LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

SEPTEMBER 2024 EDITION

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

सत्यमेव विजयते यतः

CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

SECTION 1

BOMBAY HIGH COURT DECLARES IT RULES 2023 AMENDMENT TO BE UNCONSTITUTIONAL AND HOLDS THAT THE GOVERNMENT'S 'FACT-CHECK UNITS' CREATES A CHILLING EFFECT ON FREE SPEECH

NEWS

The Bombay High Court ruled that Rule 3 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 is unconstitutional. Rule 3(1)(b)(v) empowered the central government to form Fact-Check Units ('**FCUs**') that could flag and remove online content deemed "fake" or "misleading" regarding government activities.

LEGAL TALK

This ruling resulted from a petition led by stand-up comedian Kunal Kamra, the Editors Guild of India, and other media organisations, who argued that the rules allowed the government to act as an arbiter of truth and could lead to censorship thereby having a chilling effect on free speech. The amendments were challenged on the grounds that they violated Articles 14, 19(1)(a), and 19(1)(g) of the Constitution. The petitioners argued that the rule allowed the government to arbitrarily and unilaterally decide what constituted "fake" or "misleading" news, with no clear definition of these terms, raising concerns over potential abuse of power and censorship. The court agreed with this analysis, stating that vague and undefined terms like "fake" and "misleading" could be misused to suppress legitimate criticism of the government. The court also highlighted that the government cannot be the sole arbiter of truth, as this would directly conflict with the fundamental principles of democracy. The court also noted that the rule created a chilling effect on free speech, discouraging individuals and media platforms from posting content critical of the government. The court held that the amendments imposed unreasonable restrictions that are not in consonance with constitutional protections.

THE WAY FORWARD

This ruling reinforces the need for a balance between combating misinformation and upholding free speech. While the government's intent to regulate fake news is valid the mechanisms must be non-partisan and ensure transparency. Relying solely on government led fact-checking bodies, as provided for in the amendments, raises concerns about bias and punitive enforcement. Instead, the government could explore independent, third-party fact-checking bodies that could ensure checks and balances, reducing the risk of censorship. Further, amendments that clearly define terms like "fake" or "misleading" and establish guidelines for the identification and removal of such content, may provide a more constitutionally acceptable framework.

DOT RELEASES NEW RULES FOR LAWFUL INTERCEPTION OF MESSAGES

NEWS

The Department of Telecommunications ("**DOT**") has introduced the draft Telecommunications (Procedure and Safeguards for Lawful Interception of Messages) Rules, 2024 ('**the Rules**'). The Rules are designed to modernise and strengthen legal frameworks by allowing law enforcement and government agencies to intercept communications for national security and crime prevention. However, the Rules set under the Telecommunications Act, 2023, raise serious issues regarding the balance between national security and personal privacy.

THE WAY FORWARD

The Rules aim to prevent unlawful interception of messages by establishing a system of checks and balances. While they do not significantly overhaul the existing framework for lawful message interception, most of the requirements from the Existing Rules have been retained, with only a few changes, such as the designations of officers. Given the broader definition of Telecom Entities within the Rules, it will be crucial to observe their implementation once they come into effect. As awareness of data privacy increases and cyberattacks grow more sophisticated, it remains to be seen whether the procedural safeguards and measures in the Rules achieve an appropriate balance between surveillance and privacy rights.

LEGAL TALK

The Rules reinforce Section 5(2) of the Telegraph Act, 1885 which authorises interception of messages in cases of public emergency or in the interest of public safety, provided there is a threat to national security, public order, or to prevent incitement of an offence. It requires that interception orders be issued only after obtaining prior sanction from the Union Home Secretary of the Ministry of Home Affairs or a similar office at the state level.

While the older rules introduced vital safeguards – such as centralised authority, penalties for telecom violations, and checks on unauthorised interceptions – the new rules expand state powers, potentially covering all forms of digital communication. This poses a heightened threat to individual privacy as the Rules' definitions are more expansive, allowing the government to intercept communications under broadly defined terms like "public order" and "friendly relations with foreign states." This vague terminology can easily be manipulated to justify politically motivated surveillance against journalists, activists, or dissenters.

Another pertinent issue is the absence of judicial oversight. Unlike other democratic frameworks that mandate judicial approval before communications interception, the Rules empower the executive branch without requiring any such checks. This one-sided concentration of power removes an essential layer of neutrality and opens doors to arbitrary surveillance practices.While Rule 14 and 15 of Indian Telegraph (Amendment) Rules, 2007 imposed strict penalties on telecom providers for unauthorised interception, these safeguards have been diluted by the Rules, making data breaches and surveillance by telecom companies less accountable.

DOT RELEASES NEW TELECOM CYBER SECURITY RULES

NEWS

DoT published the draft Telecommunications (Telecom Cyber Security) Rules, 2024, ('**the Rules**'). It is aimed at strengthening cyber security across India's telecommunications networks. The Rules impose compliance obligations on telecom and shall replace previous regulations under the Indian Telegraph Act, 1885. It focuses on establishing a more comprehensive framework to address emerging cyber threats.

LEGAL ANGLE

Rule 3 empowers the central government or any of its authorised agencies to collect traffic data which refers to any data generated, transmitted, received, or stored in telecommunication networks, including data related to the type, routing, duration, or time of telecommunication, thereby reinforcing government oversight of telecommunications security. Importantly, the mandate for telecom entities under Rule 7 (1) to report security incidents within six hours represents a significant compliance obligation, reflecting the urgency with which the government aims to address potential threats. The appointment of a Chief Telecommunication Security Officer (**"CTSO"**) for each entity furthers accountability and ensures a direct line of communication with the government. The Rules also require the establishment of incident response mechanisms and periodic cyber security audits, aligning with best practices in risk management. However, the expansive definition of a 'security incident', which means an event having an actual or potentially adverse effect on telecom cyber security, may lead to increased reporting burdens, raising concerns about the operational impact on telecom entities.

THE WAY FORWARD

Moving forward, telecom entities should engage in a dialogue with the government to refine reporting timelines and compliance processes, ensuring they are practical while still effectively mitigating cyber risks. Emphasising collaboration will be crucial for implementing these Rules successfully.

THE ANTI-TOBACCO RULES, 2024 FOR OTT PLATFORMS

NEWS

The Ministry of Health and Family Welfare introduced a draft amendment to Tobacco Products (Prohibition of Advertisement and Regulation of Trade and Commerce, Production, Supply and Distribution) Amendment Rules, 2024, targeting OTT streaming platforms.

LEGAL TALK

The new regulations mandate non-skippable, 30-second anti-tobacco health spots at the start of all content, 20-second audio-visual disclaimers upon opening the platform, and static health warnings during scenes depicting tobacco use. The amendment expands on earlier rules issued in 2023, intensifying the obligations on streaming platforms. This regulatory shift raises pertinent legal questions regarding jurisdiction. Historically, OTT platforms fall under the purview of the Ministry of Information and Broadcasting ('**MIB**') and the Ministry of Electronics and Information Technology ('**MeitY**'). The Ministry of Health and Family Welfare's involvement suggests a broadening interpretation of its mandate under the Cigarettes and Other Tobacco Products Act, 2003 ('**COTPA**'), which could face legal challenges. Streaming services like Netflix and Amazon Prime had already pushed back against the 2023 amendments, citing concerns about disruptions to user experience and the financial burden of compliance. Further, these platforms questioned whether requiring such intrusive health warnings aligns with constitutional protections under Article 19(1)(a) (freedom of speech and expression), especially if they argue that these rules effectively impose content censorship.

THE WAY FORWARD

A balanced regulatory approach is needed to address health concerns without undermining OTT platforms' ability to operate effectively. A potential compromise could involve less intrusive warnings for mature-rated content and more flexible placement of disclaimers. The non-skippable, mandatory warnings infringe upon creative freedom without clear empirical evidence that such measures reduce tobacco consumption. The lack of a transparent consultative process has also raised concerns about inclusivity and fairness, especially as foreign platforms with global operations may face unique compliance challenges.

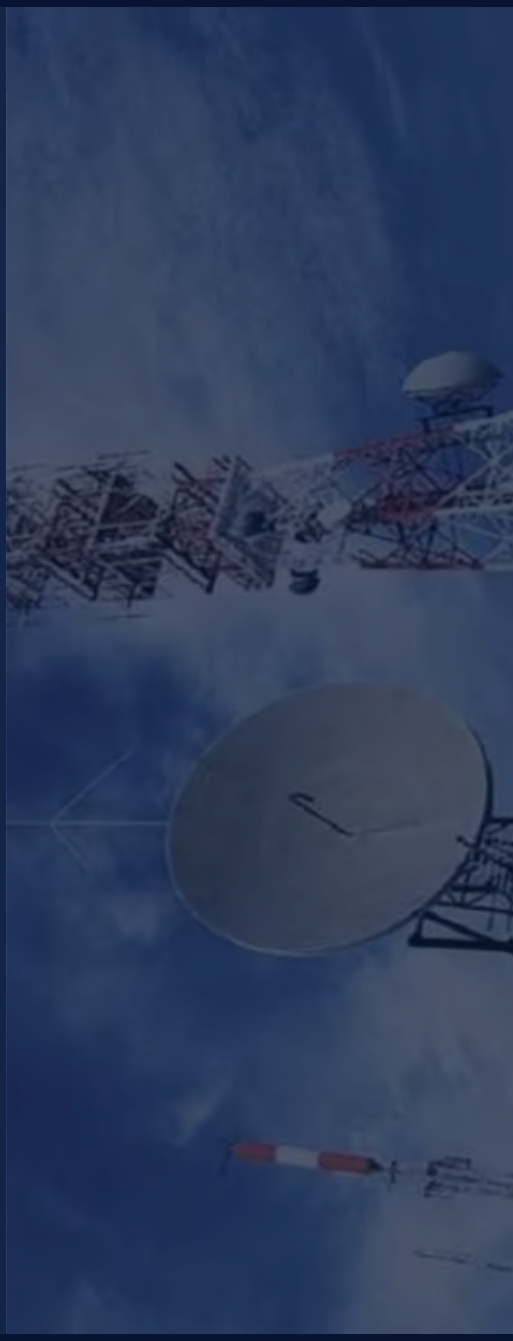
STRENGTHENING TELECOM REGULATIONS: TRAI'S PROACTIVE MEASURES AGAINST FRAUDULENT MESSAGING

NEWS

The Telecom Regulatory Authority of India ('**TRAI**') issued new directions to combat fraudulent activities associated with promotional and transactional messages ('**the Directions**'). These aim to enhance compliance and address the misuse of registered headers and content templates in unsolicited commercial communications.

LEGAL TALK

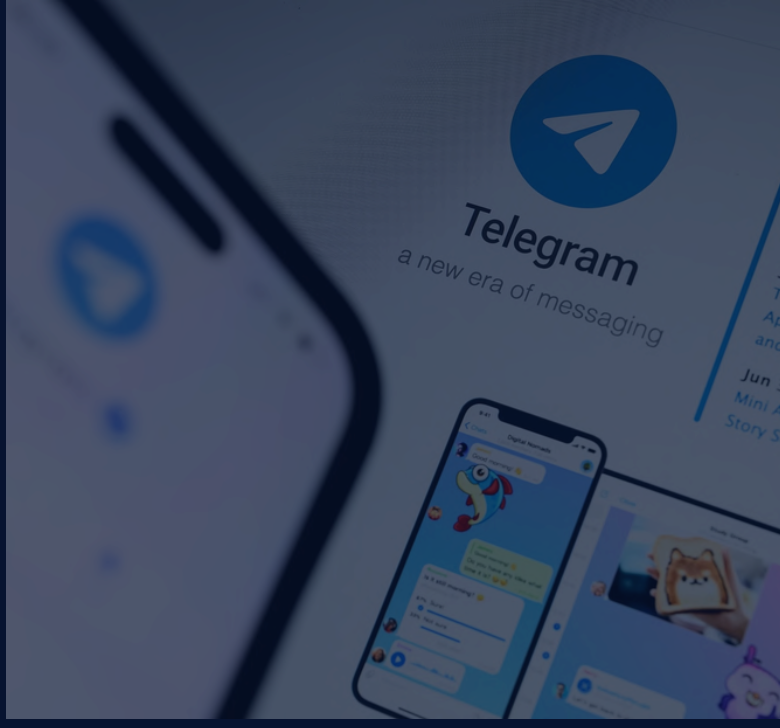
The Directions highlight a significant regulatory response to the ongoing issue of unsolicited commercial communications ('**UCC**') within the framework established by the Telecom Commercial Communication Customer Preference Regulations, 2018 ('**TCCCPR**'). Under the TCCCPR, any commercial communication must utilise registered headers and content templates to ensure transparency and accountability. However, the persistent misuse of these registered elements has prompted TRAI to adopt stringent measures to bolster enforcement and compliance. Key provisions of the new Directions have mandated the Access Service Providers to migrate telemarketing calls to the online Distributed Ledger Technology ("**DLT**") platform for better monitoring and control. This traceability is crucial for identifying the origins of messages and holding senders accountable for any fraudulent content disseminated through their registered headers. Moreover, Access Providers are prohibited from transmitting non-whitelisted URLs and APKs, effectively reducing the risk of malicious content being sent to consumers. The directives also introduce punitive measures, including the blacklisting of content templates registered in the wrong category and the suspension of services for repeat offenders. Such measures serve as deterrents against misuse while also establishing a framework for compliance reporting to TRAI. Additionally, the Digital Personal Data Protection Act, 2023, requires businesses to secure explicit consent before processing personal data, such as names and contact information for promotional communications. This dual layer of regulation emphasises the importance of adhering to data privacy principles and consumer protection in a rapidly evolving digital environment.



THE WAY FORWARD

The directions intend to curb unwarranted promotional communication, and not to eliminate promotional communication altogether. To enhance the efficacy of these measures, it is crucial for TRAI to implement regular audits and establish a feedback mechanism for consumers to report violations. Stakeholder engagement through workshops and training can further promote compliance among Access Providers, ensuring a more secure messaging ecosystem. It addresses the surge in misleading promotional messages by enforcing the use of whitelisted URLs and blacklisting miscategorized content templates. This proactive approach enhances traceability and serves as a deterrent against fraud. However, effective implementation is crucial to avoid potential disruptions in transactional and service message delivery.

FRANCE VS. TELEGRAM: HOW AN UNTESTED CYBERCRIME LAW IS SHAKING BIG TECH



NEWS

In light of the recent investigation of Telegram Founder Pavel Durov, France has become the first country to invoke a tough, untested cybercrime law that directly criminalises tech executives whose platforms enable illegal activities. The Loi d'Orientation et de Programmation du Ministère de l'Intérieur **("LOPMI")** law, enacted in January 2023, has put France at the forefront of a group of nations taking a firmer stance on crime-ridden websites.

LEGAL TALK

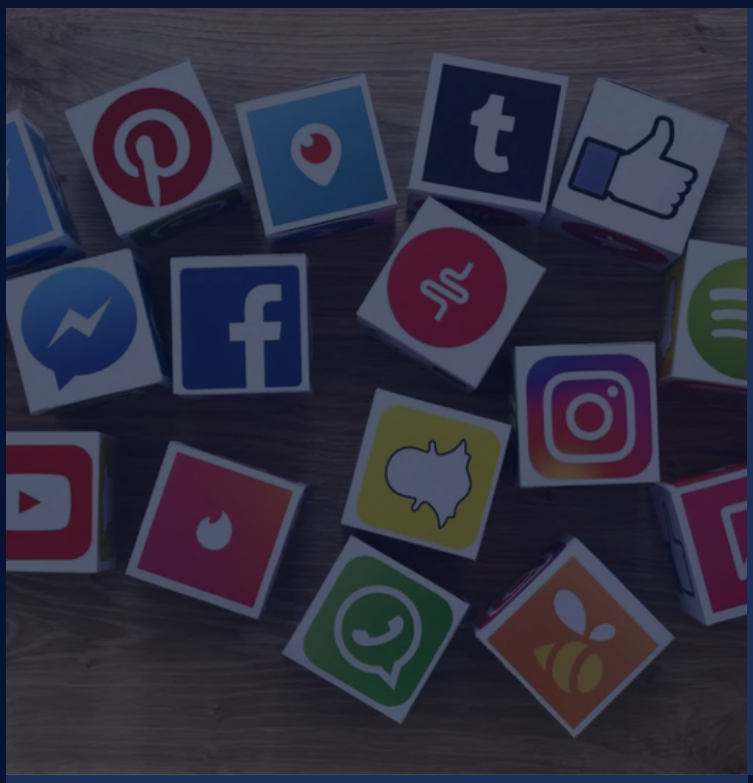
Although unique in its scope, the LOPMI law could potentially hold Durov and several other tech titans criminally liable for allowing misuse of their platforms, though no convictions under this law have been secured so far. The legislation pushes for complete digital transformation through modernisation of investigative tools, improving cybercrime response and increasing surveillance. The novel offence introduced under the law carries a hefty charge including upto 10 years of imprisonment and a €500,000 fine. Critics argue that securing such convictions in other jurisdictions, like the U.S. or India, would require proof that platform owners knew about and actively facilitated illegal activity; a difficult task, especially with platforms like Telegram that serve mostly law-abiding users. Furthermore, Telegram's case calls into question the widely accepted 'safe harbour' protections that shield social media platforms from liability, provided they remove illegal content when flagged by authorities. Although not explicitly codified in any provision, these protections are a common practice across many jurisdictions, making them easier to circumvent due to their implicit nature.

Nonetheless, France views the LOPMI law as a powerful tool in combating grave crimes such as the distribution of child pornography, fraud, and drug trafficking. Durov's arrest by French authorities marks a substantial escalation in the global conversation about the accountability of tech platform leaders. In India, Telegram is under similar scrutiny for allegedly facilitating criminal activities, which could jeopardise its safe harbour protections under Section 79 of the Information Technology Act, 2000. According to the IT Rules, 2021, a platform's 'chief compliance officer'—responsible for ensuring compliance with the IT Act and related regulations—can be held criminally liable if the platform fails to adhere to takedown requests or violates other legal mandates. However, despite this provision, the Indian government has yet to exercise this power. In the past month alone, both France and Brazil have taken significant actions against tech companies and their executives, reflecting a growing trend among nations to hold tech leaders accountable for the misuse of their platforms. This shift highlights the increasing frustration governments feel toward the perceived lack of responsibility in curbing illegal activities online.

THE WAY FORWARD

This legal action raises larger questions about the future of content moderation and platform liability. Telegram, long criticized for its lack of cooperation with law enforcement and its zero-tolerance policy on sharing user data with third parties, now signals a shift towards addressing these issues more seriously. The arrest of a major platform CEO, like Durov, is unprecedented in recent history and could prompt other platforms to tighten their moderation policies. Whether this leads to more censorship or enhanced platform accountability is a trend worth watching closely.

MEITY ISSUES ADVISORY URGING SWIFT REMOVAL OF PROHIBITED CONTENT BY SOCIAL MEDIA PLATFORMS



NEWS

The Ministry of Electronics and Information Technology ('**MeitY**') released an advisory for all intermediaries, including social media platforms, cloud service providers, and telecom operators, to swiftly remove prohibited content in compliance with the Information Technology Act, 2000 and Intermediary Guidelines, 2021. This advisory follows the Bombay High Court directive, where Meta and other platforms were ordered to take down AI-generated deepfake videos involving the National Stock Exchange's Managing Director, within 10 hours of receiving a complaint. MeitY emphasised that platforms must proactively take action within 36 hours of receiving a complaint or government notice.

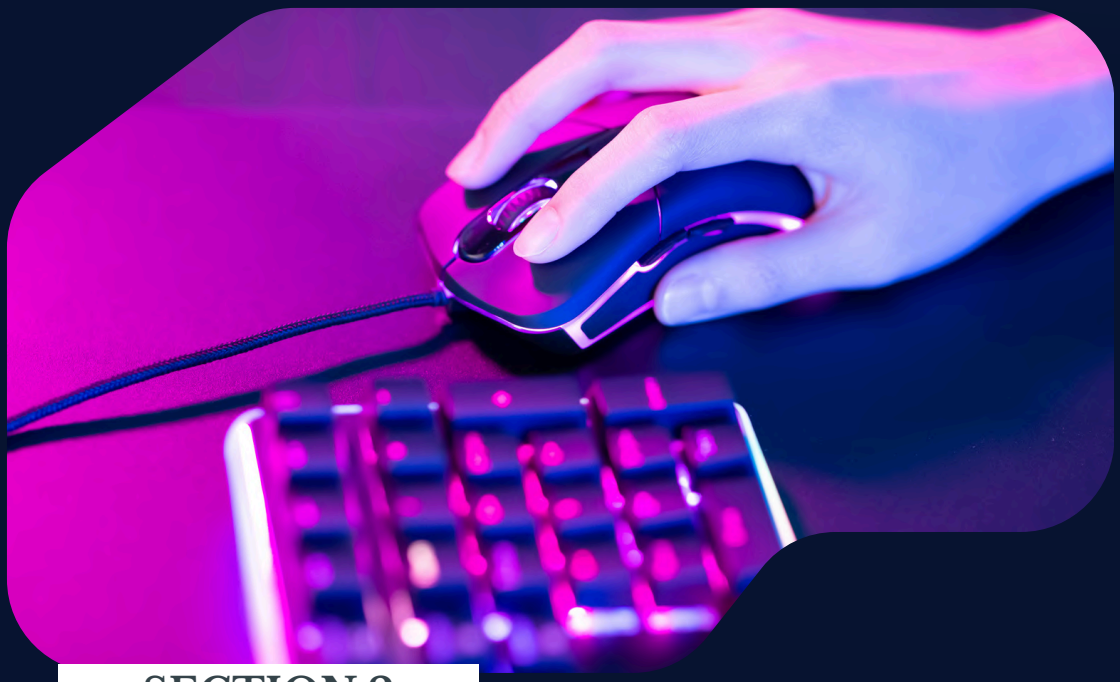
LEGAL TALK

The advisory draws attention to intermediaries' due diligence responsibilities under Rule 3(1) of the Intermediary Guidelines. The rule mandates platforms to remove illegal or prohibited content, ranging from intellectual property violations to harmful fake news, within a 36-hour timeframe. This is essential to retain intermediaries' "safe harbor" protections from liability for user-generated content. The ministry has urged intermediaries to treat the 36-hour limit as an upper threshold.

THE WAY FORWARD

MeitY's advisory signals a growing regulatory push to strengthen content moderation mechanisms, especially in light of new threats like deepfakes. Looking ahead, platforms will need to enhance their automated detection tools and collaborate with third party fact-checkers to ensure both swift compliance and respect for user rights. The ministry might also explore a collaborative framework between the government, intermediaries, and third party fact-checkers to develop clearer guidelines on content moderation, reducing the risk of governmental overreach while also protecting users from harmful content.

Online Gaming and Betting Laws



SECTION 2

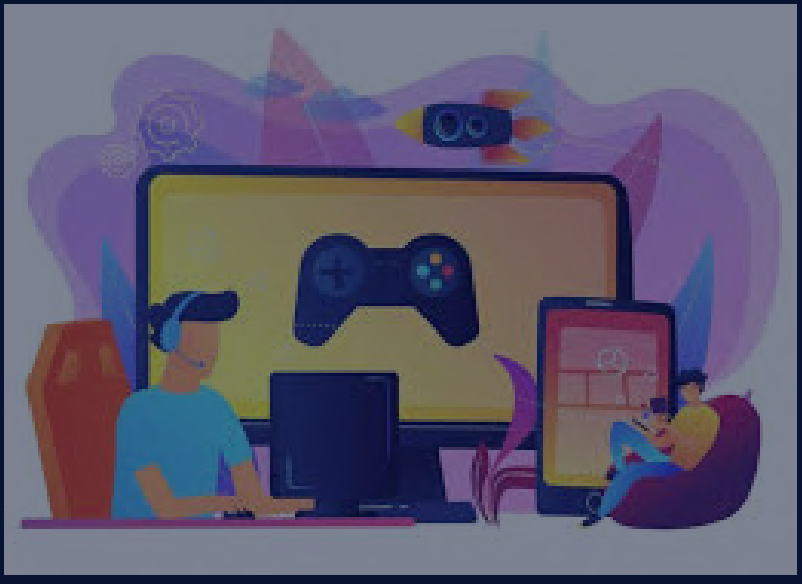
CENTRAL GOVERNMENT TO ESTABLISH PANEL FOR ONLINE GAMING REGULATORY COMPLIANCE

NEWS

In recent developments, the Union Government plans to establish an inter-department regulatory compliance authority for online gaming platforms to curtail tax evasion and other regulatory malpractices. With states like Tamil Nadu and Karnataka already attempting to regulate or ban certain forms of online gaming, the formation of the regulatory panel signifies the central government's interest in creating uniform rules that will safeguard users and help promote responsible gaming.

LEGAL TALK

The legal framework governing online gaming in India is fragmented and falls within the purview of both central and state authorities. The Central Goods and Services Tax ('**CGST**') Act, 2017, distinguishes services from "actionable claims" (which are classified as goods). Online gaming companies have been found underreporting taxable supplies and misclassifying games to avoid paying GST, which is now at 28% on all deposits. Investigations have uncovered massive non-compliance with show cause notices being sent to 34 companies demanding outstanding payment of taxes amounting to ₹1,10,531.91 crore. Several of show cause notice recipients have approached the court filing Writ Petition against the notices, and the matter is sub-judice before the Hon'ble Supreme Court of India. Many platforms exploit jurisdictional loopholes such as the absence of uniform global regulations, inadequate technological infrastructure for tracking transactions, and operating from offshore entities in tax havens. Offshore platforms present additional challenges, with many avoiding registration under Indian tax laws and utilising decentralised technologies like blockchain, making regulatory enforcement more difficult. The Directorate General of GST Intelligence ('**DGGI**') has recommended the formation of an inter-departmental committee, including representatives from agencies like the Enforcement Directorate ('**ED**') and the Reserve Bank of India ('**RBI**'), to curb such malpractices. This step is crucial to address the broader challenges of tax evasion, money laundering, and compliance in the online gaming sector. Especially at a stage when India lacks comprehensive gaming laws and recent court rulings, such as the Allahabad High Court's decision that affirmed Poker and Rummy are games of skill, not gambling, highlighting the judiciary's leniency in distinguishing between games of skill and chance. However, due to overlaps with gambling, combined with tax and compliance concerns, a more thorough legal analysis is needed for businesses operating in these sectors to ensure proper regulation and adherence to tax laws.



THE WAY FORWARD

The establishment of a central regulatory panel is expected to provide much-needed clarity and standardisation for the online gaming sector in India. Realising that only a multi-stakeholder approach can solve this issue, the government must engage with gaming platforms, legal experts, and user advocacy groups to craft regulations that balance growth with user safety.

FinTech

SECTION 3

CONTRASTING APPROACHES TO DIGITAL ASSET REGULATION: UK APPROVES OF LEGAL PROTECTION WHILE CHINA HOSTILE TOWARDS DIGITAL ASSETS

INTRODUCTION

The global world is continuously witnessing significant evolution in technology and the financial sector is no exception to it. With the emerging innovation in digital assets, blockchain, and the fintech sector, governments across the countries are also cautious of the negative impact they can have if not properly regulated. With this, two significant legislative developments have emerged recently which highlight the contrasting approaches adopted by two different nations, the UK and China, for legally regulating digital assets in the financial market.

UK'S PROGRESSIVE STANCE: LEGAL CLARITY FOR DIGITAL ASSETS

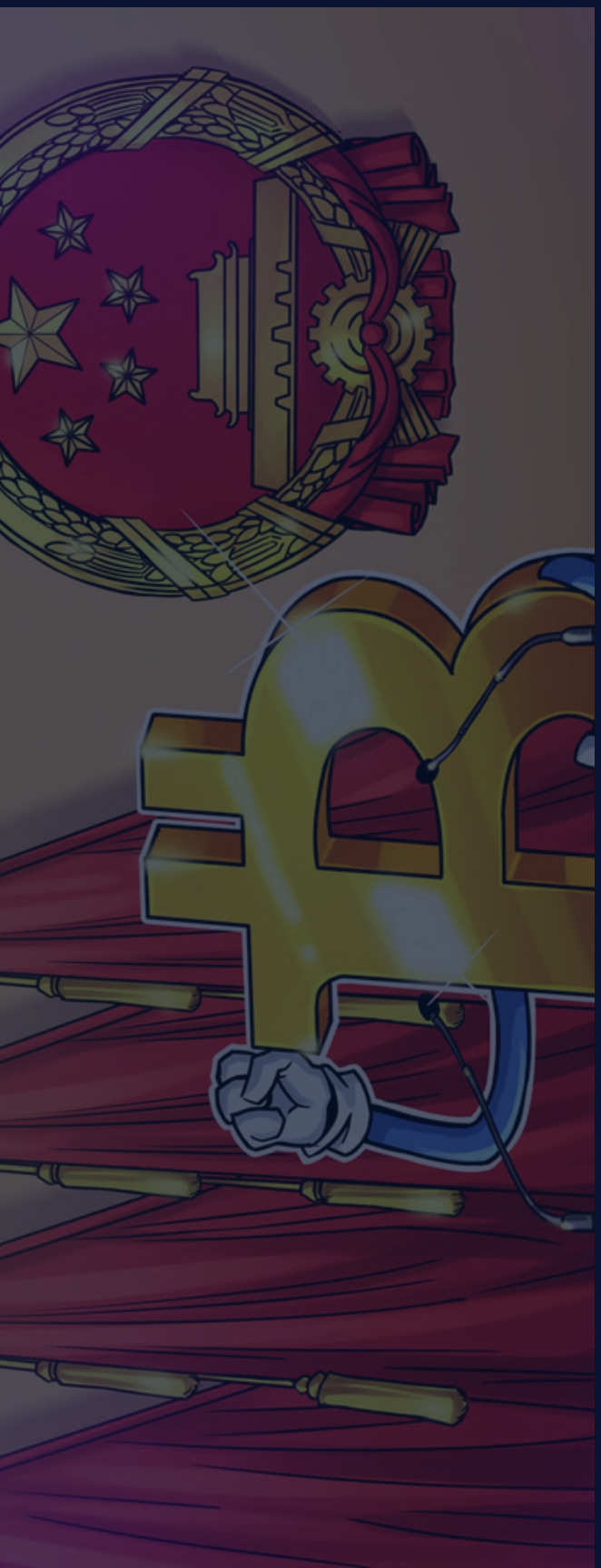
The UK government as part of a broader push to position the country as a hub for innovation in blockchain and fintech has recently introduced the Property (Digital Assets etc) Bill which aims to provide much-needed legal protection to digital assets such as cryptocurrencies and non-fungible tokens ('**NFTs**'). The bill furthers the recommendations from the Law Commission for England and Wales, which was formed to recommend solutions for the legal recognition of digital assets.

Objective:

The central objective of the bill is to ensure that digital assets like cryptocurrencies, NFTs, carbon credits, etc. are also treated as "property" under the objects of personal property, hence capable of possessing personal property rights similar to other traditional assets under UK law. Clause 1 being the main clause of the bill provides that a *"thing (including a thing that is digital or electronic in nature) is not prevented from being the object of personal property rights merely because it is neither a thing in possession, nor a thing in action."* Further, a thing may be capable of attracting property rights even if it does not fit into either of the two categories of personal property that have traditionally been recognised under the law of England and Wales.

Legal Implications:

The bill intends to legally protect the owners from potential theft or fraud in the digital spaces by enhancing digital security. The legal designation is also crucial for resolving disputes centred around the ownership, security, and transfer of assets and helps in determining complex legal relationships. The digital assets can also be a part of the bankruptcy and insolvency process whereby they can be used to repay creditors. The legal recognition helps in better regulation of the assets during the process. The bill also helps in the enforcement of contractual rights in the case of smart contracts in a manner similar to traditional legal contracts whereby they do not need to prove any property rights first.



CHINA'S APPROACH: PRIORITISING AML MEASURES IN FINTECH

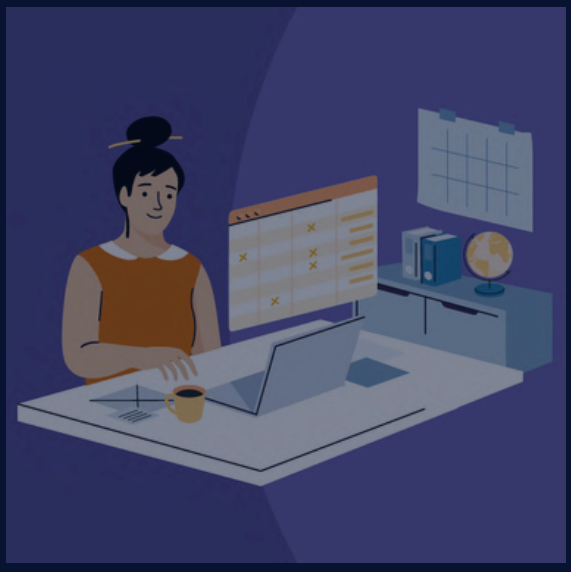
In contrast to the UK's emphasis on legal recognition of digital assets and grant of property rights, China intends to tighten the regulations to combat the potential misuse of fintech for illicit purposes. The government of the country is in the process of closely monitoring digital transactions by creating a new anti-money laundering ('**AML**') law, particularly in the emerging areas of fintech areas which include decentralized finance ('**DeFi**') and digital currencies.

Legislative Intentions:

The intention for a new AML emerge from increasing cases of digital fraud and other illicit financial activities through digital assets. There have also been instances where digital assets have been used as new channels for money laundering. The central bank of China has already rolled out its own digital currency (the digital yuan). This displays the government balanced approach of welcoming innovations in the fintech sector while also not jeopardizing the integrity of its financial system. The proposed idea of amendments in the AML law seeks to monitor fintech platforms and digital asset transactions with a particular focus on transp arency and reporting to financial institutions. The main objective is to trace and prevent money laundering activities, which could be caused by misusing the latest in blockchain and AI technologies where large volumes of digital transactions are scrutinized. This approach is in consistency with China's broader regulatory trend, which has often favoured control and oversight over rapid innovation.

LEGAL FRAMEWORKS REFLECT DIFFERING PRIORITIES

The contrasting regulatory approaches in legal protection emphasize on the differing stance adopted by both countries on developing technology. The UK's focus on legal certainty is driven by a desire to foster innovation and create a welcoming environment for blockchain-based businesses. On the other hand, China, which has provided legal tender to the digital assets to digital assets, is yet very cautious about its free circulation in the financial market. The People's Court in China in its report "Identification of the Property Attributes of Virtual Currency and Disposal of Property Involved in the Case" stated that "virtual currency is not classified as an illegal item," which does suggest a legal framework supporting ownership rights over digital assets. However, the recognition is part of a broader framework of stringent regulations; China has imposed a ban on digital asset transactions since 2021 due to concerns over illegal activities associated with these assets. The nation prioritizes maintaining tight control over financial systems and minimizing the risks of illicit activity in the fintech space. The approach adopted by China differs from that of the UK, whereby the nation instead of imposing stringent regulatory mechanisms focuses on a liberal legal framework of adoption. It fosters a non-restrictive environment for smooth financial transactions by legally recognising property rights and granting them protection.



THE WAY FORWARD

These developments are not unique to the two countries, instead they are significant financial innovations. Therefore, the key takeaway for the other countries is to adopt a balanced approach where innovation is valued but financial security is not compromised while regulating digital assets and fintech. For the global community, the UK's attempt to define legal boundaries and China's focus on stringent AML measures set forth two distinct models for how to approach the next phase of digital finance. The selection of their approach depends on the regulatory landscape present in each country.

ARTIFICIAL INTELLIGENCE

SECTION 4

GEN AI A SUPERWEAPON IN THE HANDS OF CYBERCRIMINALS?

NEWS

GenAI is becoming a superweapon in the hands of cybercriminals. It has become the perfect tool for social engineering activities. The criminals are slyly crafting prompts to make the AI model do things that it would normally not do. AI can be used to combat AI but there are concerns regarding 'AI washing', a marketing tactic wherein people are made to believe that a product or service is safe because AI has been integrated into it. Therefore, the focus should lie on the foundational legal framework of cybersecurity.

LEGAL TALK

Offenders of cybercrime are often known but hard to reach legally which is why disruption as a policing method can be used to prevent it. One way to disrupt criminal activity is through the enforcement of law. The law enforcement agencies may focus on prosecuting minor offences instead of the major hard-to-prove ones. This way the offender's main operation would be halted and it will deter others from committing similar crimes. For e.g. laws against identity theft aim to stop the misuse of personal information before it leads to fraud. Another tried and tested way of hindering AI-based cybercrime is through lawsuits. Microsoft for instance collaborated with Europol, other tech leaders, and the FBI to disrupt the Sirefef botnet by filing a civil suit against the botnet operators and obtained court authorization to block communications between US computers and 18 identified IP addresses linked to the botnet and Europol coordinated actions in Europe executing search warrants in several countries. AI misuse is often transnational, hence intelligence sharing is a key tool to combat this as iterated in the Budapest Convention as it enables the nations to pool their technical expertise, and knowledge to identify threats early. For e.g. nations can work together to trace the origins of ransomware attacks and disrupt the operations of AI-powered botnets. Article 33 of the GDPR seeks prompt notice of data breaches to the relevant authorities, this could help the authorities limit the damage.

THE WAY FORWARD

Cybercriminals have always been early adopters of the latest technology and AI is no different. Combating this problem requires a multi-faceted approach. Firstly, it is essential to update the existing laws to address the unique challenges posed by AI, ensuring areas like deepfake and AI-driven fraud are addressed. Investing in AI-driven security tools can also help detect and respond to cyber threats in real time. Additionally, enterprises should make sure their AI chatbots, built on large language models, stay focused on the specific areas they were trained for. Public awareness and education initiatives also play a major role as it encourages individuals to report suspicious activities.

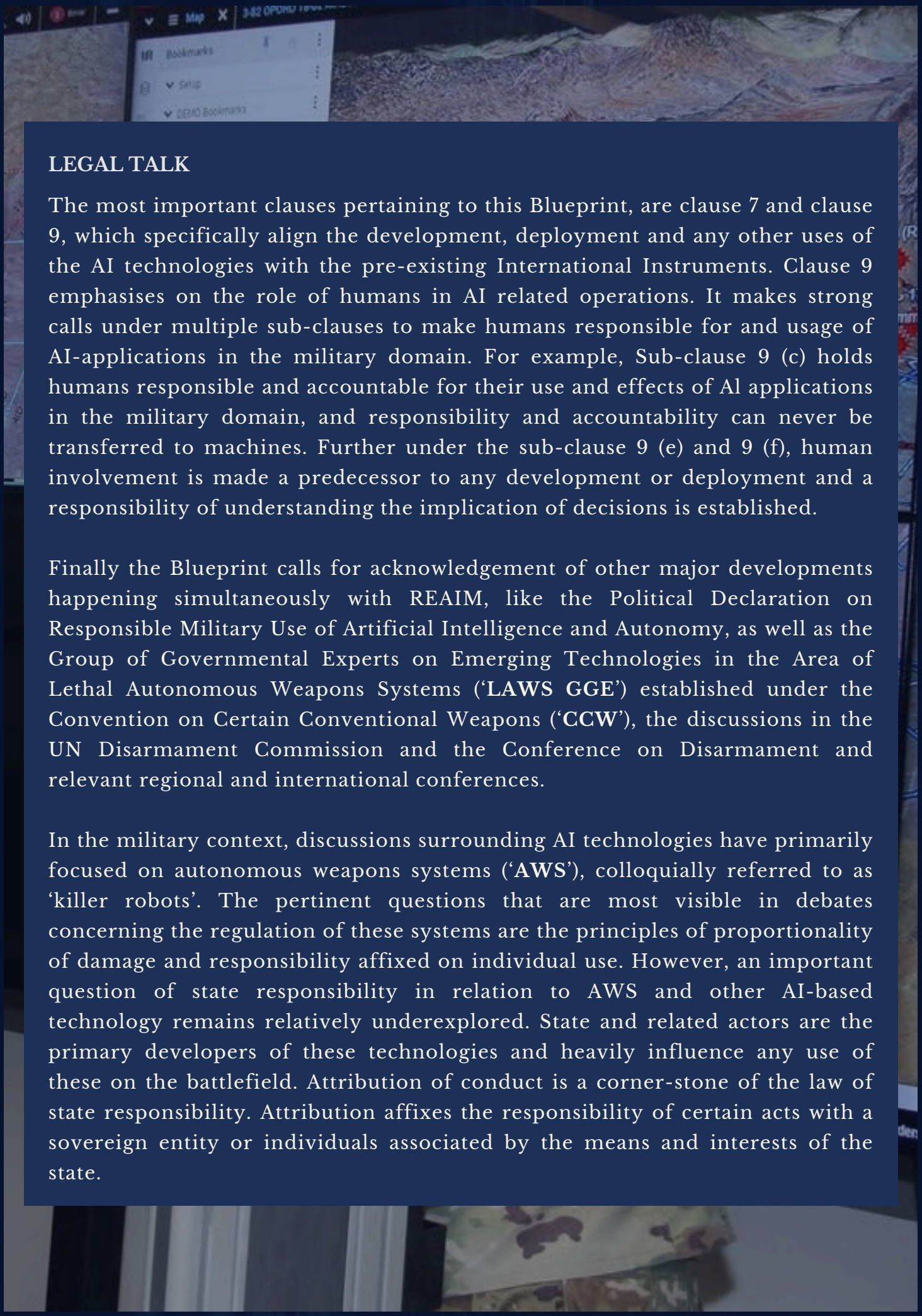
REAIM SEOUL BLUEPRINT: A DOORWAY TO INTERNATIONAL REGULATION IN MILITARY AI USE

NEWS

In the recently held second edition of the Responsible AI in the Military Domain ('REAIM') summit in Seoul, co-organized by the Republic of Korea's Ministry of Foreign Affairs and Ministry of National Defense, around 60 nations including the USA and multiple European nations endorsed a "Blueprint for action" in the domain, setting up traces of development by this non-binding document. China opted out of the same for unstated reasons. The two-day summit circled around the topic of AI use in military applications, focusing on general approaches, priorities, concerns, challenges, and prospects of international collaborations in developing responsible governance frameworks. In the event's conclusion, this Blueprint was laid out for endorsements, establishing non-binding norms for the responsible use of AI in military conflicts. The major calls for action pertained to the recognition of effects of AI in the military domain and importance of a consolidated framework. Further, the Blueprint sought application of these tools to be made according to applicable international laws like the UN Charter as well as regional instruments. Most importantly, the Blueprint calls for fixing the responsibility of AI use on human actors, vitiating the ambiguity created with ownership of thoughts in other domains.

INFLUENCE ON TECH COMPETITION

International laws have a set hierarchy of authorities that are binding based on consent and context. In all those authorities, such non-binding papers and blueprints, while the most feeble in the hierarchy, are significant because they are the stepping stone in this process which eventually leads to formation of a multilateral treaty that would be governing the domain. Soft laws like this lubricate the transition from a regulation-less regime to a solidified regime, especially in the context of rapid global changes and a decreasing consensus at the multilateral level. At the same time, such documents are criticised for a lack of specificity and consistency.



LEGAL TALK

The most important clauses pertaining to this Blueprint, are clause 7 and clause 9, which specifically align the development, deployment and any other uses of the AI technologies with the pre-existing International Instruments. Clause 9 emphasises on the role of humans in AI related operations. It makes strong calls under multiple sub-clauses to make humans responsible for and usage of AI-applications in the military domain. For example, Sub-clause 9 (c) holds humans responsible and accountable for their use and effects of Al applications in the military domain, and responsibility and accountability can never be transferred to machines. Further under the sub-clause 9 (e) and 9 (f), human involvement is made a predecessor to any development or deployment and a responsibility of understanding the implication of decisions is established.

Finally the Blueprint calls for acknowledgement of other major developments happening simultaneously with REAIM, like the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, as well as the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (‘**LAWS GGE**’) established under the Convention on Certain Conventional Weapons (‘**CCW**’), the discussions in the UN Disarmament Commission and the Conference on Disarmament and relevant regional and international conferences.

In the military context, discussions surrounding AI technologies have primarily focused on autonomous weapons systems (‘**AWS**’), colloquially referred to as ‘killer robots’. The pertinent questions that are most visible in debates concerning the regulation of these systems are the principles of proportionality of damage and responsibility affixed on individual use. However, an important question of state responsibility in relation to AWS and other AI-based technology remains relatively underexplored. State and related actors are the primary developers of these technologies and heavily influence any use of these on the battlefield. Attribution of conduct is a corner-stone of the law of state responsibility. Attribution affixes the responsibility of certain acts with a sovereign entity or individuals associated by the means and interests of the state.

The strict restriction of onus to human actors is an important step towards the development of soft law in this domain which would help minimise ambiguity in adjudication that has been seen in the case of other domains of law with relation to AI. For example, in the domain of copyright laws. The strict call for human responsibility displays the intent of a riddance sought from any ambiguity that can give benefit of doubt to an illegitimate actor. Such a clause could later be associated with important provisions like the article 8 of the UN Articles for responsibility of states for Internationally Wrongful Acts, which is relevant to the attribution of conduct to a state, wherein the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.

THE WAY FORWARD

Overall, the Blueprint laid out in Seoul marks a significant step towards the responsible use of AI in military contexts. The non-binding document emphasises human accountability in AI applications, aligning developments with international laws. As the framework evolves, it will help shape multilateral treaties, fostering global collaboration while ensuring ethical governance in military AI. Future efforts should focus on addressing state responsibility and refining legal norms for autonomous weapons systems, ensuring transparency and compliance with international legal instruments for sustainable military AI deployment.

CALIFORNIA PASSES NEW LAWS TO REGULATE AI-GENERATED DEEP FAKES

NEWS

California has passed new laws to regulate the use of AI-generated content; specifically targeting the use of deepfakes in elections and protecting actors from unauthorised use of AI replicas. Two other laws have also been passed that target the media industry and were backed by the Screen Actors Guild - American Federation of Television and Radio Artists. These legislative moves address the growing concern over AI misuse in media and politics, putting California at the forefront of AI regulation.

LEGAL TALK

India lacks a dedicated legal framework to address AI's role in political and electoral contexts. Current general laws, such as S.353 of the BNS have been amended from it's predecessor S.505 of the IPC, which addresses public mischief, to include the offenses committed "through electronic means," and Section 66 of the IT Act, which deals with 'computer-related offenses,' are general provisions may cover the issue of deep fakes within it's ambit. However, these laws are punitive measures rather than preventive, which leaves significant gaps in ensuring AI is used responsibly. Additionally, these laws do not target AI-related crimes but are rather fitted into it in lieu of an AI-specific legal framework.

In contrast, California has taken significant strides in regulating the use of AI, particularly in political content. Laws such as AB 2655 and AB 2355, enacted ahead of upcoming elections, aim to ensure transparency and prevent the misuse of AI-generated content that could manipulate voters. AB 2355 mandates that electoral advertisements using AI-generated or significantly altered content must disclose this fact. The Fair Political Practices Commission enforces these provisions, ensuring compliance through remedies available under the Political Reform Act- this establishes a robust mechanism for immediate intervention, thereby deterring potential offenders and providing immediate remedies. This is especially crucial during elections, where any delay in addressing misleading AI content can have dire consequences. Such preventive approach is key—rather than just penalizing offenders after the damage is done, the law seeks to curtail the misuse of AI at its inception.

The recent proposal for the Digital India Act (DIA) offers a glimmer of hope for more robust AI regulation in India. Bearing in mind that the IT act is unable to adapt to the rapidly changing tech sector, the proposed legislation should ideally address the gaps in the current system with the prevalence of AI use in today's cyber landscape. However, to be effective, the DIA must move beyond the broad, punitive measures of the current framework and adopt preventive mechanisms similar to those seen in California. With EU's AI Act, the world's first AI law that follows a risk-based regulatory model, serving as a reliable predecessor as well as the new Californian law- India has multiple sources for inspiration for the drafting of the legislation.

THE WAY FORWARD

As the applications of AI continue to evolve and broaden, it is crucial for India to adopt a proactive approach by implementing a comprehensive regulatory framework, like that of California and the EU, to address the challenges that come with AI misuse. This step taken by the California governors may also indicate a move towards the USA making a comprehensive AI act for the entire nation much alike to the EU; an opportunity that India shares with the forthcoming Digital India Act. By anticipating and mitigating AI risks, nations such as the USA and India can ensure transparency, protect individual rights and safeguard electoral integrity in the rapidly advancing technological landscape.

DATA PRIVACY

SECTION 5

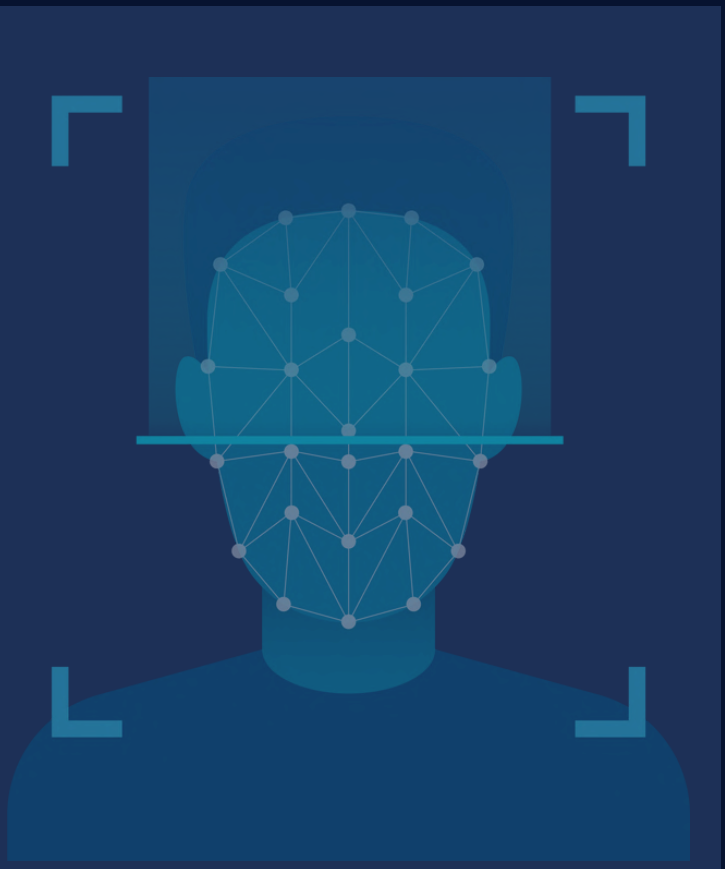
FACIAL RECOGNITION APP CLEARVIEW AI FINED BY DUTCH REGULATOR FOR CREATING 'ILLEGAL DATABASE'

NEWS

The Dutch Data Protection Authority imposed a fine of 30.5 million euros and ordered a penalty for non-compliance up to more than 5 million euros on facial recognition app Clearview AI under the General Data Protection Regulation ('**GDPR**'). Among other things, Clearview built an illegal database with billions of photos of faces collected from social media and the internet. This raises serious privacy concerns as there is no way for an individual to know that their photo is being used for such purposes as this is done without their consent.

LEGAL TALK

Facial recognition technology ('**FRT**') is a biometric identification technology. It can use facial features to recognize individuals in inputs (photographs, videos, or real-time feeds) through the use of both visible light and infrared waves. Among the multiple violations committed by Clearview, Article 9(1) of the GDPR specifically prohibits the processing of biometric data except in certain circumstances. In India, biometric data is defined and classified as 'sensitive personal data' in the Information Technology Rules, 2011, which will be replaced by the Digital Personal Data Protection Act ('**DPDPA**') once the rules are enforced. At present, the US is the only country that has taken active steps to either ban or curb the use of FRTs, although it is mostly limited to police use of the technology. By the end of 2020, around 18 cities had enacted laws forbidding the police from adopting the technology. One legislation that makes the use of FRTs by private companies without consent illegal is the Biometric Information Protection Act (BIPA) of 2008. The Indian media first reported about the potential use of FRTs in mid-2018 by the Unique Identification Authority of India, in the telecom sector. The last five years have seen an exponential, and most importantly, unregulated growth in the use of FRTs, especially by law enforcement and state agencies. Under the current data privacy regime, Data Fiduciaries may only process personal data for the certain legitimate uses as per Section 7 of the DPDPA. In this case, it is imperative to wait for the DPDPA rules to address biometric data specifically, since the Act does not mention it.



THE WAY FORWARD

Privacy advocates and public interest groups have long had concerns about the invasiveness of FRTs. Regulatory legislations in the tech sector in India are in a very nascent stage, especially considering the DPDPA is not operative in the absence of the rules. In the current technological landscape, it is essential for India to formulate policy approaches for tackling issues like FRT, in order to ensure effective digital privacy of its citizens.

ANALYSING AUSTRALIA'S NEW PRIVACY BILL

NEWS

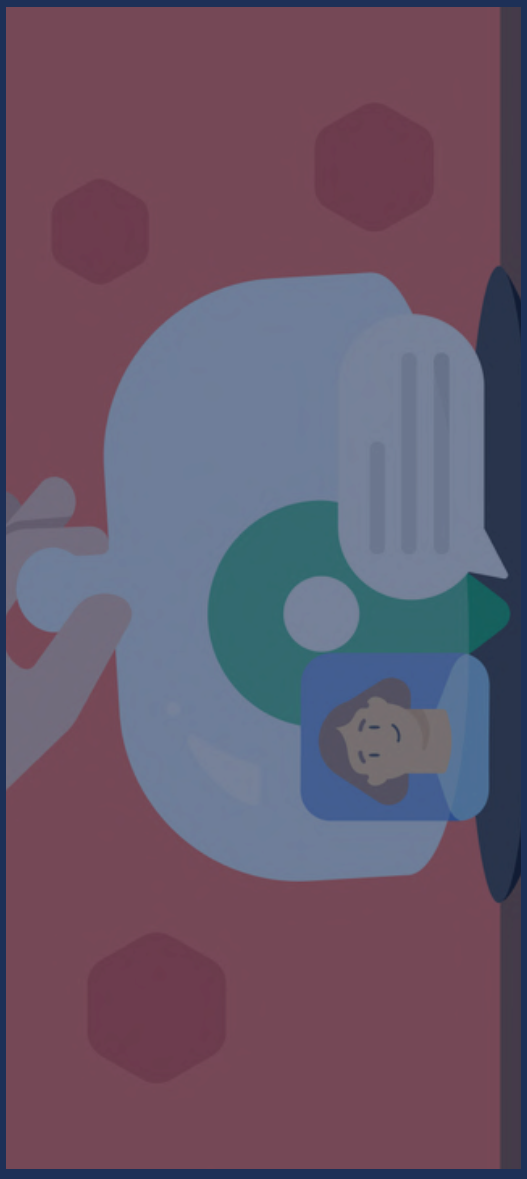
After nearly five years of review, Australia has introduced the first set of amendments to its Privacy Act through the Privacy and Other Legislation Amendment Bill 2024 (**'the Bill'**). This comes nearly a year after the Government's Response to the Privacy Act Review, which called for a generational overhaul of the Act. However, the reforms outlined in the Bill are much narrower in scope than initially anticipated.

LEGAL TALK

The current Privacy Act lacks a rights-based approach and instead strikes a pragmatic balance between the interests of data collectors and data subjects. Its key aim, though understated, is to offer privacy protection without imposing heavy regulatory burdens on businesses. As a result, there are significant carve-outs, such as exemptions for small businesses, employee records, and political parties, and the Australian Privacy Principles are filled with complex exceptions, making their application less robust. Compared to global standards, Australia's privacy laws are considered weak. This weakness is worsened by the lack of resources for the Office of the Australian Information Commissioner (**'OAIC'**), leading to poor enforcement and an inability to keep up with evolving data practices of platforms like Meta and Google. The broad definition of 'consent', which includes 'implied consent', allows businesses to argue that in certain contexts, the absence of an objection by individuals can be interpreted as consent. Furthermore, while explicit consent is required for 'sensitive information' (such as sexual orientation), a broader category — personal information (**'PI'**) includes data like credit information, employee records, and other details that can reasonably identify an individual. Although this personal information seems equally or even more important in certain contexts, it does not receive the same level of privacy protection as sensitive information. As such, Australia's privacy law urgently needed an overhaul to better protect personal privacy in the digital age, which was the main aim of the bill. Most of the amendments focus on filling these gaps. Schedule 1 of the Bill strengthens the enforcement powers of the OAIC and the courts, giving them broader enforcement options and new capabilities to address privacy violations.

A key feature is the introduction of a statutory tort for serious invasions of privacy, applicable to acts committed after the Bill's commencement. This tort outlines four elements for establishing a cause of action, including intrusion upon seclusion or misuse of personal information, reasonable expectation of privacy, intentional or reckless invasion, and the seriousness of the breach. The Bill also provides guidance on determining whether a privacy interference is "serious" by considering factors such as the degree of offence, distress, or harm to dignity caused and whether the defendant acted with knowledge or malice. There are exceptions for journalists and those assisting them in collecting or publishing journalistic material. The wide scope of these protections might allow them to evade accountability under the guise of journalistic work. Moreover, the shift towards online media has blurred the lines of what qualifies as 'journalistic material'. The term "serious" remains broad, and even with attempts to define it, disputes are likely to arise over what constitutes a serious invasion of privacy. The exclusion of harm caused by organisational negligence also limits recourse for individuals affected by privacy failures.

The Bill also introduces tiered civil penalties for privacy violations, marking progress toward accountability. However, simply having different penalty tiers may not serve as an effective deterrent. For these penalties to be truly effective, they must be paired with strong mechanisms that allow individuals to correct, delete, or regain control over their personal data after a breach. Laws like the GDPR and DPDPA grant individuals these rights, giving them more authority over their personal data. Similar provisions in Australia could better empower individuals. The Bill mandates greater transparency in how personal information is used by automated decision-making systems. Companies must now publish updated privacy policies specifying the PI they are collecting and processing. Unlike the DPDPA, where the request for consent has to be accompanied by a notice informing its purpose, here there is a greater focus on notification rather than obtaining *informed* consent. This approach risks treating consent as a mere formality, where users are informed after the fact rather than actively engaged in the decision-making process. The absence of a "fair and reasonable" test for handling personal information enables businesses to exploit vague consents, potentially using data in ways that individuals may not fully understand or agree to. A key oversight is not removing the small business exemption, leaving 95% of Australian businesses outside privacy laws. This creates a significant gap in consumer protections as small businesses increasingly handle personal data.



The Bill unexpectedly introduces amendments to the Criminal Code, creating new offences to target ‘doxxing’. It is defined as publishing an individual's name, image, and phone number online while encouraging others to send violent or threatening messages. This enhancement of legal protections is crucial in an age where personal data can be easily disseminated online, ensuring that individuals can maintain their privacy and safety in both digital and real-world interactions. DPDPA is significantly more comprehensive than Australia's current legislative framework, providing robust protections for personal data and clearer guidelines for consent. A key feature of the DPDPA is its emphasis on user empowerment, granting individuals greater control over their information through explicit consent requirements and the right to access and rectify their data. On the other hand, Australia's decision to criminalise doxxing is an approach that India could consider integrating into its own legal framework.

THE WAY FORWARD

The proposed reforms are less comprehensive than expected, focusing on "quick wins" instead of addressing complex issues the Government had only agreed to in principle. Despite being the first tranche of reform, the government has missed an opportunity to address existing loopholes, such as clarifying the definition of consent. Delays are likely for the second tranche and for developing provisions like the children's privacy code. Even if these elements take time, greater clarity on the Bill's provisions and its grey areas is essential. Still, these reforms are a positive step forward, laying the groundwork for future privacy protections and showing a commitment to addressing key issues.

CONTRIBUTORS

WRITERS

ANJALI PANDE

TRISHNA AGRAWALLA

PRATYUSH SINGH

KALYANI KIRAN

ANANYA SONAKIYA

ARUNIMA RAMAN

MAITHILI DUBEY

BHAVYA BHASKAR

ALOK SINGH MOURYA

ANUSHKA GUHA

EDITORS

HARSH MITTAL

LAVANYA CHETWANI

DESIGNERS

TRISHNA AGRAWALLA

SUBHASIS SAHOO

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL