emerging tech decoded

LEX CONSULT EDITORIAL

BYTE/WISE

KEY HIGHLIGHTS

NOV 2025

Privacy

Regulatory Updates

- Final Digital Personal Data Protection Rules, 2025 Notified
- WhatsApp–Meta Case Highlights DPDP-Era Consent Risks
- EU Considers Major GDPR Reforms Under "Digital Omnibus"
- California Introduces Personal Accountability for Privacy, Cybersecurity and AI Compliance

Clause in Focus - Data retention and deletion
Compliance Snapshot - Personal Data Breach
Knowledge Corner - (Explicit) Consent versus Deemed Consent

Artificial Intelligence

Regulatory Updates

- India proposes amendments to Tackle AI-Generated Content
- India releases AI Governance Guidelines
- Croatia Proposes to Criminalize AI Endangerment
- California's enacts robust new AI Laws
- European Commission Reports on GPAI Regulation
- Reddit's Case Against Perplexity

Clause in Focus - Human oversight and explainability
Compliance Snapshot - Platform duties under Indian IT Rules
Knowledge Corner - Provider versus Deployer

Digital Assets

Regulatory Updates

- Cryptocurrency recognized as 'Property' under Indian Law
- RBI to Pilot Certificate of Deposit Tokenization
- EU Moves Toward a Single Supervisor for Crypto Exchanges.

Clause in Focus - Segregation & safeguarding of Client Assets
Knowledge Corner - Tokenization of Real-World Assets

Dark Patterns Check – False Urgency

BYTE/WISE

PART ONE

PRIVACY

NOV 2025

Privacy / REGULATORY UPDATES

Final Digital Personal Data Protection Rules, 2025 Notified

The Government of India has notified the final Digital Personal Data Protection (DPDP) Rules, 2025 (**Final Rules**), setting a clear 18-month compliance runway. While most provisions remain consistent with the earlier draft, a few important refinements stand out.

Material New Additions:

- A new minimum retention obligation: Mandatory retention of personal data, traffic data and processing logs for at least 1 (one) year, unless a longer period applies under other specific laws.
- A defined 90-day cap for grievance redressal: Data Fiduciaries and Consent Managers must resolve grievances within a strict 90-day limit.
- A new definition of "techno-legal measures" in the context of virtual hearings, remote participation, authentication for proceedings, and other measures that allow adjudicatory functions to be conducted without requiring physical presence.
- Tightened and more precise definitions across the Rules: Notably, the definition of "social media intermediary" is referred to and aligned with the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, providing regulatory consistency.

Phased implementation approach: The final Rules adopt a structured, staggered rollout, allowing organizations time to operationalize their compliance programs.

- Phase 1 (Immediate): Setting up of adjudicatory and regulatory machinery such as the establishment of the Data Protection Board.
- Phase 2 (within one year): Integration of the Consent Manager ecosystem.
- Phase 3 (Within 18 months): Full organizational compliance, covering notices, consent flows, retention–deletion systems, vendor governance, cross-border controls and request-handling protocols.

The Final Rules provide clarity, sequencing and a predictable transition period, enabling organizations to operationalize compliance with the Digital Personal Data Protection Act ("DPDP Act") in a structured, prioritized manner.

BYTE/WISE

WhatsApp–Meta Case Highlights DPDP-Era Consent Risks

The National Company Law Appellate Tribunal (NCLAT) has partly upheld the Competition Commission of India's (CCI) order against Meta Platforms in relation to WhatsApp's 2021 privacy policy update, which required users to accept data sharing with Meta group entities as a condition for continued service.

While the NCLAT lifted the operational ban on data sharing, it sustained the ₹210-crore penalty, finding that WhatsApp's consent design amounted to an abuse of dominance by depriving users of meaningful choice. The tribunal's reasoning underscores concerns now formalized under the DPDP Act. The CCI's focus on "forced consent" aligns with DPDP principles of specific, free, and informed consent under Section 6, and the purpose limitation requirement under Section 5. Had the DPDP Act been operational then, WhatsApp's bundled-consent model would likely have attracted regulatory scrutiny for failing to provide users with granular control over data sharing.

With Final Rules announced, digital platforms should review whether their consent and data-sharing workflows truly allow users to make independent, purpose-specific choices through layered notices, opt-in structures, and transparent disclosures.

EU Considers Major GDPR Reforms Under "Digital Omnibus"

Leaked European Commission documents indicate that the General Data Protection Regulation (GDPR) could undergo its first substantial revision since 2018 as part of the forthcoming "Digital Omnibus" package, expected to be introduced in late 2025. The draft proposal suggests a re-balancing of privacy and innovation priorities, with key changes reportedly under consideration: narrowing the definition of "personal data" to exclude information that can identify individuals only through disproportionate effort, easing record-keeping and access obligations for small and medium enterprises and introducing an additional legitimate-interest ground for limited AI-training purposes.

These proposals follow the Court of Justice of the European Union's SRB ruling, which reaffirmed a "relative" approach to personal data where it was held that information counts as personal only if the data recipient has realistic means of identifying the individual.

Read together, the potential legislative revision and judicial interpretation signal an emerging shift from a strict identifiability model to a contextual, risk-based assessment of data identifiability and lawful use.

Organizations processing EU-linked or global personal data should monitor this reform closely and prepare for possible recalibration of compliance programs.

BYTE/WISE

California Introduces Personal Accountability for Privacy, Cybersecurity and AI Compliance

California has finalized new CCPA (California Consumer Privacy Act) regulations that make individual executives personally accountable for privacy, cybersecurity, and AI compliance. Under the updated framework, companies must designate a responsible officer, typically at the executive level, who will attest, under penalty of perjury, to the organization's adherence to privacy, AI, and cybersecurity risk management requirements. This move represents a significant evolution from entity-level to individual-level accountability, signaling greater regulatory scrutiny over senior leadership.

The regulations require designated individuals to oversee and certify risk assessments for high-risk data processing beginning 1 January 2026, and automated decision-making (ADMT) compliance from 1 January 2027. Independent cybersecurity audit certifications must be filed annually with the California Privacy Protection Agency, with initial filings due by April 2028.

California's approach may signal a broader global shift toward personal executive liability in privacy and AI governance. Organizations should begin identifying and empowering compliance officers with the necessary authority and operational insight to meet these obligations, integrating similar accountability structures into global privacy, AI, and cybersecurity frameworks.

Privacy/ CLAUSE IN FOCUS

DATA RETENTION AND DELETION

Background

Data retention and deletion clauses define how data is managed once its intended use is complete, establishing clear obligations for retaining, deleting, or returning data and ensuring that compliance can be verified. These clauses support responsible data-lifecycle management by ensuring data is kept only as long as necessary, aligning practices with governance standards and legal requirements, and promoting consistent handling across backups, archives, and third-party environments.

Illustrative Draft Clause Language

"The Processor shall retain personal data only for as long as necessary to fulfil the purpose of processing or to meet applicable legal or contractual obligations. Upon completion of the purpose or termination of this Agreement, the Processor shall permanently delete or return all personal data, including from backups and archives, and provide written confirmation of such deletion."

Negotiating Points

Controller:

- Require clear retention schedules or triggers based on purpose completion or contract termination.
- Mandate certification of deletion or written confirmation, including for backup systems and sub-processors.
- Include audit or inspection rights to verify deletion or retention compliance.
- Specify consequences (such as liquidated damages or termination rights) if the Processor fails to delete or return data on time.
- Require prior approval before extending retention beyond the agreed period.

Processor:

- Negotiate flexibility to retain data where required by law, regulation, or legitimate business recordkeeping.
- Limit certification obligations to "commercially reasonable" evidence rather than full audits.
- Clarify that deletion from immutable backups may be deferred until the next scheduled purge cycle.
- Seek to cap liability for delayed or partial deletion, provided reasonable safeguards are maintained.

Controllers typically seek strict deletion timelines and auditability to demonstrate accountability, while processors prefer flexibility to accommodate technical constraints, statutory retention duties, and service continuity. Balanced drafting should align contractual obligations with real operational capabilities, ensuring that data is deleted securely, verifiably, and without disrupting legitimate compliance needs.

BYTE/WISE

Privacy/ COMPLIANCE SNAPSHOT

Personal Data Breach under the DPDP Act

A personal data breach under the DPDP Act occurs when personal information is accidentally or unlawfully accessed, disclosed, altered, or destroyed, affecting its confidentiality, integrity, or availability.

The Act requires both Data Fiduciaries and Data Processors to implement reasonable security safeguards and maintain a clear breach-response chain.

Data Fiduciaries remain the primary point of statutory accountability. Where Data Processors or sub-processors are involved, the escalation must follow: sub-processor → processor → fiduciary → DPBI + Data Principals.

Notifications must follow strict timelines:

- Data Principals must be notified "without delay" in clear, simple language with details of the breach, its likely consequences, mitigation steps and contact information.
- The Data Protection Board of India (DPBI) must first be notified "without delay," followed by a detailed breach report within 72 hours of becoming aware of the breach, including the nature and scope of the incident, time of occurrence, causes, mitigation measures, responsible actors (where identified), and steps taken to prevent recurrence

Quick Self-Check for Organizations

- Do you have round-the-clock monitoring systems that can flag unauthorized access, exfiltration attempts, unusual privilege changes, or anomalous data flows?
- Is there a documented escalation chain that triggers immediately upon breach detection, along with a designated lead with authority to coordinate investigation and notifications?
- Have you mapped all vendors and sub-vendors handling personal data, with contract clauses that require equivalent security measures and breach-reporting pathways, including immediate breach-reporting obligations?
- Do you have pre-approved templates for notifying Data Principals and the DPBI within mandated timelines?
- Do your Data Processing Agreements with Data Processors include cooperation requirements, assistance in containment, and incident-specific audit rights?

Organizations should not treat breach-response as an IT-only function or rely on vendor assurances as a substitute for internal governance.

Privacy

KNOWLEDGE
CORNER

(Explicit) Consent vs. Deemed Consent

BYTE/WISE

(Explicit) Consent vs. Deemed Consent

Under the GDPR, consent under Article 4(11) must be freely given, informed, specific, and unambiguous. In addition, explicit consent is required in the context of special categories of data and certain automated decision making.

Under India's DPDP Act, consent under Section 6 remains the default lawful basis for processing personal data, requiring clear notice, informed choice, and purpose limitation, with the assurance that consent is specific to the stated purpose and can be withdrawn at any time.

While the GDPR does not recognize any formal category of "deemed consent," it offers comparable flexibility through alternative lawful bases under Article 6, allowing data processing without explicit consent where necessary for contractual performance, legal compliance, protection of vital interests, public-interest tasks, or legitimate interests pursued by the controller.

The DPDP Act codifies this flexibility through Section 7, which recognizes 'deemed consent' in situations where obtaining explicit consent may not be feasible such as processing for legal compliance or State functions, public-interest and emergency purposes, employment-related needs, and other 'fair and reasonable purposes' such as fraud prevention, network security, and credit scoring.

Consent forms the foundation of lawful data processing. It requires a conscious, informed choice by the individual, ensuring transparency, purpose limitation, and control. This means that the individual knowingly and voluntarily agrees to the processing of their personal data for a specific purpose after being clearly informed about what is collected, how it will be used, and by whom. It is the highest standard of consent and typically requires a clear affirmative action such as ticking a box, signing a form, or confirming through a digital prompt.

For example, a financial app seeking to access transaction data for personalized analytics must obtain explicit consent through a clear, separate prompt.

Deemed consent introduces flexibility by permitting data processing without express approval. It reflects a contextual or implied understanding between the data principal (data subject) and the data fiduciary (controller). It may apply when an individual voluntarily provides data for a transaction, when processing is necessary for employment, compliance with law, or reasonable security safeguards.

For example, an e-commerce platform may rely on deemed consent to process delivery details shared by the customer during checkout, since such use is directly related to the original purpose.

BYTE/WISE

PART TWO

Ai

NOV 2025

Ai / REGULATORY UPDATES

India Proposes amendment to IT Rules to Tackle AI-Generated Content

India's Ministry of Electronics and Information Technology (MeitY) has proposed amendments to the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, introducing new obligations to curb deepfakes and AI-generated misinformation.

The draft defines "synthetically generated information" as content created or altered using computer resources to appear authentic and extends enhanced due-diligence requirements for intermediaries, particularly large social media platforms.

Under the draft framework, platforms that host or disseminate user-generated content must require uploaders to disclose whether material has been synthetically generated, ensure that such content carries visible and persistent labels, and deploy automated tools to detect and remove deepfakes and other harmful media.

Additionally, the ministry has also issued a Standard Operating Procedure to combat the spread of Non-Consensual Intimate Imagery (NCII), expanding on Rule 3(2)(b) of the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The SOP mandates that intermediaries remove or disable access to flagged NCII content within 24 hours of receiving a valid complaint from the affected individual or their authorized representative.

Platforms are required not only to remove reported content but also to proactively deploy crawler technology to detect and prevent re-uploads of hashed NCII material, share hash data with authorities, and provide complainants with real-time status updates.

From a compliance perspective, organizations and platforms in India should begin auditing their upload workflows, moderation pipelines, and vendor contracts. This includes requiring user declarations during upload, deploying automated or semi-automated verification tools, ensuring clear and persistent labels or watermarks, implementing proactive detection tools, and maintaining audit logs that capture content origin and processing.

India releases AI Governance Guidelines

India has recently issued AI Governance Guidelines under the India AI Mission, marking a significant step toward structured AI oversight in India. Centered on seven foundational sutras of Trust, People First, Innovation over Restraint, Fairness and Equity, Accountability, Understandable by Design, and Safety, Resilience and Sustainability, these Guidelines introduce a voluntary graded responsibility framework, that aim to balance innovation with accountability.

The accountability and understandability principles align with the human oversight and transparency requirements under Articles 13 to 15 of the EU AI Act. The focus on risk assessment, bias mitigation, and grievance redressal mechanisms reflects international standards such as the OECD AI Principles and Singapore's Model AI Governance Framework.

The guidelines also include privacy-preserving architectures, content authentication measures, and a "DEPA for AI Training" framework that parallels the EU's compliance-by-design concept. Over time, the Guidelines are expected to interface closely with the Digital India Act, the DPDP Act, and the Information Technology Act, forming an integrated framework for AI, data, and digital governance in India.

Croatia Proposes to Criminalize AI Endangerment

Croatia's Ministry of Justice, Administration and Digital Affairs recently proposed an amendment to its Criminal Code that would create a new criminal offence if the development, testing, verification, supervision, management, or use of an AI system causes endangerment of life or property by an AI system.

While initial discussions have centered on risks like automated vehicles, the proposed law is written to have a much wider applicability. It introduces a new trend in European criminal law, creating derivative accountability for AI-related harm and effectively treats failures in design, oversight, or risk mitigation as potential bases for criminal negligence, aligning with principles under the EU Product Liability Directive (recast 2024) and the forthcoming AI Liability Directive.

In the UK, the Automated Vehicles Act 2024 assigns liability for self-driving incidents to authorized entities but stops short of criminalizing "AI endangerment." Singapore and Japan are adopting proportionate, fault-based approaches within existing civil frameworks rather than introducing standalone criminal offences.

Although India's evolving AI framework do not address criminal liability for AI-related harm, organizations developing or deploying AI systems should begin mapping accountability chains across design, testing, and deployment, and maintain verifiable safety documentation as deficient oversight or model governance could raise liability concerns under existing civil and criminal frameworks.

California's enacts robust new AI Laws

California has enacted three new laws that collectively establish one of the world's most robust state-level frameworks for AI transparency, safety, and accountability. These laws significantly strengthen AI transparency, consumer protection, and civil accountability.

AB 853 (GenAI Transparency) primarily focuses on authenticity in media. It mandates that, starting January 1, 2027, large online platforms offering Generative AI (GenAI) functionality must provide users with a free AI detection tool. This tool allows users to verify whether any image, video, or audio content was altered by that platform's GenAI system, addressing the rise of deepfakes and synthetic media. This measure directly tackles deepfakes and synthetic media manipulation, paralleling the EU AI Act's Article 52 watermarking requirement and China's synthetic content labelling rules, previously discussed in *ByteWise* (October 2025), along with the recently proposed amendments to India's IT Rules (discussed above). California's version, however, seems to go a step further by mandating user-accessible authenticity tools, instead of just backend labelling obligations.

SB 243 (Chatbot Safety) targets social interactions by imposing strict disclosure and safety obligations on companion chatbot providers. Businesses must clearly disclose when users are interacting with AI systems instead of humans, whenever there is a likelihood that a reasonable person could mistake the interaction for one with a natural person. For minors, the law requires stricter disclosures, content-filtering obligations, and, critically, compels providers to implement protocols to prevent the AI from generating self-harm or suicide-related content. Notably, the law introduces a private right of action, enabling affected users to bring civil claims - a first for AI-specific consumer protection.

AB 316 (Liability) addresses courtroom accountability. It removes the "AI Autonomy" defense in civil harm claims, meaning developers or users of an AI system can no longer argue that the harm was caused solely by the system's independent, autonomous action. This ensures that the human or corporate entity behind the AI remains legally responsible, even as the AI becomes more sophisticated. While the EU AI Act focuses on preventive obligations like human oversight and risk management before harm occurs, California's AB 316 addresses accountability after the fact, ensuring that developers and operators cannot evade liability by attributing harm to AI 'autonomy'.

European Commission Reports on GPAI Regulation

The European Commission's Joint Research Centre (JRC) has recently published six scientific reports aimed at providing the technical framework for regulating General-Purpose AI (GPAI) models under the EU AI Act.

The first major focus is GPAI identification, which establishes metrics (linked to cognitive domains) to help providers determine when their model is complex enough to be classified as GPAI and thus subject to the Act's obligations.

A second critical area addressed is systemic risk, where the reports propose measurable factors like compute thresholds, safety benchmarks, and high-impact capabilities to categorize models that require the highest level of regulatory scrutiny.

Additionally, the research addresses behavioral change, providing criteria to assess when a modification to an existing GPAI model is so significant that it essentially becomes a "new" model, thereby triggering a complete set of fresh compliance requirements for the provider.

Reddit's Case Against Perplexity

A federal lawsuit was filed by Reddit, Inc. against Perplexity AI, Inc. on October 22, 2025, where Reddit's complaint strategically leveraged the Digital Millennium Copyright Act's (DMCA) anti-circumvention provisions, asserting that Perplexity AI engaged in "industrial-scale" evasion of technical controls. By centering its claims on the DMCA's anti-circumvention provisions, Reddit advances a theory under which liability turns on the act of defeating technological access controls on Reddit's systems, without requiring the court to decide whether Perplexity's downstream model outputs are infringing or protected as fair use.

Ai / CLAUSE IN FOCUS

HUMAN OVERSIGHT OBLIGATIONS FOR AI SYSTEMS

SB 243 (Chatbot Safety) targets social interactions by imposing strict disclosure and safety obligations on companion chatbot providers. Businesses must clearly disclose when users are interacting with AI systems instead of humans, whenever there is a likelihood that a reasonable person could mistake the interaction for one with a natural person. For minors, the law requires stricter disclosures, content-filtering obligations, and, critically, compels providers to implement protocols to prevent the AI from generating self-harm or suicide-related content. Notably, the law introduces a private right of action, enabling affected users to bring civil claims - a first for AI-specific consumer protection.

AB 316 (Liability) addresses courtroom accountability. It removes the "AI Autonomy" defense in civil harm claims, meaning developers or users of an AI system can no longer argue that the harm was caused solely by the system's independent, autonomous action. This ensures that the human or corporate entity behind the AI remains legally responsible, even as the AI becomes more sophisticated. While the EU AI Act focuses on preventive obligations like human oversight and risk management before harm occurs, California's AB 316 addresses accountability after the fact, ensuring that developers and operators cannot evade liability by attributing harm to AI 'autonomy'.

European Commission Reports on GPAI Regulation

The European Commission's Joint Research Centre (JRC) has recently published six scientific reports aimed at providing the technical framework for regulating General-Purpose AI (GPAI) models under the EU AI Act.

- Insist on human-review triggers for high-impact decisions or when the system generates low-confidence or anomalous outputs.
- Seek explicit provider accountability for incomplete documentation, failure to disclose foreseeable misuse cases, or omissions that materially impair human oversight.
- Require the Provider to supply adequate training materials for deployer personnel to competently supervise, challenge, or override system outputs.

Provider:

- Limit obligations to what is technically feasible, clearly definable, and within the Provider's direct control.
- Clarify that the Deployer bears responsibility for ensuring that oversight personnel are trained, competent, and available, and for maintaining internal supervision processes.
- Protect proprietary information by limiting disclosure to operational documentation, avoiding requirements to reveal model internals, weights, or sensitive IP.
- Cap liability for oversight-related failures, especially where override functions rely on deployer infrastructure, and align liability to "commercially reasonable" technical safeguards.

Providers typically aim to limit oversight obligations to what is technically feasible and within their control, while deployers seek stronger guarantees around documentation, interpretability, and real-time intervention to ensure accountability in operational environments. Balanced drafting should align human-oversight responsibilities with the AI system's risk profile and the parties' respective roles, ensuring that supervision remains

BYTE/WISE

Ai / COMPLIANCE SNAPSHOT

Strengthening Platform Duties under India's IT Rules and Proposed Amendments

India's intermediary compliance landscape is entering a new phase of enforcement and accountability. MeitY's Non-Consensual Intimate Imagery (NCII) Standard Operating Procedure (SOP) under the IT Rules requires intermediaries to remove NCII within 24 hours, prevent re-uploads using hash-matching tools, and coordinate responses with the National Cybercrime Reporting Portal (NCRP) and One Stop Centres.

In parallel, amendments introduce duties to label synthetically generated information, require users to declare AI-altered content, and mandate automated authenticity and deepfake-detection systems, aligning with the India AI Governance Guidelines' emphasis on trust, traceability, and safety by design.

Quick Self-Check for Platforms

- Do upload workflows capture a declaration from users on whether content is synthetically generated, and store it against the asset ID?
- Are visible labels or watermarks applied to AI-generated media and preserved across edits and shares?
- Do moderation systems detect and block re-uploads of NCII content using hash or metadata matching?
- Are takedown responses logged with timestamps and escalation records to meet the 24-hour removal requirement?
- Have vendor and creator contracts been updated to reflect authenticity, provenance, and content-traceability duties?

Platforms should not treat technical deployments or vendor reliance as risk transfer. Embedding authenticity, traceability, and rapid-response requirements into operational workflows and contracts will be essential to meeting obligations under the amended IT Rules and ensuring alignment with India's broader digital-governance framework.

Ai

KNOWLEDGE
CORNER

Provider vs Deployer (EU AI Act)

BYTE/WISE

Defined Terms (Article 3)

Provider: *"The natural or legal person, public authority, agency, or other body that develops an AI system or has it developed and places it on the market or puts it into service under its own name or trademark, whether for payment or free of charge."*

Deployer: *"The natural or legal person, public authority, agency, or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity."*

Explanation:

Under the EU AI Act, the distinction between provider and deployer determines who bears compliance obligations at different stages of an AI system's lifecycle.

A provider is responsible for developing or commercializing the AI system. Essential functions include overseeing design, testing, risk management, data governance, and conformity assessment before the system reaches the market.

A deployer is the entity that uses the AI system in practice. This could include financial institutions applying automated credit-scoring models, public authorities operating predictive-analytics systems, or private organizations integrating AI tools into customer service or logistics.

Deployers must ensure that the AI is used in accordance with the provider's instructions, maintain effective human oversight, and keep logs demonstrating lawful, transparent, and accountable use.

For example, if a software company builds a resume-screening AI tool and licenses it to organizations, the company is the provider, while each organization using the system for employment services is a deployer.

Under the EU AI Act, providers must implement risk-management, data-governance, testing, and documentation obligations consistent with the relevant provisions.

While deployers must comply with use-based obligations under the relevant provisions, including ensuring that the system is used in line with the provider's instructions, maintaining human oversight, and monitoring impacts on fundamental rights in real-world deployment. This division matters for liability and contracts. Providers carry upstream product-like duties to ensure system safety and compliance risks, whereas deployers hold downstream operational responsibilities tied to real-world use and harm prevention.

For companies building or integrating AI systems, early role mapping is critical. Contracts should explicitly define whether a party acts as provider, deployer, or both, and allocate responsibilities for dataset quality, bias mitigation, and post-market monitoring accordingly.

BYTE/WISE

PART THREE

DIGITAL ASSETS

NOV 2025

Landmark Ruling: Madras High Court Recognizes Cryptocurrency as 'Property' Under Indian Law

In a significant decision on 25 October 2025, the Hon'ble Madras High Court officially recognized cryptocurrency as "property" under Indian law in the case of *Rhutikumari v. Zanmai Labs Pvt. Ltd. & Others*. This landmark ruling brings the digital assets at par with traditional assets and confirms that cryptocurrency can be owned, possessed, and held in trust, thereby qualifying as 'property'.

The case stemmed from a major cyberattack in 2024 that compromised the WazirX exchange, resulting in platform-wide losses estimated at over USD 230 million. WazirX proposed an arrangement under which these losses would be proportionately borne by all users/investors. However, the petitioner argued that her cryptocurrency holdings (specifically XRP) were unaffected by the breach and that she retained full beneficial ownership. The Hon'ble High Court accepted this position, noting that cryptocurrency assets can be "enjoyed and possessed in a beneficial form," and directed the exchange to furnish a bank guarantee covering the value of the petitioner's disputed assets.

To reach this conclusion, the Hon'ble High Court examined how various jurisdictions classify cryptocurrency. It noted that El Salvador has recognized Bitcoin as legal tender; that courts in the UK, Singapore, and New Zealand have treated cryptocurrency as property; and that the United States follows a layered, use-based approach when categorizing crypto assets. The Honorable Court also referred to past Supreme Court judgments, like Ahmed G.H. Ariff vs. CWT and Jilubhai Nanbhai Khachar vs. State of Gujarat, which helped define what "property" means under the Indian Constitution.

The Court further observed that cryptocurrency is already classified as a "Virtual Digital Asset" (VDA) under Section 2(47A) of the Income-tax Act, 1961, reinforcing its character as an asset capable of being stored, traded, and transferred, and not merely a speculative instrument. The ruling also echoed a decision from another recent judgment of Bombay High Court in Zanmai Labs Private Limited vs. Bitcipher Labs LLP, which stated that companies holding cryptocurrencies have a special duty to protect them and can't transfer them without the owner's permission.

While this is judgment is likely to be appealed, it's a significant moment for India's crypto industry. By laying down this basic legal understanding, the courts have opened the door for lawmakers to create clear, comprehensive rules that support new technologies while making sure investors are well-protected.

BYTE/WISE

RBI to Pilot Certificate of Deposit Tokenization, Advancing India's Digital Finance Agenda

The RBI has launched a pilot programme in October 2025 to test the tokenization of certificates of deposit, marking a significant step forward in India's digital financial infrastructure. The initiative will evaluate how blockchain or distributed-ledger technology/DLT technology can make markets for traditional financial instruments more secure, efficient, and transparent.

Tokenization is a process which converts traditional financial assets into digital tokens recorded on a secure distributed ledger, enabling faster and more efficient transfer and settlement. For certificates of deposit, this means banks can issue and transfer them digitally, improving operational efficiency and interbank movement. The pilot, conducted with a select group of banks, will explore how digital tokens, representing real-world assets such as certificates of deposit, stocks, or bonds can streamline transactions, reduce settlement risks, and improve liquidity.

EU Moves Toward a Single Supervisor for Crypto Exchanges

The European Union is preparing for a major shift in how crypto exchanges are supervised. In December, as part of its Capital Markets Union and Single Rulebook package, the European Commission is expected to propose placing the most significant cross-border crypto-asset service providers (CASPs) under the direct supervision of the European Securities and Markets Authority (ESMA). ESMA's chair has already indicated that the agency is preparing to expand its remit over crypto markets, noting that a centralized oversight model would enhance investor protection and improve supervisory consistency across the EU.

Deployers must ensure that the AI is used in accordance with the provider's instructions, maintain effective human oversight, and keep logs demonstrating lawful, transparent, and accountable use.

For example, if a software company builds a resume-screening AI tool and licenses it to organizations, the company is the provider, while each organization using the system for employment services is a deployer.

Under the EU AI Act, providers must` implement risk-management, data-governance, testing, and documentation obligations consistent with the relevant provisions.

While deployers must comply with use-based obligations under the relevant provisions, including ensuring that the system is used in line with the provider's instructions, maintaining human oversight, and monitoring impacts on fundamental rights in real-world deployment. This division matters for liability and contracts. Providers carry upstream product-like duties to ensure system safety and compliance risks, whereas deployers hold downstream operational responsibilities tied to real-world use and harm prevention.

For companies building or integrating AI systems, early role mapping is critical. Contracts should explicitly define whether a party acts as provider, deployer, or both, and allocate responsibilities for dataset quality, bias mitigation, and post-market monitoring accordingly.

Digital Assets / CLAUSE IN FOCUS

SEGREGATION & SAFEGUARDING OF CLIENT ASSETS (DIGITAL ASSET CUSTODY)

Background

Segregation and safeguarding clauses are now central to digital-asset custody, driven by regulatory frameworks such as EU MiCA Title V, the MAS DPT Safeguarding Rules, and the NYDFS BitLicense regime, all of which require clear separation of client assets, secure key management, and verifiable record-keeping. These standards now shape global drafting norms, with custody agreements increasingly mandating segregated wallets, transparent ownership records, disclosure of sub-custodians, and explicit liability for safeguarding failures.

These clauses help safeguard against insolvency, operational breakdowns, and key-management failures, ensuring that custody arrangements meet the compliance expectations of institutional and regulatory stakeholders.

Illustrative Draft Clause Language

"The Custodian shall maintain Client Assets in segregated wallets that are clearly identified as belonging to the Client and shall ensure that such assets are not commingled with the Custodian's proprietary assets or with assets of other clients, except where pooling is expressly permitted and adequately recorded in accordance with applicable law. The Custodian shall implement and maintain safeguarding controls consistent with industry standards, including: (a) secure private-key management, (b) multi-factor authentication and multi-signature access controls, (c) immutable, real-time ledgering of client entitlements, and (d) daily reconciliation of on-chain and off-chain records."

Negotiation Points

Client/Asset owner:

- Require clearly segregated, preferably dedicated or trust-labelled wallets, and prohibit omnibus arrangements unless expressly consented to and transparently recorded.
- Push for indemnity or enhanced liability standards for losses caused by key compromise, reconciliation failures, internal misconduct, or inadequate controls.
- Require prompt notice of security incidents, private-key compromise, reconciliation breaks, or irregularities.

Custodian:

- Preserve operational flexibility in how segregation is implemented (e.g., omnibus wallets with internal ledger segregation).
- Exclude or cap liability for protocol-level risks (e.g., chain reorgs), network attacks, or force-majeure blockchain failures
- Align liability caps with insurance coverage limits (crime, cyber, or digital-asset theft policies).

Clients increasingly expect MiCA-grade segregation and safeguarding protections, while custodians seek flexibility to operate efficiently and avoid strict liability for risks beyond their control. Balanced drafting anchors custody obligations to recognized regulatory standards such as MiCA, MAS, NYDFS, ensuring that a contract that is legally defensible, operationally workable, and aligned with the fast-maturing regulatory landscape for digital-asset safekeeping.

Digital Assets

KNOWLEDGE
CORNER

Tokenization of Real-World Assets

BYTE/WISE

Tokenization of Real-World Assets

The Reserve Bank of India (RBI) recently launched a pilot to tokenize certificates of deposit (CDs) via its wholesale CBDC infrastructure, marking a major step towards "real-world asset" tokenization.

Tokenization refers to the process of representing real-world assets (RWAs), whether physical, financial, or intangible assets, like real-estate, bonds, art, or CDs, into digital tokens on a blockchain or distributed-ledger system. The mechanics involve creation of a unified digital layer over traditionally illiquid or paper-based assets, allowing them to be transferred, divided, or traded with the efficiency of digital information. This gives benefits such as improved liquidity, faster settlement and fractional ownership.

Classification: A central question is how tokenized RWAs should be classified under law. Their treatment as securities, commodities, or a distinct digital-asset class determines which regulatory regimes apply.

For instance, a token linked to a financial instrument such as a bond or certificate of deposit may trigger securities-law obligations, while a token representing a purely custodial or reference interest may fall outside traditional securities definitions. This initial characterization shapes the compliance expectations for issuers, custodians, and market participants.

Custody & Legal Rights: Another key theme is the legal nature of the rights embedded in the token. When a token changes hands, the underlying question is whether the buyer acquires a direct ownership interest in the real-world asset, a fractional entitlement, or only a contractual claim against an intermediary. The answer affects how disputes are resolved, how transfers are recorded, and how insolvency or enforcement actions would apply.

Regulatory Guardrails: Regulators emphasize the need for clarity on enforceability, transparency, reserve-backing, and operational governance. For tokenized structures, this includes ensuring that the underlying asset is properly recorded, that custodial arrangements are secure, and that token issuance and redemption are consistent with financial-sector norms.

As India experiments with tokenized wholesale market instruments, these evolving guardrails are likely to influence broader RWA tokenization frameworks, including potential policy considerations around cross-border flows of digital representations of Indian assets. For Indian businesses, investors, and financial institutions, the rise of tokenized RWAs presents both opportunity and complexity.

Firms should begin mapping their potential exposure to tokenization and review internal policies on custody, disclosure, and operational risk. As regulatory expectations develop, early preparedness will be essential to participating in India's emerging digital-assets framework.

BYTE/WISE

PART FOUR

DARK PATTERNS

NOV 2025

BYTE/WISE

FALSE URGENCY

The Guidelines for Prevention and Regulation of Dark Patterns, 2023 define "False Urgency" as the practice of creating artificial time pressure or misleading scarcity signals to rush a user into making a decision they would not otherwise make. This includes overstating demand, exaggerating stock limits, or displaying countdown timers that do not correspond to genuine, time-bound offers. This form of manipulation is explicitly recognized as an unfair trade practice under the Consumer Protection Act, 2019

Examples:

❌ Fake scarcity badges ("Only 1 left!" when stock is high)

❌ Exaggerated real-time counters ("50 people viewing this now!")

❌ Countdown timers attached to non-expiring offers

❌ Misleading "exclusive" or "VIP-only" messaging

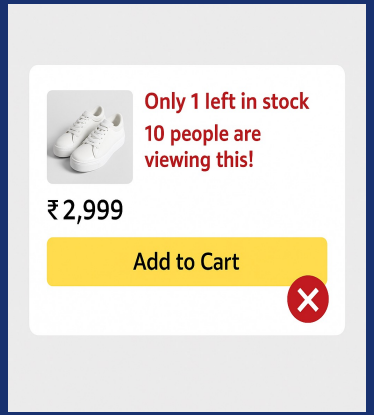
Better Practice: Use only verifiable urgency cues grounded in real business data

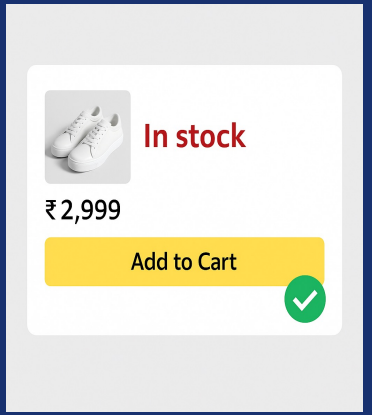
✅ Transparent inventory or pricing information based on actual backend data

✅ No auto-resetting timers or inflated view counters

✅ No unverifiable popularity claims

✅ Clear, stable pricing and offer windows





Tip for businesses

Audit all urgency cues across your websites and apps to ensure every urgency cue in the user interface can be substantiated by real-time logs or documented business rules.

Eliminate countdown timers that reset, unverifiable popularity counters, or generic scarcity banners. Replace them with fixed, transparent deadlines and data-backed signals, and maintain audit trails to demonstrate compliance

COMING SOON

DEC ISSUE

ISSUE EDITORS

Partner: Naresh Pareek
Consultant: Shravan Kalluri

CONTRIBUTORS

Abhishek Nair
Jash Doshi

PUBLISHING SUPPORT

Vivek Yadav

309-10 Madhava,
C5, E Block, BKC,
Bandra East,
Mumbai 400 051