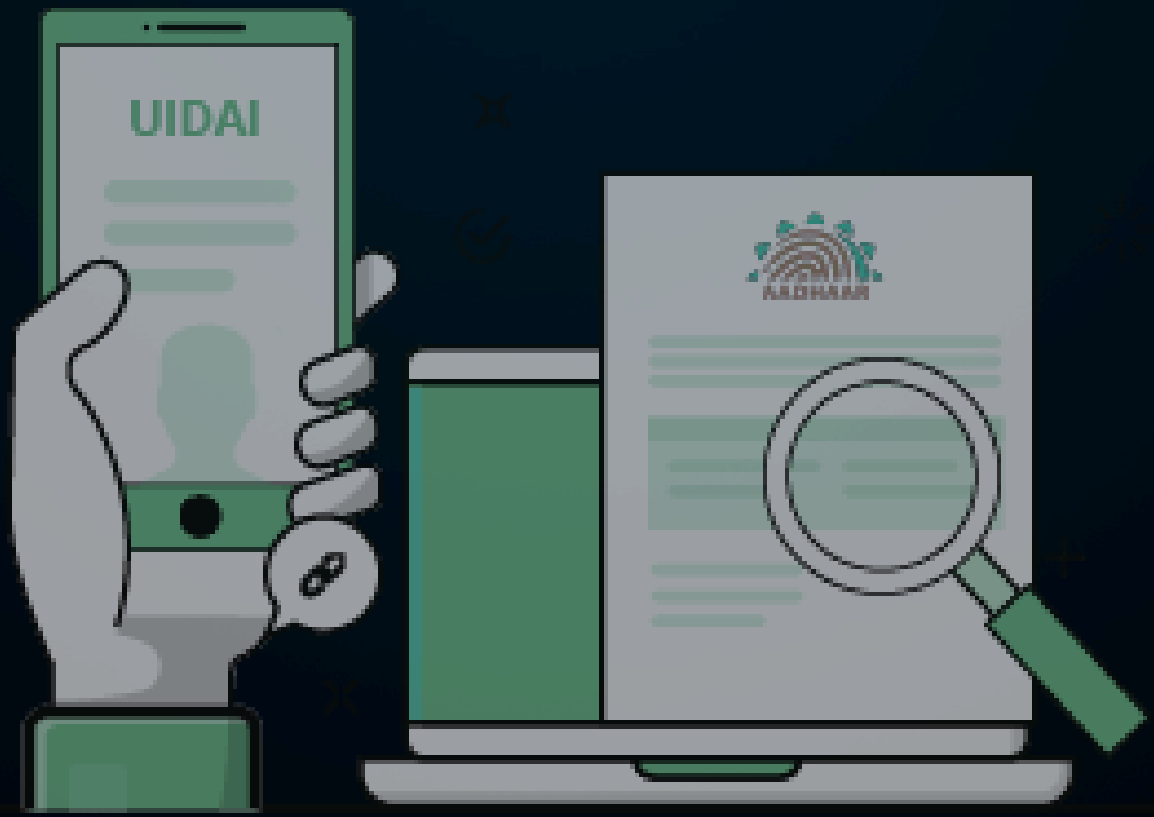
The amendment recognises an official Aadhaar application to be introduced soon, which the customers can install and use for Aadhaar services instead of existing apps. This app will be used to store AVC and enable sharing through QR codes. They also add offline face verification as a legal authentication method at par with other existing biometric authentications, which previously operated in a grey area.

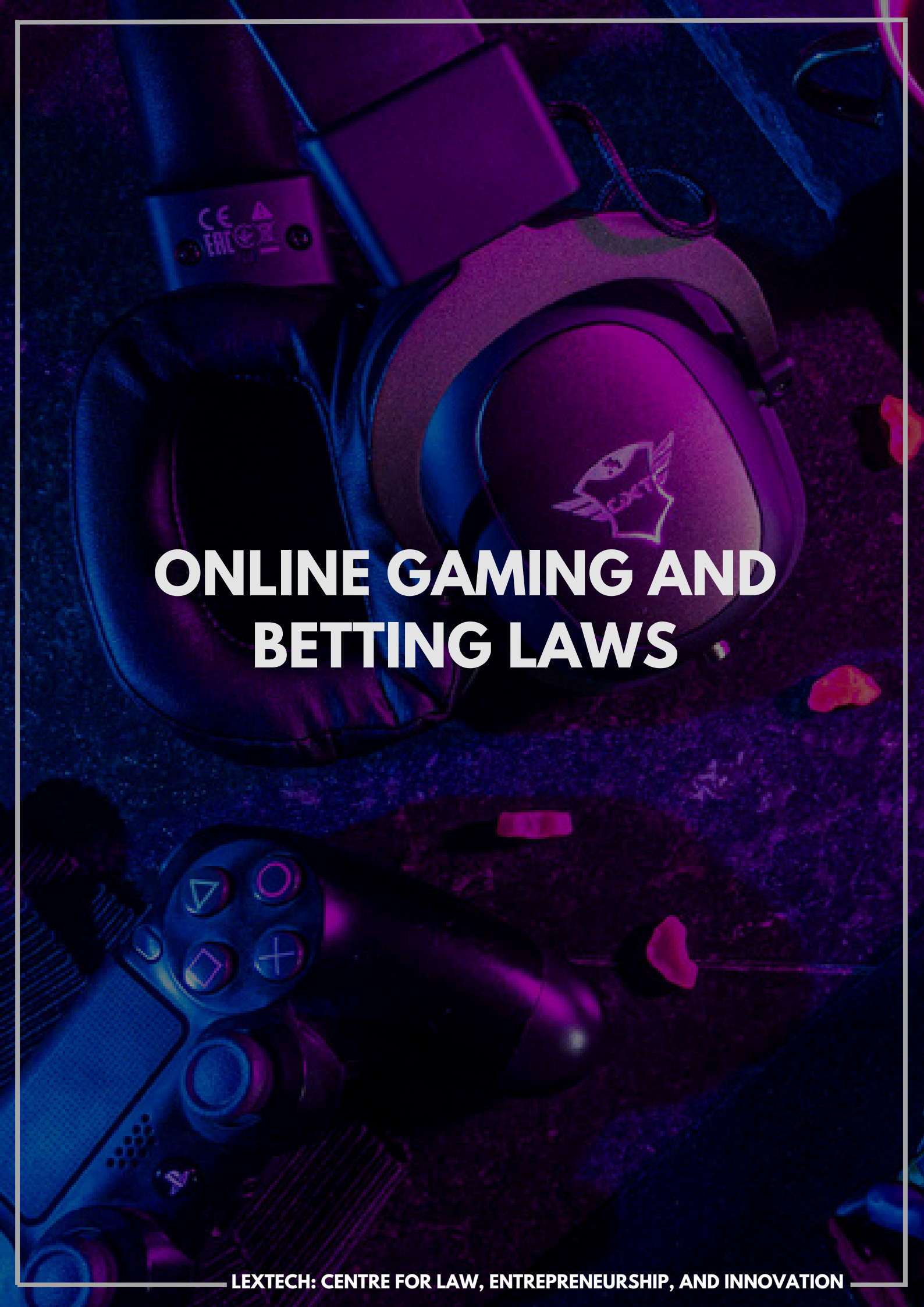
UIDAI UPDATES AADHAAR AUTHENTICATION RULES

Continued...

The amendment further requires any organisation using Aadhaar paperless offline e-KYC, or verifiable credentials, to register with UIDAI. These organisations will be termed as Offline Verification Seeking Entities ("**OVSEs**") under Regulation 13A. UIDAI may now seek more information, a fee, approve or reject OVSE applications with reasons within 15 days, with a 30-day window for reconsideration requests. The amendment also lets UIDAI penalise OVSEs for misuse, and mandates that any entity whose registration ends must stop using the Aadhaar name and logo, hence strengthening enforcement procedures.

The new process aligns with the Digital Personal Data Protection Act, 2023 by giving users control over what data is being shared, autonomy over the authentication process and mandating that the OVSE specify the purpose of authentication. Nevertheless, the increasing instances of Aadhaar being used as proof of identity, despite other safer alternatives could create hardships for users who do not wish to opt for this method.





ONLINE GAMING AND BETTING LAWS

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP, AND INNOVATION

RAJASTHAN HC DENIES BAIL IN ₹95 CRORE GAMING GST SCAM

NEWS

IIn a significant order, the Rajasthan High Court refused to grant bail to certain individuals accused of organising a massive ₹95 crore GST evasion scheme, which involved shell companies utilising online payment methods to process illicit gaming revenues. It has been alleged that this has led to the collection of almost ₹90 crore in commission and fees.

Further investigation revealed the presence of a foreign-based individual, suspected to be a resident of China or Hong Kong, which indicated a cross-border financial racket. The HC classified it as an act of white-collar crime with a significant negative impact on the national economy.

ANALYSIS

The High Court's decision in this case underscores its increasing scrutiny of intermediaries and strict adherence to the Central Goods and Services Act, 2017 ("**CGST Act**"). The court justified its decision of not granting bail by highlighting that the evasion amount far exceeded the threshold of ₹5 crore under Section 132(1)(i) of the CGST Act, making the offence both cognizable and non-bailable. Additionally, there was a possibility, beyond mere speculation, of the accused absconding to foreign jurisdictions or tampering with important financial records.

While analysing the *Vinnet Jain v Union of India* judgment, the court observed that although the established rule in GST matters is to grant bail, in the particular case, the magnitude and the link to foreign countries constitute an extraordinary situation and thus require rejection of bail.

Although the case has not been decided and the facts are not yet certain, it is evident that electronic communications and digital financial trails are used by investigative agencies in establishing foreign attachments and preventing bail of white-collar criminals. This case also reinforces the concerns raised by the government as to the likely risks associated with real money online games.

BUENOS AIRES PROVINCE MANDATES BIOMETRIC VERIFICATION FOR ONLINE GAMING

NEWS

The government of the Province of Buenos, in a significant move to combat underage gambling and identity theft, has announced mandatory **biometric identification** and facial recognition for all authorised online gaming and sports betting platforms. The government announced the new rule for all seven licensed platforms in the province and also provided a 60-day window to implement these identity verification systems.

Additionally, the Provincial Institute of Lotteries and Casinos is also finalising rules to control the gambling advertisements on social media and TV. It aims to ban advertisements that show betting as a form of personal success.

ANALYSIS

While the measures for mandatory biometric identification are specific to Buenos Aires, it highlights a growing global trend of using technology to enforce age restrictions and also ensure user accountability. One of the most common methods used by minors is "proxy betting", where they use the credentials or accounts of an adult family member, thereby bypassing the traditional age gates. To prevent this, every user will be required to show proof of life through their device's camera every time they log in.

The new mandate balances the privacy rights along with the State's duty to prevent underage betting. Similar to the Digital Personal Data Protection framework in India, the burden to verify the identity falls on the platform operators. The new mandate also suggests that previous methods of self-declaration might be obsolete, with biometric verification likely being used by most digital applications.

An interesting and indirect consequence of the new mandate, is the de-platforming of users on older hardware. Only users with camera-equipped devices will be able to access and use the online betting platforms. A potential follow-up of the mandate would be an integration of government authorised identity tokens for the verification of age, which would ensure that the biometric data matches a verified legal identity.


st point
2640
2530
1650
1620
1510
1520
1520
1450
1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3
VII
VIII
IX
X
XI
XII

FINTECH

GOOGLE PAY ROLLS OUT ITS FIRST DIGITAL CREDIT CARD IN INDIA

NEWS

Google Pay has introduced the first digital credit card in India in association with Axis bank using RuPay.
The card is issued digitally through Google Pay's app, and provides the use of UPI-linked credit payments, including QR-based transactions.

ANALYSIS

Google rush into the credit card arena marks a fundamental change to India's model of digital finance from transaction infrastructure to participating financial services. By having credit cards embedded into the Google Pay interface, Google is putting itself at the centre of the payment system, claiming neutrality, but also the gatekeeper of access to consumer credit, even though formally itself is not part of the regulated lender category.

The partnership model is key. Axis Bank is carrying risk of balance sheet and regulatory compliance and Google controls user interface and data visibility, behavioural nudges and transaction routing. As a result of its asymmetry, the big-tech platforms get away with extracting value without any corresponding regulatory obligations, a type of model that is increasingly coming under scrutiny by financial regulators around the globe.

More importantly, this move affects the consumption of credit. When credit is seamlessly built into UPI payments, the risks of credit will become a default of behaviour rather than a conscious financial choice, which will lead to concerns about informed consent, over-borrowing and algorithmic steering - especially for first-time borrowers.

On the level of markets, the product launch would accelerate the concentration of the platform. Fintech competition may appear to be alive and well, but distribution advantages enjoyed by the big-tech players could easily stunt the presence of smaller lenders and apps, forcing the ecosystem into a platform dependency rather than financial inclusion.

NPCI SUBSIDIARY NBBL ROLLS OUT BANKING CONNECT AS A NET-BANKING SOLUTION

NEWS

The National Payments Corporation of India's ("**NPCI**") subsidiary NPCI Bharat BillPay Limited ("**NBBL**") launched Banking Connect, a digital payments platform which aims to simplify internet and mobile banking transactions. The platform brings to life RBI's Payments Vision 2025 of enabling "E-payments for Everyone, Everywhere, Everytime."

Bharat Connect is proposed as an interoperable net banking solution, increasing banking oversight by bringing net banking based payments into a single platform regulated through NPCI and aligned with Reserve Bank of India ("**RBI**") frameworks. It will provide services to customers across banks and payment aggregators.

ANALYSIS

Current net banking processes currently involve multiple integrations with banks, payment gateways and merchants operating on different systems. Additionally, it requires different customer credentials and does not rely on a uniform standard for settlement flows. As a result, it makes the payment mechanisms slower, less reliable, reducing the overall efficiency. NBBL intends to simplify this.

The immediate changes for customers will be the availability of three payment options: using their bank's mobile application, scanning a QR code, or continuing with the existing net banking website if their bank has not yet migrated to Banking Connect. The service also provides for improved grievance redressal, improving the consumer experience.

Through Banking connect, users will be directed to their own bank apps. This platform will support biometric authentication, remove transaction caps and introduce standardised Application Programming Interfaces ("**APIs**"). API is a secure digital connector that allows different banks, payment systems, and applications to communicate with each other in an uniform manner.

NPCI SUBSIDIARY NBBL ROLLS OUT BANKING CONNECT AS A NET-BANKING SOLUTION

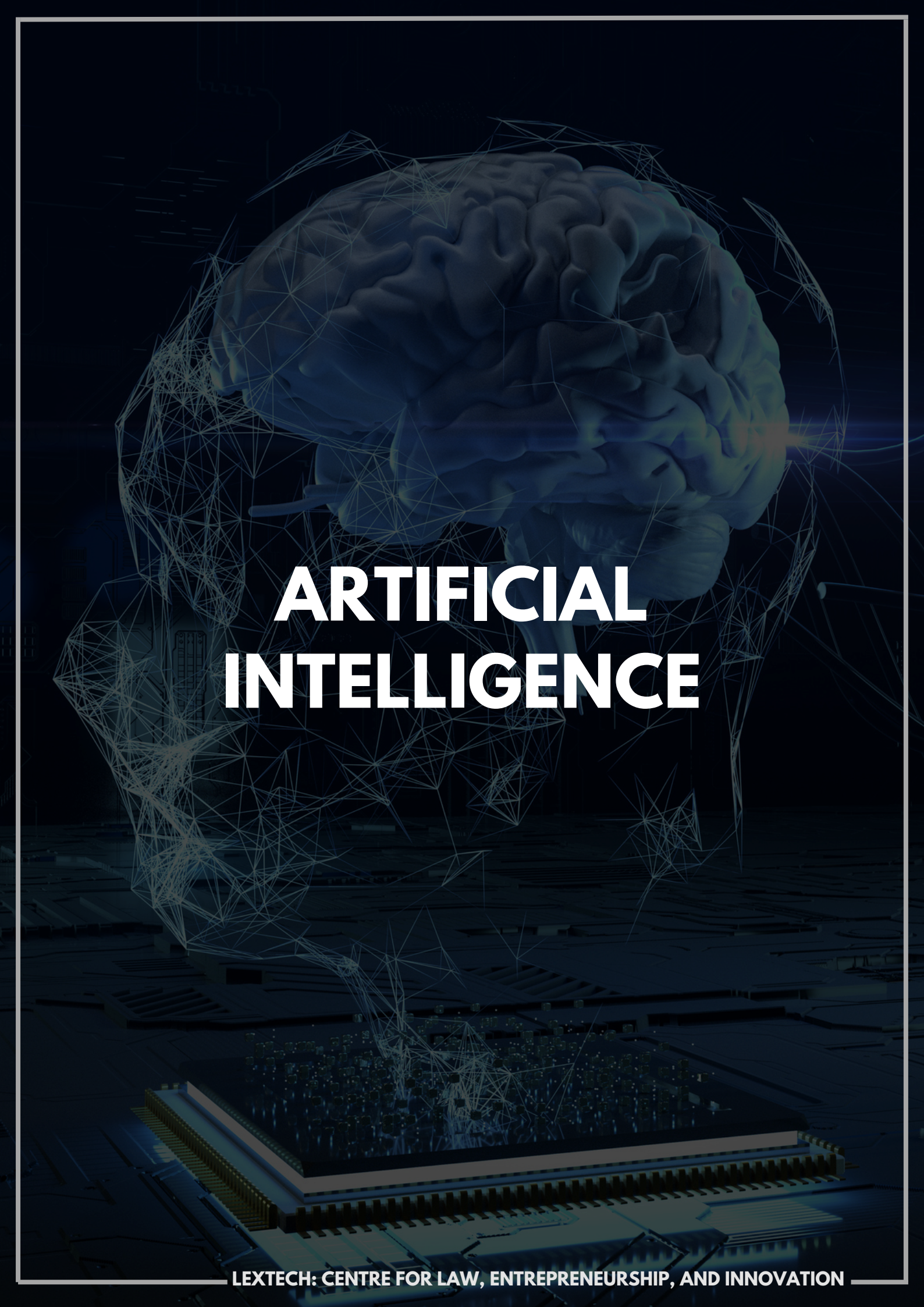
Continued...

The launch of Banking Connect signals various implications. Firstly, the delay in reporting the data of net banking transactions to RBI by the banks will be minimised. This will enable the RBI meaningfully oversee compliance and ensure transparency, efficiency, and systemic stability.

The faster and standardised data flow will enable the regulator to monitor the risks in real-time, especially in areas of financial abuse, personal cryptocurrencies, and regulated practices such as online gaming sectors. Secondly, it will become easier for banks to complete verification requirements like KYCs as the fraud-monitoring service of the platform will help monitoring suspicious activities.

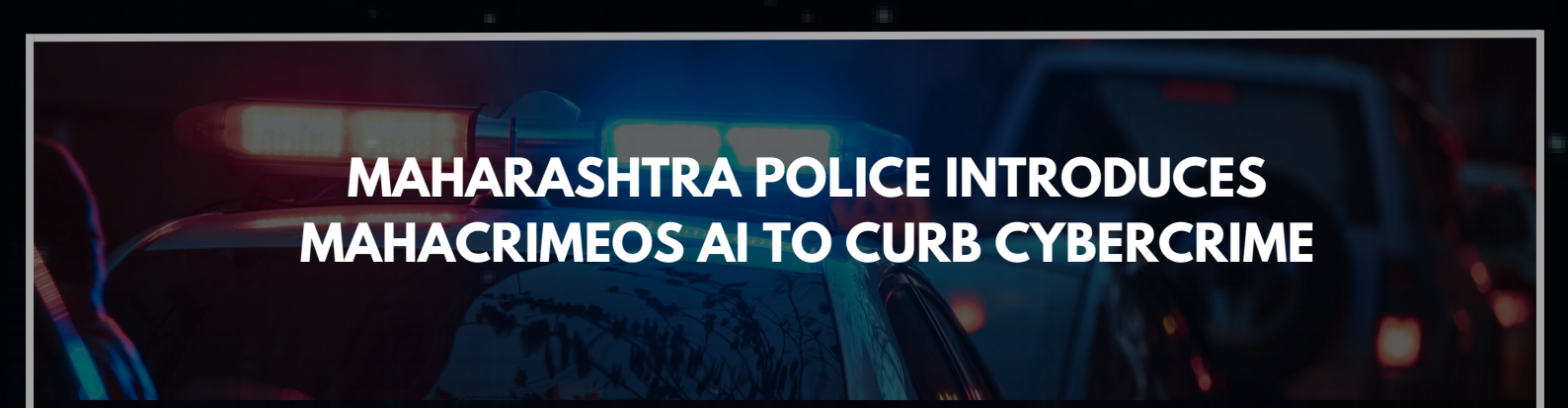
Third, non-discriminatory access and interoperability promotes healthy competition and standardised APIs among banks and payment aggregators. Lastly, more open disclosure of complaints, timeframes of chargeback, and other accountability measures will enhance consumer protection and accountability. These are also mandatory requirements under the digital payment directions of RBI and furthering these initiatives will ensure a secure and controlled payment environment.

Currently, around 80 million customers use net banking, with monthly transaction value exceeding Rs. 6 lakh crore. With Bharat Connect, NBBL aims to make digital bill-related transactions more safe and accessible, enabling more people to use digital payments through net banking.



ARTIFICIAL INTELLIGENCE

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP, AND INNOVATION



MAHARASHTRA POLICE INTRODUCES MAHACRIMEOS AI TO CURB CYBERCRIME

News

The Maharashtra Government has decided to expand MahaCrimeOS AI, a pilot project in Nagpur, to all 1,100 police stations across the state. The AI tool assists police in analysing cybercrime complaints, drafting first information reports ("**FIRs**") and legal notices, and suggesting investigation pathways.

Analysis

MahaCrimeOS AI was started against the backdrop of the rise in cybercrime complaints in recent years. Apart from automating paperwork it influences investigative decision-making by analysing material and recommending next steps. It also drafts requests to banks, telecom companies, and online platforms which includes requests for account freezes, call detail records and account takedowns.

While it has the potential to be helpful, AI led policing raises very pressing concerns which operate in a regulatory grey area. Firstly, it remains unclear how such an AI would operate under the Indian evidence law framework. Automation of paperwork, or reliance on AI-generated analyses, and AI-driven strategy challenges the principles of due process and fair trial.

Secondly, there is little information available pertaining to the datasets that MahaCrimeOS AI relies on, how long it retains information, or whether independent audits have examined the data for bias or gaps. Moreover, state agencies sharing large volumes of personal and sensitive information with private companies to operate such a system raises flaring privacy concerns.

Thirdly, as with most other AI models, issues of hallucination, misclassification, and bias are relevant concerns, especially when dealing with matters as sensitive as crime detection and resolution. In cybercrime investigations, these can lead to errors in interpreting messages which can misdirect law enforcement or delay actions.

MAHARASHTRA POLICE INTRODUCES MAHACRIMEOS AI TO CURB CYBERCRIME

Continued.....

MahaCrimeOS AI represents a big shift in criminal investigations especially in cybercrime investigations. While it may offer many benefits in terms of detection and efficiency, its integration into core investigative and procedural functions raises serious concerns relating to evidentiary reliability, privacy and accountability. As these AI tools increasingly shape law-enforcement outcomes, it remains to be seen if these serve as a net-positive for law enforcement.

DONALD TRUMP SIGNED AN EXECUTIVE ORDER PREVENTING STATES FROM REGULATING AI

NEWS

The White House recently released the executive order titled "*Ensuring a National Policy Framework for Artificial Intelligence*" ("**the executive order**"), aimed at preventing states from making regulations for AI. It sets out the US's AI policy as one of sustaining the country's global AI dominance through "a minimally burdensome national policy framework for AI" and takes several steps to implement the same.

ANALYSIS

At the federal level, while the US has released certain policy documents, such as the AI Action Plan, there has been no concrete law passed to regulate AI. In its absence, numerous states like California and Colorado took the lead in making AI regulations. This executive order highlights that the states creating "burdensome" regulations could hinder AI companies' innovation prospects. Further, since a national standard on AI regulation does not exist, regulation by individual states could lead to a patchwork of multiple frameworks. Thus, this order's goal is to ensure that onerous regulations are kept in check until a national framework is created.

The order directs the Attorney General to create an AI Litigation Task Force to challenge the State AI regulations inconsistent with its policy. The grounds may include unconstitutional regulation of interstate commerce, preemption by existing Federal regulations, and so on. Furthermore, it also directs the Secretary of Commerce to publish an evaluation of all the existing state AI laws, identifying laws that are against the policy laid down and the ones to be referred to the Task Force. It states that the evaluation should identify laws that require AI models to alter their outputs, or that may compel AI developers or deployers to disclose information in a manner that would violate the US Constitution's First Amendment.

DONALD TRUMP SIGNED AN EXECUTIVE ORDER PREVENTING STATES FROM REGULATING AI

Continued.....

The order directs the Attorney General to create an AI Litigation Task Force to challenge the State AI regulations inconsistent with its policy. The grounds may include unconstitutional regulation of interstate commerce, preemption by existing Federal regulations, and so on. Furthermore, it also directs the Secretary of Commerce to publish an evaluation of all the existing state AI laws, identifying laws that are against the policy laid down and the ones to be referred to the Task Force. It states that the evaluation should identify laws that require AI models to alter their outputs, or that may compel AI developers or deployers to disclose information in a manner that would violate the US Constitution's First Amendment.

The order also proposes certain restrictions on funding for states conflicting with the said policy. Moreover, it directs the Special Advisor for AI and Crypto and the Assistant to the President for Science and Technology to jointly prepare a uniform federal policy framework that pre-empts the State AI laws in conflict with the order's policy.

This executive order has received mixed reactions: while some people consider that it will foster innovation, critics claim that it will block all meaningful regulation towards AI. Since AI regulation is still in a nascent stage globally, including in the US, any attempts to hinder meaningful regulation could further slow down the process.


DATA
PRIVACY

NCLAT REINFORCES USER CONSENT IN WHATSAPP DATA PRACTICES

NEWS

TThe recent order of National Company Law Appellate Tribunal ("**NCLAT**") has clarified that WhatsApp will be required to **seek consent** from the users before collecting data that is exchanged for advertising and non-advertising purposes. The Hon'bl tribunal addressed the issue of data sharing pending since 2021 by providing users optionality at any stage to opt in or out of data sharing.

ANALYSIS

The order of NCLAT emerged from an application submitted by the Competition Commission of India ("**CCI**") regarding the rights of users in open ended data sharing. This order marks a clear shift towards a user-consent driven era, in line with the DPDP framework. By bringing a transnational digital giant like WhatsApp to the consent regime, NCLAT has compelled them to comply with the data protection requirements of purpose, user control and proportionality.The decision of NCLAT compels WhatsApp to switch from "take it or leave it" terms to a privacy first approach. It requires data collection to be strictly limited to specific goals with complete user liberty and appropriate usage. This update effectively aligns the tech giant's operations with the core principles of the core fundamentals of the DPDP architecture by guaranteeing that cross platform data sharing is no longer a prerequisite for service.

Further, the order has enforced the 'opt-in' and 'opt-out' rights of users with respect to data sharing at any stage to secure their rights. The order acknowledges the exploitation of data as a competition issue, particularly when dominant platforms use data to prevent entry in complementary markets.Problem of competition is created when dominant platforms use huge amounts of data to create obstacles to entry.Tech giants such as Meta exclude competitors in market by using this data to unfairly control related markets which are related to industries like digital payments or advertising.

NCLAT REINFORCES USER CONSENT IN WHATSAPP DATA PRACTICES

Continued.....

This order paves the way for digital platforms to redesign data governance structures to ensure purpose specific consent. It will serve as a strong benchmark that consent cannot be twisted to gain unfair advantage by accessing core services. It will help interpreting consent and strengthen user control, pushing India toward a more rights oriented and accountable data ecosystem.By enforcing rigid "take-it-or-leave-it" agreements that force customers to give data in order to access essential core services, dominant platforms obtain an unfair advantage. Unmatched targeting advantages and overwhelming entry barriers are created in complementary areas by this obligatory data integration

EU RENEWS ITS ADEQUACY DECISIONS FOR THE FLOW OF PERSONAL DATA WITH THE UK

NEWS

Recently, the European Commission renewed its adequacy decisions for the free flow of data with the United Kingdom (**"UK"**), thereby enabling the continued flow of personal data between the latter and the European Economic Area. The decisions, originally adopted in 2021, stem from the European Commission's power under the GDPR to allow the flow of personal data between the EU and a third country/international organisation without hurdles. Having been due to expire in December 2025, they have now been extended for another 6 years till 2031.

ANALYSIS

According to Article 45 of the EU's General Data Protection Regulation (**"GDPR"**), the European Commission, after deciding that a third country ensures adequate levels of data protection, may allow for a free flow of personal data with that country. In the absence of such a decision, the transfer of data requires multiple appropriate safeguards and a condition that individuals will have enforceable rights and legal remedies.

In the UK's case, after parting with the European Union in 2020, its data protection regime drew heavily from the GDPR. Consequently, both regimes essentially contain similar standards of data protection, thereby enabling the Commission to consider it adequate and allow for the data sharing decision under Article 45.

In June 2025, the UK introduced the Data (Use and Access) Act to relax regulations surrounding data sharing and ease compliance. To this, certain civil society organisations expressed concerns about renewing the data adequacy decision after its introduction. However, the Commission, in its draft adequacy decision published in July 2025, made clear that the UK's levels of data protection remain adequate even after the new Act's introduction.

This decision is symbolic of the continued regulatory co-operation between the EU and the UK. By ensuring the free flow of data between the EU and the UK, this decision helps in reducing the costs and compliance burdens. This will likely help in fostering better innovation and competitiveness for both countries in the long run.

CONTRIBUTORS

WRITERS

ARANYA SEN
ARNAV RAJ
DIYA JAIN
ISHANI GARG
SANIDHYA GURUDEV
SANSKRITI VERMA
SUBHASIS SAHOO
SHRUTI SRIRAM

EDITOR-IN-CHIEF

PRATYUSH SINGH

DESIGNERS

ISHANI GARG
MAITHILI DUBEY
SANSKRITI VERMA

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION