LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

OCTOBER-NOVEMBER 2025

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP, AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

CONTENTS

TECHNOLOGY, MEDIA, AND TELECOMMUNICATIONS

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP, AND INNOVATION

DOT ISSUES DRAFT TELECOMMUNICATIONS (USER IDENTIFICATION) RULES, 2025

NEWS

The Department of Telecommunications (**"DoT"**) has published the Draft Telecommunications (User Identification) Rules, 2025 (**"Rules"**). The Rules propose a mandatory regime of user-verification before obtaining telecom services. The Rules also seek to collect this user data and maintain a Biometric Identity Verification System database (**"BIVS"**).

ANALYSIS

As per the Telecommunications Act, 2023 (**"the Act"**), any entity that provides any telecom service or possesses radio equipment must seek government authorisation to function. This creates ambiguity regarding the application of these rules to online services like WhatsApp, Telegram and OTT platforms which will be clarified only through a notification specifying the telecom services to which the Rules will be applicable. A user of notified telecom services holding an Aadhaar number must be authenticated and identified through Electronic Know Your Customer (**"e-KYC"**) processes, or Digital Know Your Customer (**"D-KYC"**) process when an Aadhaar number is not present. Likewise, when a business utilises a notified telecom service, the representative of the business must undergo biometric-based verification along with all end-users of such service.

Businesses may be exempted from this requirement if they send such a request to the government and the government accepts it. Such identification process sought to be achieved by these Rules has already been in practice pursuant to multiple past DoT circulars. As per Rule 4(2), users with Aadhar numbers will mandatorily have to complete the authentication process. The Rules thus assume that all Aadhaar number holders would want their Aadhaar details to be linked with the telecommunication service. Under Rules 5 and 7, service providers must also obtain users' consent before collecting and storing such biometric data. However, the rules are silent on what happens if a user refuses such consent, with the requirement to authenticate oneself being mandatory under the same framework.

DOT ISSUES DRAFT TELECOMMUNICATIONS (USER IDENTIFICATION) RULES, 2025

continued....

The BIVS to be made by telecom service providers under these Rules must be encrypted, access-controlled, and tamper-proof, with regular government audits to ensure compliance. The database will track users' telecom connections across all service providers by generating unique user-IDs. It essentially creates a parallel to Aadhaar Act's Central Identities Data Repository, but lacks provisions providing for "protection of information" as seen in chapters VI and VII of the Aadhaar Act.

The Rules thus ambitiously push toward a centralised, biometric-backed telecom ID system, but leave key questions like scope of the Rules and privacy concerns unresolved.

TRAI RELEASES RECOMMENDATIONS ON DIGITAL RADIO POLICY

NEWS

The Telecom Regulatory Authority of India (**"TRAI"**) released the Recommendations on Formulating a Digital Radio Broadcast Policy for Private Broadcasters (**"Recommendations"**). The recommendations outline the new framework and also delves into operational details, licensing guidelines, and the reserve prices for the spectrum auction. It seeks to launch digital radio services in 13 Indian cities.

ANALYSIS

The proposed framework elaborates on Simulcast services in which new private broadcasters are required to maintain one analogue and three other digital channels, while existing broadcasters can voluntarily migrate to this mode. According to the recommendations, once the licence is given it is valid for a period of 15 years.

The Recommendation provides that 4% of the Adjusted Gross Revenue will be collected as an annual fee by the government. With respect to the existing broadcasters, TRAI has provided that they can migrate to digital radio by paying the difference between the auction price and the Non-Refundable One-Time Entry Fee. Annual instalments over 15-20 years have also been introduced to ease the financial burden on service providers.

A major change is the removal of mandatory co-location of transmission infrastructure between operators. Earlier, operators had to co-locate transmission facilities in all the cities with government infrastructure. However, the recommendations suggest removal of such a mandatory requirement and envision a framework that would enable infrastructure sharing on a voluntary basis for operators. As stated in the recommendations, there would be a gradual phase-out of the Frequency Modulation (**"FM"**) radio in the coming years. Keeping this in mind, digital radio receivers must be manufactured and distributed across the consumer base, which includes mobile phones, car infotainment systems, and other devices.

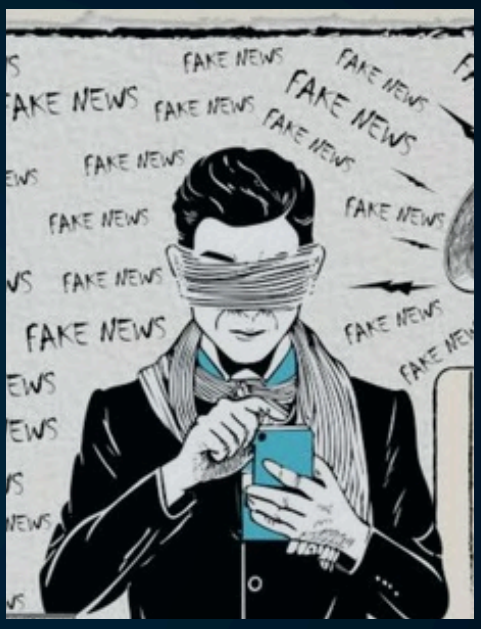
PARLIAMENTARY PANEL RELEASES REPORT ON REGULATION AND CURBING OF FAKE NEWS

NEWS

The Parliamentary Standing Committee on Communications and Information Technology has released its 22nd Report titled "Review of Mechanism to Curb Fake News". The report has provided a framework to curb misinformation across print, television and digital media platforms. Further the report also evaluates the effectiveness of existing laws and coordination between ministries.

ANALYSIS

The committee's recommendations include the topic of granting the Press Information Bureau's Fact Check Unit (**"PIB FCU"**) statutory backing. The move is proposed to provide the government-run body with greater credibility and a statutory framework to act against misinformation, especially against government schemes and policies. The recommendation also highlights the need to frame a legal definition of "fake news" and permissible reforms to curb the same.



However, in defining "fake news" one challenge is to achieve a definition which punishes misinformation while protecting satire, opinion and genuine errors. It will also be important to ensure that the FCU does not become the sole arbiter of regulating information. Independent journalists, media houses and their internal fact-checking procedures, must retain the freedom to analyse information.

While the intention to combat misinformation is novel, the recommendations raise many concerns. A singular body, without further statutory checks, deciding whether some news is true or not, raises glaring questions of press freedom and abuse of power by the government. Critics fear that a powerful, statutorily backed FCU could be misused to label criticism, dissent or unfavourable reporting as "fake news".

MEITY ISSUES NEW SOP FOR REMOVAL AND PREVENTION OF NCII

NEWS

The Ministry of Electronics and Information Technology (**"MeitY"**) issued a Standard Operating Procedure (**"SOP"**) to enhance the mechanism for the removal and prevention of Non-Consensual Intimate Imagery (**"NCII"**) across online platforms. The SOP released complies with the Madras High Court's directive to the Ministry in ***X v. Union of India*** to provide a "prototype as to what a victim girl must do when faced with situations of dissemination of NCII content".

ANALYSIS

For the first time, we now have a uniform, victim-first mechanism which operationalises Rule 3(2)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**"Rules"**). The rule mandates measures by intermediaries to remove such content within twenty-four hours. The SOP has set up multiple reporting channels for the victims that go beyond the intermediaries and law enforcement agencies to also include the National Cybercrime Reporting Portal (**"NCRP"**) and One Stop Centres (**"OSCs"**). If the victim is dissatisfied with an intermediary's response, they can further appeal to the Grievance Appellate Committee. In addition, the central aggregation point for secure NCII hash bank will be the Indian Cybercrime Coordination Centre under the Ministry of Home Affairs. The DoT will Coordinate with Internet Service Providers to block flagged URLs and MeitY will monitor compliance and coordinate with intermediaries and other government stakeholders. The SOP thus establishes a multi agency setup. The SOP essentially consolidates existing obligations instead of creating a new legal regime. It does not amend Section 79 of the IT Act or dilute the safe-harbour protection that intermediaries enjoy. Intermediaries still cannot be held liable for third-party content as long as they comply with this raised standard of due-diligence requirements under the IT Rules.

Thus the focus must be on increasing awareness of these remedies available to victims on timely managing the dissemination of NCII. The ministry has also described these procedures as an "evolving document" which may be updated over time.

NEW SAFEGUARDS FOR TRANSPARENCY IN GOVERNMENT TAKEDOWN ORDERS UNDER THE AMENDED IT RULES, 2025

NEWS

The Ministry of Electronics and Information Technology recently notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025 (**"Amended Rules"**) to bring greater transparency and accountability to governmental processes in issuing takedown orders. These amendments specifically replace the original clause (d) under Rule 3(1) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**"2021 Rules"**).

ANALYSIS

The original 2021 Rule required intermediaries (such as social media platforms) to remove unlawful information within 36 hours of receiving "actual knowledge" through a court order or "any notification" from the "Appropriate Government, or its agency".

The amendment firstly defines which officers can issue takedown orders stating that intimations to intermediaries can now only come from senior officers not below the rank of Joint Secretary, or equivalent. For police authorities, the officer must be not below the rank of Deputy Inspector General. This replaces the previous wide range of officers that were empowered under this rule's vague text.

Secondly, it replaces "any notification" with "reasoned intimation". Each order must clearly specify the legal basis and statutory provision invoked, the nature of the unlawful act, and the precise URL, identifier, or electronic location of the content to be removed.

Thirdly, a periodic review mechanism has been introduced. All intimations issued under the rule will undergo a monthly review by a Secretary-level officer of the appropriate government to ensure the actions remain necessary, proportionate, and consistent with the law.

The amended rules essentially bring Rule 3(1)(d) closer to the framework of Section 69A of the Information Technology Act, 2000 (**"IT Act"**) and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. Section 69A also has the same senior level authorisation and reasoned intimation requirement.

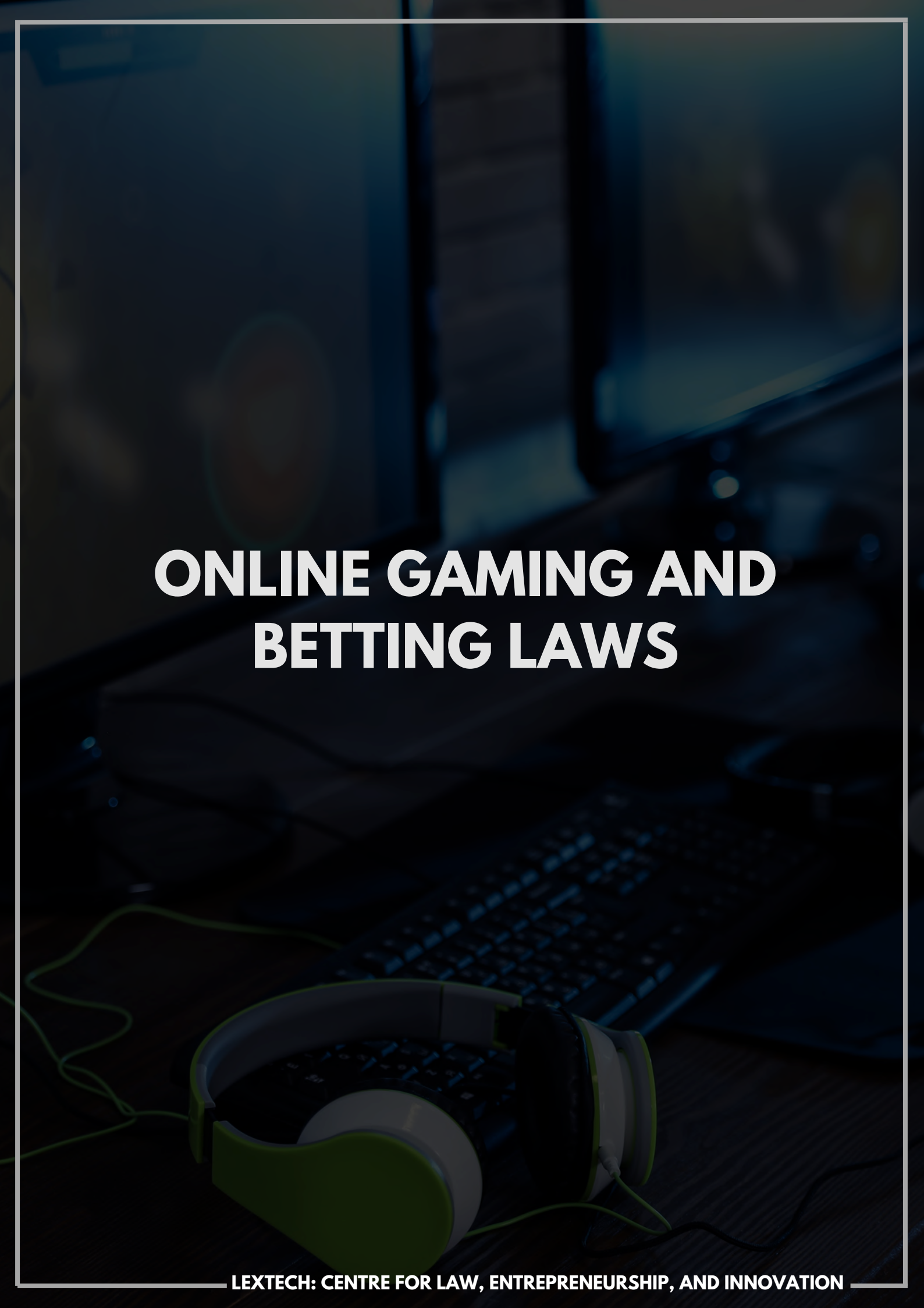
NEW SAFEGUARDS FOR TRANSPARENCY IN GOVERNMENT TAKEDOWN ORDERS UNDER THE AMENDED IT RULES, 2025

continued....

Recently the Karnataka High Court dealt with the legality of the Sahyog Portal and Rule 3(1)(d) of the 2021 Rules. One of the grounds was that circumstances under which Rule 3(1)(d) of the 2021 Rules and Section 69A of the IT Act operate are overlapping. This was neither discussed by the court or the Amended Rules and hence remains an ambiguous area.

The Sahyog Portal's mechanism for checking whether an intimation contains the required information supports the amendments' objective of making takedown processes more consistent with statutory safeguards. Significant concerns regarding transparency also remain as the new rules still do not mandate the publication of takedown directions, keeping the user and general public in the dark about what restrictions are being imposed.

Nevertheless, the amendment addresses the common issues raised by intermediaries as a large number of directives used to be issued without any clear reasoning or authority. This along with the power of the intermediary to signify when a takedown request lacks necessary information on the Sahyog Portal will operationalise a more rational, quicker and transparent process.



ONLINE GAMING AND BETTING LAWS

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP, AND INNOVATION

KARNATAKA'S DIGITAL GAMING BILL CHALLENGES UNION AUTHORITY

NEWS

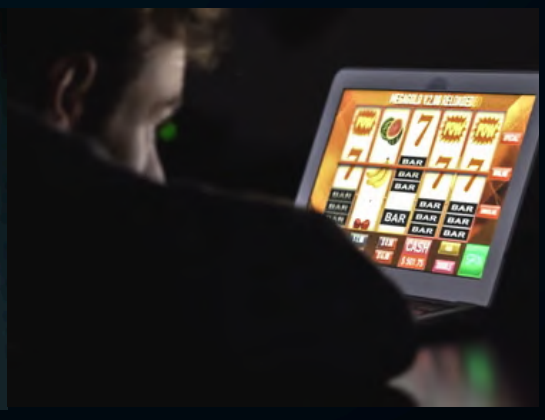
In a significant development, the Karnataka government has prepared a bill amending the Karnataka Race Courses Karnataka Act, 1952. It is expected to be tabled in the upcoming winter session of the state legislature.

The amendment legalises online betting or wagering in horse racing events. Although it stands as a direct contradiction to the centre's Promotion and Regulation of Online Gaming Act, 2025 (**"PROGA"**), it is expected that the revenue generated will help bolster the state economy and additionally make the betting regulated and controlled.

ANALYSIS

The new amendment will spark an old national debate over the power of the state legislatures to challenge the Union's power to make laws in the digital sphere. The state has argued that the "betting and gambling" are reserved for states under the Seventh Schedule of the Constitution and only they are competent enough to pass laws to that respect. The action of the centre is encroaching on the state subjects and thus qualifies as a colourable exercise of power. With respect to this the Karnataka government is actively finalising a constitutional challenge to the Supreme Court, which will join a number of similar constitutional challenges already lying before the apex court.

The amendment is based on the distinction made by the Supreme Court between the games of skill and games of chance. They have asserted that betting on horse racing is an activity driven by "skill and knowledge" and thus falls under games of skill. The Centre through the PROGA had issued a blanket ban on all forms of online betting, which has been bypassed by the state through the assertion that horse betting would be a game of skill.



KARNATAKA'S DIGITAL GAMING BILL CHALLENGES UNION AUTHORITY

continued....

Rather than letting people engage in illegal horse betting activities, in violation of the law, the amendment bill seeks to integrate the online platforms into the existing licensing and oversight mechanisms for race clubs.

This will ensure that these online platforms are transparent, regulated and undertake responsible gaming practices. One of the major issues identified through this conflict is the immediate need of legal clarity for various digital platforms engaging in betting activities. The activities of these apps fall under a legal zone of uncertainty, which is detrimental for the creators as well as the people using those services.

A ruling of the apex court would ensure that a precedent is set for legislative boundaries and regulatory control in the digital sector. In case the bill is upheld by the court, it might serve a template for other states attempting to make such laws.

THE ONLINE GAMING ACT FACES CHALLENGE BEFORE THE SC

News

Head Digital Works Pvt. Ltd. (**"HDW"**) has filed a petition with the Supreme Court for declaring the newly enacted PROGA 2025 as unconstitutional. According to HDW, the Act, through its overly broad prohibitions and vague definitions, prohibits a legitimate business by banning all skill-based games for real money based on their rightful use.

Specifically, HDW states that the Act eliminates the distinction between skill and chance that is well established, and therefore disallows operators from conducting operations lawfully and within the provisions of Article 19(1)(g) of the Constitution.

Analysis

HDW presents two basic challenges to the Act: (1) that the definitions set forth in the Act do not clearly delineate the key elements that distinguish skill games from gambling; and (2) that the Act places a total prohibition on skill-based games and even replaces effective regulatory frameworks (e.g., license(r), age and KYC checks, anti-money laundering controls).

According to the Central Government, this Act is a valid legislative enactment designed to protect society from real and existing harms caused by gambling, including addiction, financial exploitation and illegal money flowing in. They also argue that Parliament has the responsibility of enacting laws that regulate activities which are harmful to society. However, the manner in which the Act is written, enforced and structured creates problems for enforcement by giving the Federal Government and the States overlapping jurisdiction over gambling.

THE ONLINE GAMING ACT FACES CHALLENGE BEFORE THE SC

continued....

There are no clear definitions or safe harbours for skill-based gaming and no clear compliance pathways for both operators and payment processing companies that are deemed to operate within the law. The weaknesses created by the Act makes it vulnerable to challenge for being arbitrary or an unreasonable restriction. The Act does not provide a definitive legal standard for the test between chance and skill and rather opts to do away with such settled categorisation.

Further, it does not provide for a gradual system of implementation or a method of grandfathering existing operators. The Act does not mandate strong verification processes for underage persons, a mechanism for making complaints, a tiered system for operators' licences, or strong policies to prevent money laundering. Most importantly, it does not yet provide guidance on how operators are to proceed with advertising and payment processors.

These very central omissions defeat the very intent behind the Act. While they may be clarified through further regulations, with compliance mandated immediately, it seems the earlier measured regulatory regime might prove more suitable than the prohibition regime.

FINTECH

MADRAS HIGH COURT RECOGNISES CRYPTOCURRENCY AS PROPERTY IN WAZIRX DISPUTE

NEWS

The Madras High Court has held in its recent judgement that cryptocurrency qualifies as "property" under Indian law, capable of being owned, enjoyed, and held in trust. The case arose from a dispute following the 2024 WazirX cyberattack, where an investor's holdings of XRP tokens were frozen by the exchange. The Court granted interim protection under Section 9 of the Arbitration and Conciliation Act, 1996, restraining the exchange from interfering with the applicant's XRP holdings pending arbitration.

ANALYSIS

The High Court's ruling marks a significant development in the legal status of cryptocurrencies in India. Prior to this judgment, cryptocurrencies occupied an uncertain position within Indian law, defined as "virtual digital assets" under Section 2(47A) of the Income Tax Act, 1961, but lacking explicit status as property capable of protection.

The Court relied on settled jurisprudence on the meaning of property which includes all valuable rights and interests capable of ownership, control, and transfer, and applies this understanding to virtual digital assets without relying on any crypto-specific statute.

The Court also relied on the recognition of "virtual digital assets" under the Income Tax Act, reinforcing that cryptocurrencies are legally cognisable assets as opposed to purely abstract interests. While the tax framework was not considered determinative in this case, it provided a reference point to support that crypto holdings can attract proprietary protection.

By treating user crypto holdings as property capable of being held in trust, the judgment indirectly raises the standard of care expected from exchanges and custodians. While the ruling is fact-centric and interim still, it sets an important precedent toward the recognition and protection of user rights in India's evolving digital economy landscape.

RBI ORDERS SIMPL TO HALT PAYMENT OPERATIONS OVER REGULATORY VIOLATIONS

News

The Reserve Bank of India (**"RBI"**) has directed Bengaluru-based buy-now-pay-later (**"BNPL"**) start-up Simpl to stop all payment-related activities with immediate effect. The RBI's order states that Simpl has been operating as a payment system operator without the mandatory Certificate of Authorisation, which is in violation of the Payment and Settlement Systems Act, 2007 (**"the Act"**).

Analysis

Simpl's operations were based on a BNPL framework that is similar to a digital ledger, as opposed to a traditional lending institution. It thus avoided conventional regulated licensing, differentiating it from Non-Banking Financial Companies (**"NBFCs"**) or banks. Unlicensed activities not only face enforcement actions but also jeopardise the stability of the digital payments and consumer protection systems.

Its activities involving payments, clearings, and settlement functions fall within the scope of operations regulated by the RBI. Investigations have also revealed possible foreign exchange offences related to the funding of the company. Prior to the RBI direction, Simpl had been serving as a payment facilitator for more than 26,000 merchants, including Zomato, BigBasket, Rapido, and Box8, with millions of users across the country. The RBI's instruction reflects strict regulatory oversight, signaling to all institutions undertaking similar operations that they must acquire requisite approvals The move reinforces RBI's commitment to safeguarding consumers and maintaining confidence in the financial system. The Act empowers the RBI to oversee the security, safety, and dependability of payment systems.

RBI'S UNIFIED MARKETS INTERFACE FOR NBFCS & ACCOUNT AGGREGATORS.

News

The RBI introduced the Unified Markets Interface (**"UMI"**) at the Global Fintech Fest 2025. UMI is a financial market infrastructure designed to tokenise financial assets using wholesale Central Bank Digital Currency (**"CBDC"**) and blockchain technology. The initiative aims to enhance market efficiency, transparency, and security. It marks a step towards enabling the conversion of real world assets into digital tokens on the blockchain.

Analysis

The Unified Markets Interface enables the tokenisation of real-world physical assets such as property and bonds into digital tokens stored on a blockchain. This initiative increases the participation of small investors through fractional ownership, which means dividing a large asset into small portions, thereby encouraging smaller investments. For faster transactions, UMI uses blockchain-based smart contracts, which operate when the specified conditions are met.

For the safe transfer of data, the Account Aggregator (**"AA"**) framework empowers individuals to share their financial data safely with regulated entities. The organisations who access the financial data for providing services are the Financial information users (**"FIU"**) and the organisations who provide such data to the FIUs are the Financial information providers (**"FIP"**).

Through this initiative RBI plans to improve consent management and strengthen data privacy. Currently 17 AAs, 650 FIUs and 150 FIPs are operational in India, managing over 160 million accounts and processing billions of data requests annually.

RBI is among the first major central banks to launch tokenisation via wholesale CBDC. It ensures these settlements remain under the oversight of RBI, reducing reliance on traditional intermediaries by directly saving transactions in RBI's records. The CBDC framework allows for real time, faster settlements, but it increases the operational risks such as system downtime and component failures. The CBDC has been earlier tested in the pilot project of RBI's Digital Rupee project, where it showed promising outcomes in reducing settlement risks and improving market efficiency.

This step marks a significant shift for AAs and NBFCs as it improves and strengthens their services. NBFCs have been dependent on a limited group of lenders, facing high borrowing costs and concentration risks. The introduction of fractional ownership enables them to lessen their reliance on traditional financiers.

NPCI IS PILOTING AGENTIC AI-BASED PAYMENTS WITH UPI

News

The National Payments Corporation of India (**"NPCI"**) showcased a pilot demonstrating agentic AI payments through UPI at the Global Fintech Fest 2025. The demonstration involved an AI assistant executing a multi-step transaction, including identifying products, placing an order, and completing the payment through UPI, without requiring step-by-step user confirmation.

Analysis

Unlike conventional automation, which merely streamlines predefined steps, agentic AI systems are designed to interpret user intent, sequence actions across numerous platforms, and trigger payments. While the pilot illustrates technical feasibility, it also raises important questions. UPI's existing framework is built on explicit user consent for each transaction, strong authentication, and liability allocation among banks, payment service providers, and users. Delegating payment initiation to AI agents complicates this model, particularly in determining attribution of intent, responsibility for erroneous transactions, and compliance with RBI-mandated authentication and risk controls.

For such a mechanism to be successful, it would need clearly defined spending limits, revocation mechanisms and audit trails. Without an extensive regulatory framework, such systems risk weakening consumer protection norms that have been central to UPI's trust and wide adoption. These concerns remain entirely speculative with the NPCI only exploring its feasibility. There is no foreseeable rollout of this mechanism in the Indian UPI ecosystem. Even so, if implemented at scale, agentic UPI payments could reshape digital commerce. Novel concerns of AI-bias, analysing user preference and behavioural patterns, data privacy implications and many others will come into being. Regulators will have to ensure that convenience does not come at the cost of accountability, user control, or financial security.

ARTIFICIAL INTELLIGENCE

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP, AND INNOVATION

MEITY RELEASES DRAFT AMENDMENTS TO THE IT ACT 2021 TO CURB DEEPFAKES AND SYNTHETIC CONTENT

News

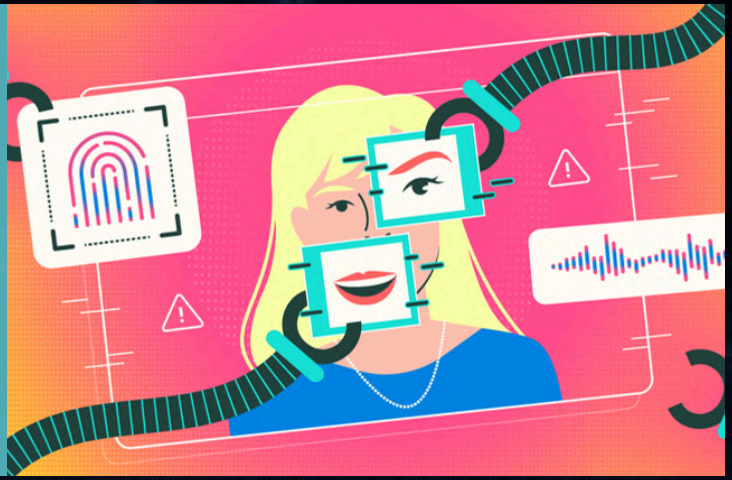
The much-needed draft amendments to Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**"Rules"**) were released by MeitY.

Broadly, the Rules mandate due diligence obligations of intermediaries, including social media intermediaries, to ensure online safety, security, and accountability. The proposed amendment requires that any form of synthetically generated information from artificial systems must be integrated with permanent labels or metadata which would help identify that such information is synthetically generated.

Analysis

The draft amendments strengthen the existing due diligence obligations for digital intermediaries. The amendment has defined synthetically generated information as any form of content which has been either created or modified by artificial intelligence in a manner which "reasonably appears to be authentic and true", that is, it appears to be human-made content.

The draft amendment introduces mandatory labelling procedures of all such synthetically generated information by platforms that support the generation of such content. Specific proportions have been provided: 10% of the display area for visual content and 10% of the clip's duration for audio content. Additionally, Significant Social Media Intermediaries (**"SSMIs"**) have to make provisions for user declarations of the method of generation of content, which must be provided at the time of uploading on platforms.



MEITY RELEASES DRAFT AMENDMENTS TO THE IT ACT 2021 TO CURB DEEPFAKES AND SYNTHETIC CONTENT

continued....

It also suggests that such SSMIs should have detection systems to evaluate the authenticity and source of any information, thus ensuring that no synthetically generated information is posted without it being labelled as such. As also seen in the IT Code, 2021, non-compliance with intermediary guidelines can lead to the termination of safe harbour protections and additional penalties for platforms.

Although the draft amendments are welcome, they do not clarify specific details creating loopholes and compliance challenges. The lack of a uniform digital metadata framework, which differentiates between human-made and synthetic content, enables platforms to design vastly different identification and labeling procedures. This could lead to non-uniform compliance and liabilities with the amendment not clarifying the method of execution.

CALIFORNIA NOTIFIES NEW FRONTIER-AI ACT

News

California introduced the Transparency in Frontier Artificial Intelligence Act (**"TFAIA"**), which made it the first state to enact legislation that specifically targets frontier AI models and developer accountability. Large AI developers with annual revenues over $500 million are required to publish a Frontier AI Framework, conduct transparency reports before deployment of their model, while also maintaining whistleblower protections with penalties of up to $1 million per violation.

Analysis

California's new act is a step towards establishing accountability and transparency for developers in the evolving AI legal landscape. Up until this point, guidelines and statutory frameworks in major countries, barring the EU's GDPR, have set a higher threshold for business enterprises and companies to comply with the laws for data generation and protection, but not for the deployers of that information. With the introduction of this provision, there are now checks and balances to keep major AI developers in check as well.

Frontier AI models are highly capable AI models that were trained using computing power greater than 10^26 integer or floating-point operations; these include large language models (LLMs); examples include ChatGPT, Claude, Bard, etc.

The act requires the developers to implement and publicly publish a Frontier AI framework, which includes the governance structures, industry-specific best practices and a detailed account of the process of identification, assessment and mitigation of "catastrophic risks" in the life cycle of a frontier model. A catastrophic risk is defined in depth to be a foreseeable and material risk that will materially contribute to serious mass injury (more than 50 people) or severe financial damage ($1 billion) from an incident involving the use of a frontier model from a specified list.

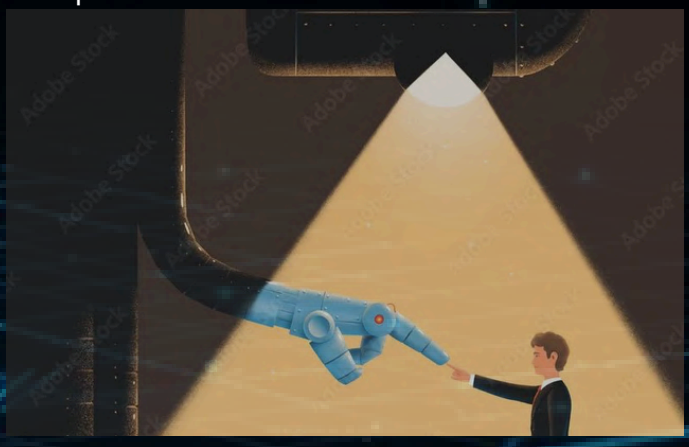
CALIFORNIA NOTIFIES NEW FRONTIER-AI ACT

continued....

While this is an applauded step to usher in serious accountability, the threshold to establish such catastrophic risk is very high, and the Act does not specify any recourse for damages even marginally lower than the prescribed threshold. Such a framework could benefit from revisions which introduce a tiered model of punitive action, ensuring that smaller harms are not entirely neglected.

The Act also requires the developers to publish a transparency report detailing the intended uses of the model, its release date and the modalities of the output supported. However, crucial issues posed by generative AI have been left unaddressed. Large frontier model-based generative AI models have been under scrutiny for following a black box model system wherein the users are only made aware of the input and output, but the data being used to generate the output is unknown and hidden. While developers largely attribute this to the volume of data being used, the opaque algorithms and data being used to generate the output raise concerns of copyright infringement, falsified data and misinformation, which need to be urgently addressed.

The law also details whistleblower protections for employees who report major health and safety risks associated with the frontier AI models, and developers are required to inform their employees of these rights and their relevant responsibilities. This provision was likely a result of the controversies surrounding OpenAI, which restricted the employees from flagging internal safety concerns. To ensure proper implementation, deployer companies are required to set up an anonymised internal reporting system, which would additionally provide the whistleblowers with updates on their complaints.



MEITY RELEASED GUIDELINES TO SET OUT THE INDIAN VISION FOR AI

News

MeitY released a report titled 'India AI Governance Guidelines' (**"Guidelines"**) which outlines the Indian vision for the future of AI regulation and considers a 'pro-innovation' approach to both the integration and accountability model of AI systems. It also recommends a risk governance and classification system that envisions accountability through a graded liability regime based on the function performed by a system, the level of risk, and the degree of due diligence required.

Analysis

The Guidelines build on the principles laid down in the RBI's FREE-AI Framework and the EU's 2019 Guidelines. It lays down similar 'Sutras' for the integration and development of AI systems to support institutions and includes principles like 'People first', 'Innovation over Restraint' among others. The report provides broad insights into the government's likely regulatory approach in the following years through its outlined Action plan, which is divided into three phases with a list of their expected outcomes.

The report also stresses on the integration of AI regulations in existing legal frameworks rather than constructing a legal statute specifically for the regulation of AI. There are also multiple recommendations regarding setting up independent AI governance groups to oversee the overall policy development of the AI governance frameworks.

While these plans are ambitious and holistic in their approach to the integration of AI, the report does not address the practical challenges that are likely to arise during the implementation of these recommendations. Establishing multi-sectoral bodies to oversee AI will inevitably trigger jurisdictional conflicts and regulatory overlap. Moreover, the report places reliance on voluntary compliance mechanisms as the primary accountability model which may be insufficient for the current scale and impact that AI technologies have. Unless such critical gaps in oversight and enforceability are addressed, the report may remain merely an ambitious vision and would fall behind governance mechanisms adopted in jurisdictions such as the EU and the United States.

ITALY BECOMES THE FIRST EU STATE TO ENACT A COMPREHENSIVE AI FRAMEWORK

News

Italy adopted Law 132/2025 becoming the first EU Member State to enact a comprehensive national AI framework. This AI law covers a broad array of domains such as the protection of minors, AI training data usage, copyright and text-and-data mining (**"TDM"**), deepfakes, and sector-specific oversight. The law also limits AI usage to auxiliary tasks for legal functions and retains that core decision-making or intellectual work must remain with humans. Copyright protection is recognised for human authored works created with AI assistance provided they reflect meaningful intellectual work. It also extends TDM exceptions to allow AI based reproductions for data mining under certain circumstances.

Analysis

The law simultaneously introduces distinct national-sectoral rules and broader obligations while remaining in compliance with the EU AI Act. It is likely that other EU countries may come up with their own AI laws in time. This could complicate cross-border deployment of AI systems leading to an increase in compliance costs which may impose disproportionate burdens on smaller developers and start-ups. The European Commission raised similar concerns while reviewing Italy's draft bill. Such a move could benefit larger players who can absorb these costs and could undermine the laws which aim to support small and medium enterprises and national digital sovereignty.

The law's inclusion of a provision prohibiting AI systems that "prejudice the conduct of institutional and political life" and "undermine democratic debate or territorial institutional autonomy" marks an attempt to embed constitutional safeguarding within AI governance. However, there is no prescribed definition for when an AI system is deemed to "prejudice democratic debate" and without clear procedural guidelines or restrictions for enforcement, this provision risks disproportionate application. Unless proper accountability mechanisms and transparent oversight are established, the safeguard may end up as a tool for state control and censorship.

The law also assigns regulatory and surveillance powers to national authorities such as the Agency for Digital Italy and the National Cybersecurity Agency in addition to sectoral regulators.This framework may become a model should it prove to be successful in laying down a balanced approach: being able to preserve democratic integrity without centralising unchecked administrative power, protecting rights without stifling innovation among others.


DATA
PRIVACY

MEITY NOTIFIES THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025

News

The Digital Personal Data Protection Rules, 2025 (**"DPDP Rules"**) have been published by MeitY, thereby marking the implementation of the DPDP Act, 2023 (**"DPDP Act"**). These newly notified rules will complement the act to provide a comprehensive framework for governing the processing of digital personal data. Additionally, the Government also notified an enforcement timeline for various provisions of the Act and established the Data Protection Board of India **("the Board"**).

Analysis

The DPDP Act and the Rules are to be implemented in a phased manner over a period of 18 months. Certain primary provisions, such as the definition clauses, the establishment and functioning of the Board, and the Government's rule-making power under the Act, have come into force with immediate effect. For the Second Phase, the provisions relating to the consent manager framework will come into force one year after the Gazette notification. Lastly, for the third phase, all the remaining substantive and procedural aspects shall come into force 18 months after the notification. This phased implementation, as per the official press release, will give the stakeholders time to comply with the framework's requirements by making necessary changes in their systems.

The law takes a consent-based approach, i.e, every data fiduciary is supposed to give a consent notice to the data principal in plain language, describing the purpose and extent of data collected. Further, they are required to provide means for users to conveniently withdraw their consent, exercise their rights under the Act, and make complaints to the Board. Moreover, for processing the data of a child or a person with disability, the fiduciaries must ensure that they have obtained verifiable consent from their parent or lawful guardian, respectively.

The Rules lay down a newer, detailed set of reasonable security safeguards, as opposed to the older framework under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

MEITY NOTIFIES THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025

continued....

These safeguards include measures such as data security through encryption, prevention of unauthorised access to data, backing up of data to ensure continued processing in the event of its loss or destruction, etc.

On top of that, a significant data fiduciary notified under the act has to follow additional obligations like undertaking an impact assessment and an audit of compliance with the Act and the Rules. Furthermore, in case of a data breach, the rules mandate swift and detailed disclosure to the principal and the Board.

The Rules also mandate that a fiduciary must erase a principal's personal data within three years of inactivity, except when otherwise provided. However, at least forty-eight hours before such erasure, the fiduciary must give the principal a warning regarding the same.

With regard to transparency and accountability, the Rules require the fiduciaries to display clear contact information of a designated officer or a data protection officer for queries related to personal data.

Additionally, all the requests by the principals to exercise their rights must be processed within ninety days.

With the notification of the DPDP Rules, the provisions of the DPDP Act are finally going to come into force.

Its impact will be seen on all major companies like Meta, Amazon and suchlike, who will have to move to a more defined, consent-based approach on processing personal data, which is accountability-oriented, marking a significant step in modernising India's personal data protection regime.

DOT RECALLS SANCHAR SAATHI PRE-INSTALLATION MANDATE FOLLOWING PRIVACY CONCERNS

News

The DoT recently issued a direction requiring smartphone manufacturers and importers to pre-install the Sanchar Saathi application on smartphones sold in India. The application, developed by the Government, is intended to assist users in reporting telecom fraud, verifying IMEI numbers, and blocking lost or stolen devices.

Following public criticism and concerns raised in Parliament regarding privacy and surveillance, the Union Telecom Minister clarified that pre-installation would not be mandatory and that users would retain the freedom to delete the application. Subsequently, the government withdrew the requirement and stated that the goals of the initiative would be met even by voluntary adoption.

Analysis

The controversy centred around the question of user consent and autonomy. Mandatory pre-installation at the point of manufacture or import, even with post-purchase deletion options, would have normalised state presence on personal devices. This approach differs materially from voluntary downloads or opt-in digital services and risks setting a precedent where personal hardware becomes a playground for state interests. From a constitutional perspective, the direction must be assessed against the right to privacy under Article 21 as provided in the landmark judgement in Justice K.S. Puttaswamy v. Union of India.

Any intrusion into privacy must satisfy the tests of legality, legitimate state aim, necessity, and proportionality. While preventing fraud is a legitimate objective, the pre-installation requirement suffered from the absence of a statutory basis, narrowly tailored safeguards, or independent oversight mechanisms governing data access and future use.The DoT's direction stemmed from the Telecommunication Cyber Security Rules, 2024 (**"TCS Rules"**). The rules were further amended in 2025, expanding the ambit of measures to bolster cyber security, mobile identification, and other safeguards. While broad, the TCS Rules do not explicitly lay down the criteria or limits to compel installation of any apps.

DOT RECALLS SANCHAR SAATHI PRE-INSTALLATION MANDATE FOLLOWING PRIVACY CONCERNS

continued....

Rule 5 of the amended TCS Rules empowers the Central Government to establish digital mechanisms "necessary to identify and report acts that may endanger telecom cyber security," and the Sanchar Saathi mandate was justified under this provision. However, the absence of express legislative backing regarding the nature and permissibility of such executive powers undermines the legality of such measures.

Broad references to "telecom cybersecurity" under the rules leaves scope for such directions. In the absence of explicit limits, state-mandated digital tools could operate beyond their original purpose with next to no accountability.

The recall of the directions by the DoT has avoided the creation of a precedent that allows state-software and infrastructure from encroaching on the private domain. However, this highlights the need for greater restraint in digital governance. Measures aimed at public security must be statutorily sanctioned and have the requisite safeguards, as opposed to relying on only executive directions. Legitimate as they may be, cybersecurity objectives cannot be pursued at the cost of user autonomy and constitutional privacy guarantees.

SWITZERLAND'S DATA PROTECTION COMMISSIONER PUBLISHED ITS UPDATED GUIDELINES ON COOKIE USAGE

News

The Federal Data Protection and Information Commissioner (**"FDPIC"**) of Switzerland has released its revised guidelines on Data Processing Using Cookies and Similar Technologies (**"Guidelines"**). These Guidelines explain the manner in which online service providers may deploy technology like cookies and pixels. The updated version introduces additional provisions on user consent, third-party responsibility, and handling of cookie paywalls.

Analysis

Cookies are small text files containing information like saved passwords and user preferences stored on the user's device by the website operator and aims to optimise user experience. Keeping in mind the nature of the information they store, unregulated usage may lead to data privacy concerns.

The Guidelines stem from Article 45c of Switzerland's Telecommunications Act, which governs the storage of cookies on user devices, and the Federal Act on Data Protection, which regulates the processing of personal data. The revised version contains provisions to strengthen user data protection. For instance, it mandates acquiring explicit consent for using third-party cookies to deliver personalised advertising. Further, operators need to ensure that users are intimated about the collection of their data and the operator cannot shirk liability entirely on the external service provider.

The guidelines also add a new section addressing "cookie paywalls", which compels users to either agree to data tracking or pay a fee to access the website. It has been clarified that in such cases, consent is considered voluntary only if the payment alternative is not disproportionate, thus undermining user data protection.
It also addresses dark pattern concerns, highlighting that consent must not be given under deception and the opt-out notices must be prominently placed with no default-checked boxes.These updated guidelines highlight the importance placed on data privacy across European countries. As usage of cookies has increased, their regulation has become vital to ensure the protection of user data.

THE EUROPEAN COMMISSION PRESENTED A DIGITAL PACKAGE TO SIMPLIFY EU RULES

News

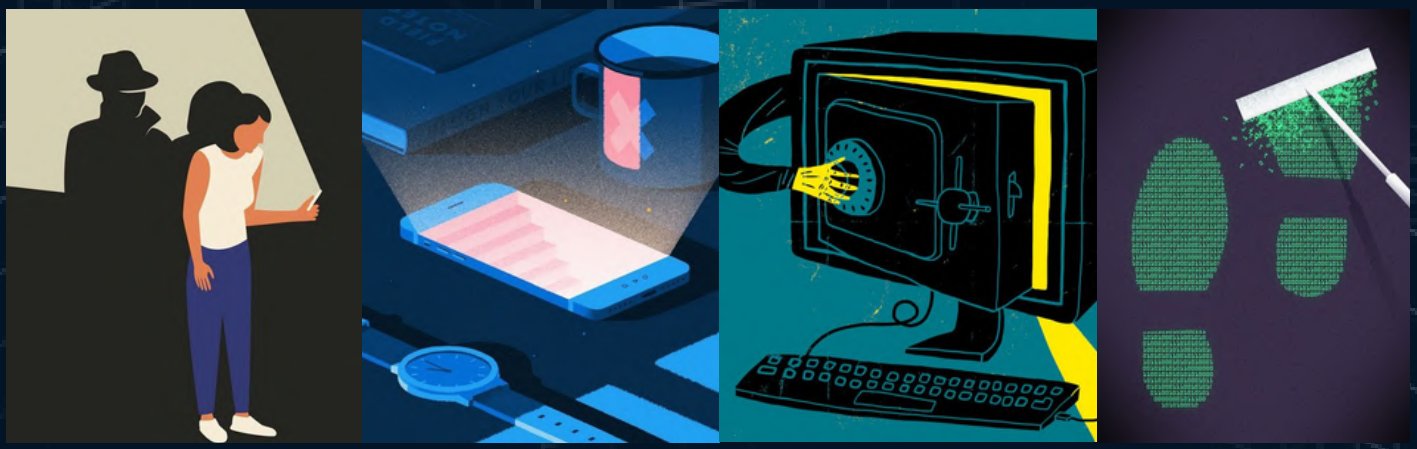
The European Commission has proposed a new Digital Package for simplifying and streamlining major EU digital laws, such as the GDPR, the Data Act and the AI Act. It includes a digital omnibus, which is designed to ease compliance and foster innovation.

Analysis

This package is designed to address issues raised in the Draghi Report, and is a part of the EU's effort to balance competitiveness in its markets while maintaining its tough regulations. Instead of introducing any new laws, the proposed omnibus adjusts the existing frameworks to work smoothly.

As for the GDPR, the omnibus primarily focuses on modernising cookie rules. According to the Commission, citizens are currently faced with multiple pop-up cookie banners, which makes it difficult for them to understand what data they are consenting to be processed and stored. Consequently, they often lack any real choice as they click on any button just to access a website. Thus, the amendments will mandate simplifying the designs of such cookie banners and reducing the number of times they pop up.

Users can now indicate their consent with one click and save their cookie preferences through their browser settings. Additionally, it clarifies what constitutes personal data, and identifies situations where it could be shared with third parties without sharing the data subjects' identities. Moreover, it also emphasises on legitimate usage of data for AI training, while protecting user interests.



THE EUROPEAN COMMISSION PRESENTED A DIGITAL PACKAGE TO SIMPLIFY EU RULES

continued....

The commission has also introduced the new Data Union Strategy, which will help companies to get access to more high-quality data for AI training, through initiatives like Data Labs. These Data Labs are data service providers that link these data spaces with the AI ecosystem.

They give companies and researchers secure, practical access to high-quality datasets, the support they need to ensure compliance with EU rules, and offer tools, guidance, and trusted environments for data pooling, curation, labelling and pseudonymisation.

Further, it also introduces a Data Act Legal Helpdesk to ease compliance. Lastly, this strategy focuses on strengthening the EU's data sovereignty, ensuring fair cross-border data flows while maintaining safeguards for EU-sensitive non-personal data.

This Digital Package is one of several omnibus simplification packages released across different sectors to boost competitiveness in EU markets. While the EU is known for its strict data protection regime, complex and overlapping regulations often work to the detriment of businesses. Thus, this package is a positive step towards fostering innovation and scaling up. As the next step, these proposals shall be sent to the European Parliament and the Council for adoption.

However, there have been criticisms of the proposal, as businesses are pushing for a further reduction in regulatory burdens, while the civil rights organisations claim it will negatively impact the EU's existing stance on Data Protection. Thus, going forward, this omnibus proposal might face a challenging legislative process.

THE EUROPEAN COMMISSION RELEASED THE SECOND VERSION OF ITS AGE-VERIFICATION BLUEPRINT

News

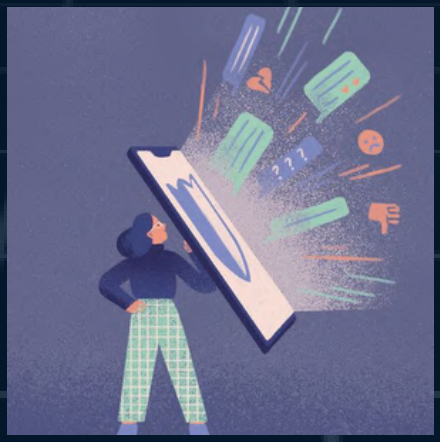
The European Commission has released the enhanced version of its blueprint for age-verification methods. The blueprint permits the use of passports and ID cards, alongside eIDs, as onboarding methods to create proof of age. It supports user-friendly proof submission, allowing for smoother implementation across browsers and operating systems.

Analysis

The Commission had previously published its guidelines on the protection of minors, laying down measures to protect children from harmful content, grooming, cyberbullying, etc. The guidelines also suggested the use of age-verification methods to ensure the safety and privacy of minors.

In furtherance of that, the Commission released the first blueprint for age-verification to create a robust, user-friendly and privacy-preserving method. This mechanism intends to meet the highest privacy standards, which checks user identity only once at the time of verification. It will prevent exposure of minors to age-inappropriate and potentially harmful content, without revealing any personal information.

This blueprint marks an important development in age-verification mechanisms, as the privacy standards set by it are extremely high. In fact, the commission also stated that it is working towards a zero-knowledge age verification system, announced while releasing the first blueprint, which it aims to operationalise soon. With growing global concern over data protection norms, appropriate age-verification mechanisms could harmonise data minimisation goals while ensuring safe and accessible online spaces for all users.



CONTRIBUTORS

WRITERS

ARANYA SEN
ARNAV RAJ
DIYA JAIN
ISHANI GARG
MAITHILI DUBEY
SANIDHYA GURUDEV
SANSKRITI VERMA
TRISHNA AGRAWALLA

EDITOR-IN-CHIEF

PRATYUSH SINGH

DESIGNERS

DIYA JAIN
MAITHILI DUBEY
SUSHREE TEJOSWI

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION