LEXTECH

NOVEMBER 2023
EDITION

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

SECTION 1

INFORMATION AND BROADCASTING MINISTRY RELEASES DRAFT BROADCASTING SERVICES BILL FOR PUBLIC CONSULTATION

NEWS

The Information and Broadcasting Ministry ("I&B"), Government of India has released a draft Broadcasting Services Bill to replace the Cable Television Networks (Regulation) Act, 1995. The proposed bill has widened its scope to include terrestrial and internet broadcasting networks.

LEGAL TALK

In an effort to modernize the regulatory landscape for digital media, the proposed bill seeks to extend oversight to digital news and OTT content, currently governed by the IT Rules, 2021. The preceding act, tailored solely to television and cable broadcasting services, was rendered obsolete by the advent of contemporary platforms like social media and OTT services. Recognizing this shift, the new bill introduces Content Evaluation Committees ("CECs") under Section 24(2), fostering self-certification. Composed of diverse representatives from various social groups, including women, child welfare, scheduled castes, scheduled tribes, and minorities, CECs will serve as content evaluators. Additionally, they will address grievances, hear appeals filed by complainants regarding content, and issue advisories to members to ensure compliance with the rules.

THE WAY FORWARD

The proposed bill seeks to modernize the regulatory framework for the broadcasting sector, streamlining outdated laws into a unified approach. While streamlining regulations is commendable, the requirement for CECs to include diverse individuals may strain OTT platforms, especially considering their foreign content licensing, now subject to CEC scrutiny. This could impact platforms and user experience.Additionally, the bill's ambiguous language regarding content restrictions raises concerns about authorities' discretionary power to prohibit content, potentially leading to government control over digital services.

CENTRE TELLS SOCIAL MEDIA PLATFORMS TO DISCUSS WAYS TO COMBAT THE RISING THREAT OF DEEPFAKES.

NEWS

Amidst growing concerns over the proliferation of deepfakes, the Central Government is set to summon major social media platforms to discuss strategies for mitigating the threat posed by these manipulated videos. This move comes in the wake of a deepfake video of renowned actress Rashmika Mandana that recently went viral.

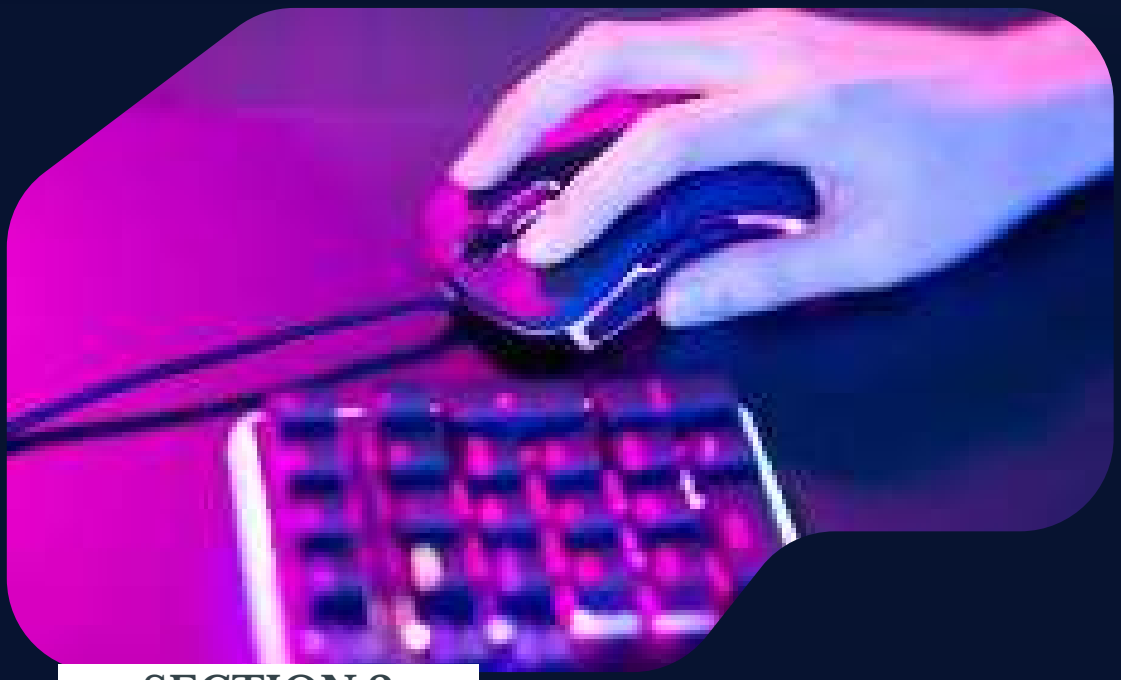
LEGAL TALK

A deepfake is an image, a video, or an audio recording that has been edited using an algorithm to replace the person in the original with someone else. To deal with such technologies from a regulatory standpoint, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules") mandate specific compliance requirements and safeguards for social media platforms. Messaging platforms must enable the identification of the first originator of content upon a judicial order, facilitating tracking of potential deepfake uploaders. Additionally, social media platforms are obligated to remove any content reported as a deepfake within 36 hours, and failure to do so renders the platform liable for the deepfake content. Further discussions are warranted to enhance and strengthen these measures against the evolving threat of deepfakes.

THE WAY FORWARD

Addressing the challenge of deepfake detection requires a crucial dialogue between the government and social media platforms. Limited identification tools complicate this issue, but social media can leverage artificial intelligence for detection. To enhance this effort, legal procedural reforms are necessary, streamlining authentication processes for digital evidence in deepfake or artificial intelligence cases. Legislatures and courts should further establish forensic standards and provide training for legal professionals handling cases focused on the authenticity of digital content.

Online Gaming and Betting Laws



SECTION 2

MADRAS HIGH COURT RULING: TN ONLINE GAMING ACT UPHELD WITH EXEMPTION FOR RUMMY, POKER, AND SKILL-BASED GAMES

NEWS

The Madras High Court ("HC") upheld the Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Act, 2022 ("Act"), but clarified that its prohibitions only apply to games of chance, not games of skill like poker and rummy. The court reasoned that prohibiting games of skill falls outside the legislative purview of the Act, and the regulation of such games is the appropriate course of action.

LEGAL TALK

The Act imposes a ban on online games, failing to distinguish between games of skill and games of chance. The HC underscored the state's justification for the Act, namely that online games pose a threat to the mental and physical well-being of individuals, particularly those under the age of 18. While acknowledging public health as a legitimate concern within the state government's purview, the HC emphasized the need for pragmatic regulatory measures rather than a sweeping ban on all online games. Addressing the state's apprehension regarding public order maintenance, the HC adhered to the established stance that public order in the State List pertains to activities that would disrupt or affect the public at large. In the present case, the HC dismissed this concern, citing a lack of evidence to support the claim that public order has been disturbed.

THE WAY FORWARD

Marking a pivotal moment for the online skill gaming industry, the HC's order stands as a beacon of hope for establishing Tamil Nadu's online skill gaming jurisprudence. The HC's emphatic declaration that an outright ban on games of skill, regardless of whether they involve real-money stakes, is both unreasonable and unconstitutional, sets a positive precedent. Further solidifying the industry's legitimacy, the HC upheld the constitutionality of online gambling operators charging a fixed service fee, provided they refrain from taking a share of players' winnings. This progressive order paves the way for further growth and legitimization of the online skill gaming sector.

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (“MEITY”) CRACKS DOWN ON 22 ILLEGAL BETTING APPS AND BLOCKED WEBSITES

NEWS

The Ministry of Electronics and Information Technology (“MEITY”), issued blocking orders against 22 illegal betting apps and websites. This action stems from the Enforcement Directorate's (“ED”) extensive investigations and raids under the Prevention of Money Laundering Act 2002 (“PMLA”) against organized syndicates operating illegal betting apps offering a plethora of live games, including card games like poker, cricket, football, badminton, tennis, and other sports-based wagering platforms.

LEGAL TALK

The government derives its authority to restrict access to these applications and websites from Section 69A of the Information Technology Act, 2000 (“IT Act”). This provision empowers the central government to curtail the operation of any website or application that infringes upon the sovereignty and integrity, defence, security of the State, friendly relations with foreign States, and public order. The apps and websites in the present situation were facing charges under Section 19 of the PMLA for their involvement in offenses related to money laundering.

THE WAY FORWARD

The initiatives undertaken by MeitY underscore its commitment to fostering a secure online environment and advocating responsible online gaming practices. These measures serve as a deterrent against the promotion of illegal betting apps and games that may have detrimental societal effects. Such steps contribute to maintaining a public space devoid of exploitative apps, fostering the growth of platforms that align with India's legal provisions and are utilized by individuals in a lawful manner.

DELHI HIGH COURT ASSERTS GOVERNMENT'S RIGHT TO REGULATE ONLINE GAMING

NEWS

The Delhi High Court ("HC") has affirmed the Union Government's legislative authority to regulate online gaming, upholding the Centre's stance in response to a petition challenging the validity of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 ("IT Rules").

LEGAL TALK

The IT Rules introduced regulatory measures for online gaming, which were challenged through a petition questioning the Centre's legislative authority over online gaming, considering gambling and betting fall under the jurisdiction of state governments. However, the court, aiming to protect vulnerable youth across the country, ruled that the Centre can indeed regulate online gaming.

In its decision, the court invoked Article 249 of the Indian Constitution, which empowers the Union to enact legislation within the state list if it secures a two-thirds majority in the upper house of Parliament. Additionally, Article 19(1)(g) grants the Union the right to oversee the online gaming industry, while Article 19(6) empowers the Union to regulate an occupation if it poses a threat to public interest or is deemed unlawful. Furthermore, Entry 42 of the 7th Schedule authorizes the Union to regulate trade between states pertaining to online gaming, Rule 4A(2)(d) of the IT Rules mandates that the governing body for regulating online gaming must be an autonomous body composed of representatives from various stakeholders and have an Appeal Committee to address appeals.

THE WAY FORWARD

The decision to uphold the central government legislative authority over online gaming, as per Entry 31 and Entry 97 (residual entries) of the Union List, contrasts with the state's jurisdiction over gambling and betting in the State List. This duality allows the centre to combat illegal online gambling and betting across states. However, the potential for misuse arises, as the central government's decision-making power might be exploited for its own benefit, presenting a nuanced, double-edged scenario.

FinTech

SECTION 3

THE RESERVE BANK OF INDIA ("RBI") ISSUES DRAFT FRAMEWORK FOR FINANCIAL OUTSOURCING

NEWS

According to the sources, the Directorate General of GST Intelligence ("DGGI") has written 12 pre-show cause notices to online real money gaming (RMG) organisations about GST obligations totaling nearly Rs 55,000 crore. These include what may be the biggest indirect tax notice ever served in the nation, a GST notice for over Rs 25,000 crore sent to the fantasy sports platform Dream11. The entire GST demand from RMG was raised by DGGI, and additional notices are anticipated in the upcoming weeks. The notices were sent out as a result of the recent change in GST rates for real money games, which raised the fee for each gaming session on RMG platforms from 2% to 28% of the entire bet.

LEGAL TALK

'Outsourcing' as defined in paragraph 4.2 of the RBI-MD refers to an RE using a third party (either an affiliated entity within a group or an external entity) to perform activities that would normally be undertaken by the RE itself on a continuing basis, now or in the future. Through these draft RBI-MD, the central bank strives to consolidate the regulatory compliances for REs with respect to financial outsourcing. The RBI-MD differentiate between material and non-material functions for the purpose of outsourcing arrangements; and state that these guidelines would apply only to the former. Material arrangements are defined as those that, if breached, could significantly affect an RE's business operations, reputation, profitability, customer service or its ability to handle risks and follow laws and regulations. Let us understand some of the key provisions in more detail:

(i)Regulatory and Supervisory Requirements and Role of REs

REs engaging in outsourcing must comply with applicable laws, conduct due diligence on service providers, and maintain control over outsourced activities. REs are responsible for ensuring service providers uphold high standards and refrain from compromising internal controls or reputation. They must maintain an inventory of outsourced services and periodically evaluate relevant information. REs bear responsibility for the actions of service providers and their sub-agents. Further, they must establish a robust grievance redressal mechanism for outsourced financial services, which cannot be outsourced.

These requirements aim to ensure responsible and compliant outsourcing practices. Assessing service providers helps REs maintain their standards and reputation. By establishing a dedicated mechanism for addressing customer complaints related to outsourced financial services, REs can proactively identify and resolve issues, safeguarding customer interests and protecting their reputation.

(ii) Risk Management Practices for Outsourcing

The RBI-MD mandates that REs implement a comprehensive board-approved outsourcing policy. REs must meticulously evaluate outsourcing risks, including compliance, contractual, and strategic risks. Outsourcing agreements must be carefully defined and documented in writing. Maintaining customer data confidentiality and security is paramount, and service provider access to information should be restricted to a "need-to-know" basis. Additionally, REs must require service providers to develop and implement robust frameworks for documenting, maintaining, and testing Business Continuity and Recovery Procedures.

THE WAY FORWARD

These provisions reflect RBI's forward-looking approach. Regular testing emphasizes the importance of preparedness for potential disruptions across various scenarios. The mandated Board-approved outsourcing policy and thorough risk evaluation ensure informed outsourcing decisions. RBI's emphasis on data privacy and security is evident in the "need-to-know" approach. Harmonizing regulations across REs is a positive step towards a stable financial system. Uniform regulations will provide REs with a centralized repository of current outsourcing guidelines for financial services. The RBI has aligned the Proposed Master Directions with existing outsourcing guidelines for financial services, adhering to the Basel Committee’s Report on Financial Outsourcing 2005 and international risk management standards.

RBI NOTIFIES NEW INFORMATION TECHNOLOGY (“IT”) GOVERNANCE AND CYBERSECURITY GUIDELINES

NEWS

The Reserve Bank of India (“RBI”) has recently issued the final Master Direction on IT Governance, Risk, Controls, and Assurance Practices (“Directions”), which will be applicable to banks and non-banking financial institutions (“NBFCs”), excluding Local Area Banks and NBFC-Core Investment Companies. Foreign banks operating through branches in India are subject to a 'comply or explain' approach, allowing them to deviate from specific directions provided they obtain RBI's approval with a well-reasoned explanation.

LEGAL TALK

(i) Emphasizing Resilience in IT Services Management

The Directions mandate that Regulated Entities (“REs”) implement a robust IT Service Management Framework to support their information systems and infrastructure, ensuring the operational resilience of their entire IT environment. Additionally, REs must ensure that their information systems and infrastructure can support business functions and guarantee the availability of all services (Capacity Management). Furthermore, the Directions emphasize the need for a documented data migration policy outlining a systematic process for data migration, safeguarding data integrity. In light of rising cyber and IT fraud, the RBI has also stressed the importance of IT applications possessing the necessary audit and system logging capabilities to generate audit trails.

These provisions, by emphasizing the significance of robust IT infrastructure, data management, and security practices, underscore the criticality of maintaining a secure and resilient IT environment to minimize the likelihood of cyber-attacks and fraud. Comprehensive audit trails will facilitate traceability, aligning with the broader objective of strengthening the security and reliability of financial systems.

(ii) Proactive Stance on Risk Management

REs are obligated to conduct periodic reviews of their IT-related services. Additionally, they must implement a comprehensive Information Security Management function, along with robust internal controls and processes, to effectively mitigate and manage identified risks. Moreover, REs are mandated to establish and implement an Information Security Policy, a Cyber Security Policy, and a Cyber Crisis Management Plan.

These provisions underscore the importance of vulnerability assessments and mandate the establishment of a Cyber Incident Response and Recovery Management policy. This policy ensures that regulated entities possess the necessary capabilities to effectively handle cyber incidents. The policy should encompass a clear communication strategy and plan to effectively manage such incidents, limit potential exposures, and achieve timely recovery.

(iii) Ensuring Continuity and Recovery

According to the Directions, REs are obligated to establish a Business Continuity Plan and Disaster Recovery policy. These guidelines aim to reduce the likelihood or impact of disruptive incidents and ensure business continuity. The policy requires regular updates based on major developments and risk assessments. Implementation of these policies yields benefits such as reduced disruption likelihood, minimized impact, heightened business resilience, and increased customer satisfaction, emphasizing the importance of readiness through routine exercises and resilience testing.

(iv) Audits for Assurance

The REs' just establish the Audit Committee of the Board (ACB) which would be responsible for exercising oversight of Information Systems Audit. The directions also require REs to come up with an Information Systems Audit Policy which should be renewed at least annually. The Board will ensure an independent review mechanism to uphold the integrity of the IT and cybersecurity framework will also ensure its continuous improvement

THE WAY FORWARD

The Directions position will serve as a vital compass, enabling REs to navigate the intricate terrain of IT governance, risk management and operational resilience. The standardized approach is set to usher in an era of enhanced cybersecurity resilience within the Indian financial ecosystem. This will likely foster increased investor confidence and consumer trust in the digital infrastructure of financial institutions.

TIGHTENED REGULATORY MEASURES FOR CONSUMER CREDIT

NEWS

The Reserve Bank of India ("RBI") has recently issued a notification outlining regulatory measures targeting consumer credit and bank credit to non-banking financial companies ("NBFCs"). This move aligns with the RBI's earlier emphasis on the need for banks to bolster their surveillance mechanisms and implement appropriate safeguards in their best interests, given the increasing volume of consumer credit.

LEGAL TALK

The RBI has implemented revised risk weight regulations aimed at enhancing the stability of the financial sector by increasing the capital requirements for specific credit categories. Risk weights, assigned based on the perceived riskiness of different asset classes, determine the regulatory capital that financial institutions must hold against such exposures. Notably, consumer credit now attracts a risk weight of 125%, up from the previous 100%. Similarly, credit card receivables of NBFCs will now carry a risk weight of 125%. Additionally, loans provided by banks to NBFCs will be subject to a 25% increase in risk weighting, except for those already at 100%.

These increased risk weights necessitate that lenders allocate more regulatory capital to cover potential losses associated with these exposures. The move is strategically designed to mitigate emerging risks in these segments and reduce NBFCs' reliance on bank lending. NBFCs may experience two primary consequences: firstly, they will need to set aside more capital for unsecured lending, and secondly, banks lending to them will also have to increase their capital buffers, leading to a higher cost of capital.

THE WAY FORWARD

The implementation of guidelines aimed at curbing the rapid growth of credit cards and unsecured personal loans represents a positive step towards promoting financial stability. However, the associated increase in risk weights will inevitably impact lenders' capital adequacy ratios, necessitating the allocation of more capital to support these exposures.

ARTIFICIAL INTELLIGENCE

SECTION 4

FLIPKART FOUNDER LAUNCHES AI OUTSOURCING START-UP

NEWS

The co-founder of the e-commerce platform Flipkart, Benny Bansalhas started a new venture offering AI-as-a-service ("AIaas"). This innovative approach allows companies to efficiently explore and scale AI techniques at minimal costs. Many businesses are increasingly adopting this approach to unlock the potential of artificial intelligence, making it a rapidly growing segment in the tech industry.

LEGAL TALK

The utilization of AI through AIaaS platforms, akin to intellectual property outsourcing, entails the disclosure of confidential information to the businesses employing AI. This practice elevates the risk of patent infringement, particularly when the AI developer shares proprietary information with multiple companies. The potential for these companies to independently utilize AI systems derived from the developer's work for their own commercial gain poses a significant threat of patent infringement under the Patents Act, 1970. The absence of specific AI-related patent laws further complicates this issue, leading to varying interpretations of the applicability of existing patent laws in this domain.

THE WAY FORWARD

In the "AI for All "report, the Niti Aayog has stressed on the importance of harnessing AI's full potential. Furthering these goals, Outsourcing AI shall help companies utilise AI at a minimal cost, by improving customer experiences and automating redundant tasks. However, companies have to comply with patent laws until specific regulations for using AIaaS are released in order to ensure market transparency.

AI SAFETY SUMMIT IN THE UK

NEWS

A significant breakthrough occurred at the UK's AI Safety Summit ('Summit') as 28 governments and leading AI companies committed to subjecting advanced AI models to safety tests before release. The urgency stemmed from the rapid improvement of advanced AI systems and the potential risks they pose.

LEGAL TALK

The advent of self-learning AI tools has necessitated a thorough understanding of liability attribution in instances where AI actions contravene legal norms. Two potential entities bear the brunt of liability in such scenarios: the AI developer and the AI tool itself. This ambiguity has impeded the widespread adoption of AI technologies. Consider a hypothetical scenario where an AI tool commits a criminal offense. The AI tool, lacking personhood, cannot be held liable for its actions. Simultaneously, the AI developer cannot be held accountable due to the absence of mens rea (criminal intent) in the commission of the offense. However, the Summit has endeavoured to dispel this uncertainty by clarifying that liability will be imposed on the AI developer in such circumstances and similar situations. This clarification serves as a crucial step towards fostering responsible AI development and promoting the ethical utilization of AI technologies.

THE WAY FORWARD

AI continues to revolutionize various industries, ensuring AI safety and upholding human rights have emerged as paramount concerns. The current Indian legal framework falls short in adequately addressing these concerns. However, the AI Safety Summit has taken a significant step towards addressing this gap by highlighting the need for comprehensive AI regulations. India should now prioritize the enactment of specific laws that effectively regulate AI across various domains, thereby safeguarding human rights and ensuring responsible AI development and deployment.

NEW GUIDELINES FOR SECURE SYSTEM AI DEVELOPMENT

NEWS

UK's National Cybersecurity Centre ('NCSC') and US Cybersecurity Infrastructure Security Agency ('CISA') have developed the first global agreement on AI safety. The Guidelines for Secure system AI development ('Guidelines') focus on four key areas within the AI system development life cycle: secure design, secure development, secure deployment, and secure operation and maintenance.

LEGAL TALK

The aforementioned guidelines aim to address critical issues such as manipulated outcomes and unauthorized data usage. They emphasize the responsibility of AI developers to implement robust tracking and monitoring mechanisms for prompts and verify the authenticity of outcomes. The proposed Digital India Act, 2023 promotes the utilization and development of AI technology. However, the widespread adoption of safe AI systems can only be achieved if these or similar guidelines are integrated into the Indian legal framework. Additionally, in line with the Information Technology Act, 2000, the Guidelines establish the AI developer's accountability for ensuring safe AI usage. While the current Indian legal framework remains silent on AI regulation, the new DPDP Act, 2023, introduces data protection policies that safeguard individual rights.

THE WAY FORWARD

They prioritise taking ownership of security outcomes for customers which help in safe development of AI, in accordance with 'secure by design principles' published by CISA. The implementation of these guidelines will empower providers to construct AI systems that function as intended, remain accessible when required, and operate without divulging sensitive data to unauthorized parties.

DATA PRIVACY

SECTION *5*

CYBERSECURITY FIRM REPORTS LEAK OF PERSONAL DATA OF MILLIONS OF INDIANS

NEWS

In a recent report, US cybersecurity firm Resecurity claims that the dark web has exposed personal data of approximately 815 million Indians, including names, phone numbers, a adhaar, and passport details, all available for sale online. There are suspicions that the Indian Council of Medical Research("ICMR") is the source of the compromised data. Analysts in this sample leak ensured the validity of the IDs from the 'Verify Aadhaar' feature of the central government.

LEGAL TALK

Various stakeholders, including service providers, intermediaries, data centres, corporate entities, and government organizations, bear the responsibility of undertaking specific actions or providing information for cyber incident response, as well as implementing protective and preventive measures to mitigate cyber threats. In accordance with Section 70(B) of the Information Technology Act 2000, the Indian Computer Emergency Response Team ("CERT-In") functions as the National Nodal Agency, establishing guidelines for monitoring, detecting, preventing, and managing cybersecurity incidents. CERT-In has developed comprehensive frameworks to identify and minimize the occurrence of cyber-attacks. However, its most prominent role lies in addressing the aftermath of cybercrime, involving the assessment, handling, and response to the damage caused.

THE WAY FORWARD

India's current legislative approach primarily reacts to cybersecurity breaches rather than proactively preventing them. Although CERT-In guidelines provide foundational advice for enhancing security, they lack specific solutions. The absence of an enforcement mechanism allows platforms to implement measures without validation, creating a critical gap in ensuring cybersecurity effectiveness. CERT-In should expand its role beyond offering basic cybersecurity tips and concentrate on establishing comprehensive, industry-specific security standards. Mandating companies to meet these standards can cultivate a proactive cybersecurity culture, ensuring preparedness against potential breaches. Learning from foreign legislations, such as Germany's BSI law, which enforces binding minimum standards on federal authorities, can provide valuable insights for regular validation and adherence to established standards—a pivotal step in preventing cyber threats.

LEGAL TALK

Ransomware, a malicious software variant, infiltrates systems, rendering them inoperable by encrypting vital files or locking the screen. This cyberattack demands a ransom payment for restoration of access and threatens to sell or expose extracted sensitive data if payment is not made. Such actions constitute various offenses under the Indian Penal Code, including criminal conspiracy and extortion. Relevant provisions of the IT Act, 2000 encompass damaging computer systems and tampering with source code. Furthermore, this attack infringes upon the fundamental right to privacy, enshrined under Article 21 of the Constitution of India. The Computer Emergency Response Team – India (CERT-In) has issued comprehensive guidelines for containing and recovering from such attacks. These guidelines cover essential aspects of cybersecurity and include measures to prevent, detect, and respond to ransomware attacks effectively

SENSITIVE DATA FROM BOEING PUBLISHED BY CYBERCRIMINAL GROUP LOCKBIT

NEWS

A cybercriminal group, Lockbit, recently exposed internal data from Boeing, a major player in defence and space. The hackers seized data and demanded a ransom for non-disclosure. Boeing declined cooperation and payment, leading to the exposure of sensitive data which includes backups for IT management software configurations and logs for monitoring and auditing tools. Lockbit, with a history of over four years, has targeted numerous sectors, including the international law firm Allen & Overy.

THE WAY FORWARD

Effective implementation of current guidelines hinges on organizations adapting to evolving threats. The surge in ransomware attacks amid business digitization necessitates urgent legislation in India, as there is currently no specific law addressing ransomware. In contrast, the European Union's Data Protection Board provides comprehensive guidelines categorizing ransomware attacks and prescribing detailed mitigation steps, offering a more comprehensive approach than India's current framework. To enhance resilience, India can collaborate with experts and establish a standardized reporting and response mechanism for ransomware incidents, mirroring the EU's model.

DEVICE SEIZURE RULES IN BNSS

NEWS

The Bharatiya Nagarik Suraksha Sanhita Bill, 2023 ("BNSS") seeks to replace the Code of Criminal Procedure, 1973 ("CrPC"), with the aim of shedding colonial vestiges and introducing a series of amendments.

LEGAL TALK

Section 94 of the BNSS empowers the court or the presiding police officer to summon any document or item for investigation, expressly including digital evidence such as messages, call recordings, and emails, as well as electronic devices such as mobile phones and laptops. The government may further specify additional electronic devices through future notifications. While the digitization of India's legal system is generally perceived positively in light of the growing reliance on electronic systems, caution must be exercised during this transition to avoid potential pitfalls. The broad authority to summon any electronic device, coupled with the absence of specific safeguards, raises concerns about the potential for accessing personal information unrelated to the investigation, thereby potentially jeopardizing the fundamental right to privacy as upheld in the landmark judgment of KS Puttaswamy. Furthermore, the BNSS lacks provisions for maintaining a proper chain of custody for digital records, a crucial safeguard present in the criminal laws of developed countries such as the USA and the UK.

THE WAY FORWARD

Unbridled authority to summon electronic devices without safeguards jeopardizes public trust in law enforcement. Insufficient safeguards risk evidence integrity, leading to unjust legal proceedings and impinging on citizens' digital activities. This vulnerability heightens the risk of discriminatory practices, exacerbating social inequalities. To rectify this, clear limitations on authority, criteria for specifying additional devices, and robust chain-of-custody protocols are recommended. These measures aim to protect against evidence tampering and reduce the risk of violating the right to privacy.

CONTRIBUTORS

DESIGNERS

SAMRIDHI BAJORIA

NAMAN OSTWAL

WRITERS

LAVANYA CHETWANI

ANJALI PANDE

TRISHNA AGRAWALLA

KUSHAL AGRAWAL

UTSAV BISWAS

EDITORS

NIKHIL JAVALI

HARSH MITTAL

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL