CONSTITUIONAL LAW & ETHICS

Faculty of Law

Unit 3: Cyber Law and IP Regime

Faculty of Law

CYBER LAWS

Introduction

- ‘Cyber’ is a prefix used to describe a person, thing or idea as part of the computer and information age.
- Need for Cyber laws.
- Cyber law encompasses:
  - Cyber crimes
  - Electronic and digital signatures
  - Intellectual property
  - Data protection and privacy

Introduction

- ‘Cyber crime’ is not defined in Information Technology Act 2000.
- Any illegal behavior committed by means of, or in relation to a computer system or network, including such crimes as illegal possession, offering or distributing information by means of computer system or network, or threatening the security of computer systems and the data processed by them.

CYBER LAWS

Introduction

- Cyber laws in India

- The Information Technology Act 2000 (amended in 2008).

- The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government

- The Act essentially deals with the following issues:
  - Legal Recognition of Electronic Documents
  - Legal Recognition of Digital Signatures
  - Offenses and Contraventions
  - Justice Dispensation Systems for cyber crimes.

Introduction to the IT Act, 2000

- **India's primary cyber-law statute**

  The IT Act, 2000 is India's primary law governing digital transactions and cyber-crime.

- **Alignment with UNCITRAL Model Law**

  The Act was modeled on the 1996 UNCITRAL Model Law on Electronic Commerce to ensure international compatibility.

- **Legal recognition for digital records**

  The Act gives legal validity to electronic records, signatures, and online contracts, enabling e-commerce and e-governance.

- **Entered into force in 2000**

  The IT Act, 2000 was enacted by the Indian Parliament and came into effect on October 17, 2000.

- **Amended in 2008 to address new challenges**

  The Act was extensively amended in 2008 to tackle emerging cyber-crime and data protection issues.

Salient Features of the IT Act

- **Legal status for e-documents**
  Sections 4-10A give legal recognition to electronic records and electronic signatures, enabling e-commerce and e-governance.
- **Digital/electronic signatures**
  Section 3 establishes asymmetric-cryptography-based digital signatures, while Section 3A enables other e-authentication methods.
- **Controller & Certifying Authorities (CAs)**
  Sections 17-34 license and regulate Certifying Authorities that issue digital signature certificates.
- **E-governance enablement**
  Sections 6-8 allow citizens to file forms, pay taxes, and receive licenses entirely online.
- **Civil compensation & cyber-torts**
  Section 43 and 43A impose strict civil liability (up to ₹1 crore per contravention) for unauthorized access, data leaks, and more.
- **Dedicated offences chapter**
  Sections 65-67C (plus new 66C-66F, 69A etc.) criminalize hacking, identity theft, cyber-terrorism, and child pornography.
- **Critical infrastructure protection**
  Sections 70/70A empower the government to declare
- **CERT-In made statutory**
  Section 70B designates CERT-In as India's 24x7 incident-response body.
- **Safe-harbour for intermediaries**
  Section 79 shields platforms that follow

The Act's Architecture

- **Preliminary & Definitions**
  Gives precise meanings to tech terms so courts can keep up with jargon.
- **E-Signatures & E-Governance**
  How to make a legally valid digital signature; how government accepts e-filings.
- **Controller & Certifying Authorities**
  Public-key-infra (PKI) watchdog & licensing of CAs.
- **E-Governance rules**
  Forms, filing, issue of certificates/licences electronically.
- **Civil liability & Adjudication**
  "Pay for the damage you cause" even if it wasn't a crime.
- **Cyber-Appellate Tribunal (now merged into TDSAT)**
  Speedy appeals in cyber-disputes.
- **Offences**
  All criminal provisions (65-67C, 66C-F, 69A-B, 70-84C).
- **Intermediary liability & Misc.**
  Section 79 safe-harbour, search-seizure powers, rule-making.

Key Definitions in the IT Act

IT-Act clause	Statutory term	Simplified meaning	Everyday example
2(1)(a)	Access	Gaining entry to or communicating with any part of a computer/system/network	Typing a URL, SSH-ing into a server
2(1)(f)	Asymmetric Crypto System	Pair of mathematically linked public & private keys used for digital signatures	RSA key pair in Aadhaar e-sign
2(1)(g)	Certifying Authority (CA)	Licensed body that issues Digital / Electronic Signature Certificates	NIC-CA, e-Mudhra
2(1)(ha)	Communication Device	Any gadget (phone, tablet, etc.) used to send text, audio, video or images	Smartphone used for WhatsApp
2(1)(i)	Computer	Any electronic, magnetic, optical device that processes data	Laptop, Raspberry Pi, smart TV

The 2008 Amendment

- **New Section 66C - Identity Theft**
  Targets the misuse of passwords, biometric data, and other identity information for fraudulent purposes.
- **New Section 66D - Online Cheating and Phishing**
  Criminalizes fraudulent online practices like phishing and other forms of internet-based cheating.
- **New Section 66E - Voyeurism and Privacy Breach**
  Addresses the growing concerns around the unauthorized capture and dissemination of private images and videos.
- **New Section 66F - Cyber-Terrorism**
  Establishes strict penalties for cyber-attacks targeting India's critical information infrastructure.
- **New Section 69A - Government Blocking of URLs/Apps**
  Empowers the government to block access to online content deemed a threat to national security or public order.

Integrating with Criminal Procedures

Defining

The Bharatiya Nyaya Sanhita (BNS) 2023 S 318 ensures continuity in defining

Getting an e-search warrant for a hacker's laptop

The BNS 2023, Chapter IX allows for online warrants and mandatory video-recorded searches, facilitating digital-age investigations.

Admitting server logs & hash values in court

The Bharatiya Sakshya Adhiniyam (BSA) 2023 SS 61-77, especially S 73, modernizes digital evidence rules for admissibility in court.

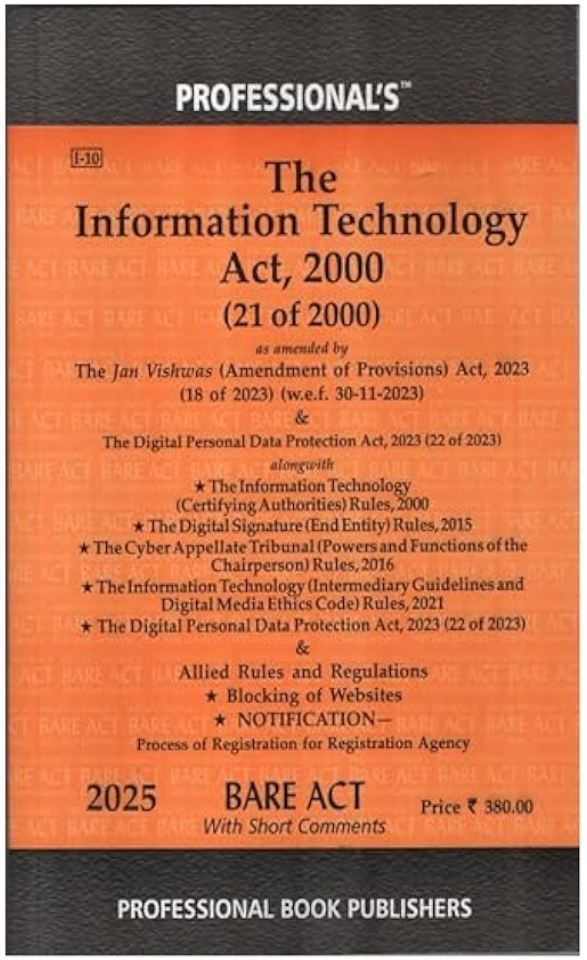
The integration of the IT Act with the updated criminal procedures and evidence codes ensures a cohesive legal framework to address digital-age offences. This enables engineers to build secure systems that adhere to the law and protects both their clients and users.

Why These Basics Matter to Engineers

Every line of code you write touches the definitions in the Information Technology Act, 2000. Calling an API without authorization may be considered 'access' under Section 2(1)(a), and storing user passwords in plain text risks civil compensation under Section 43A and criminal charges under Section 66C. Understanding the statutory vocabulary and salient features of the IT Act early on can shield you from accidental breaches and help you architect secure, compliant digital systems.

The Information Technology Act, 2000: Navigating India's Digital Landscape

The Information Technology Act, 2000 is a foundational piece of legislation that governs India's digital landscape. By understanding its key provisions, definitions, and recent amendments, engineers can ensure their work aligns with the legal framework, protecting both their clients and users.



Penalties under the IT Act, AI Voice-Clone Fraud & Deepfake Imagery

An introductory slide providing an overview of the key legal sections of the Indian IT Act that every engineer must be aware of, particularly regarding emerging AI-powered cyber crimes like voice cloning and deepfake imagery.

Why This Matters

Gen-AI can clone voices in 15 s

Emerging AI capabilities enable quick voice cloning, scaling up old cybercrime tactics

Swap faces in 15 frames

Synthetic media like deepfakes can be generated rapidly, increasing threat

Old cyber-crimes now scale instantly

Faster creation and distribution of fraudulent content leads to bigger losses

Engineers designing these AI systems must be aware of the legal implications and potential misuse, in order to build secure and ethical applications.

IT Act: Quick Refresher

Primary cyber-law statute

The Indian IT Act, 2000 is the primary law governing cybersecurity and digital transactions in the country.

Gives e-records & e-signatures legal validity

The act provides legal recognition to electronic records and digital signatures, making them admissible in court.

2008 amendment added AI-era offences

The 2008 amendment to the IT Act introduced new sections (66C-F, 69A) to address emerging threats from AI-powered cyber crimes.

The IT Act, 2000 and its subsequent amendments form the backbone of India's cybersecurity legal framework, providing the necessary laws to tackle evolving digital threats.

ITA Section	Offence (plain wording)	Max Jail (1st conviction*)	Max Fine (1st conviction*)
65	Tampering with computer-source documents (alter, conceal, destroy)	**3 years**	**₹ 2 lakh**
66	"Computer-related offences" (unauthorised access/damage covered in S43)	3 years	₹ 5 lakh
66C	Identity theft – fraudulent use of password, digital signature, etc.	3 years	₹ 1 lakh
66D	Cheating by personation via computer resources (e-mail, deep-fake call)	3 years	₹ 1 lakh
66E	Violation of privacy – capturing/transmitting private images	3 years	₹ 2 lakh
66F	**Cyber-terrorism** – attack or threat against Critical Info Infrastructure	**Imprisonment for life**	—
67	Publishing / transmitting **obscene** electronic content	3 years → 5 years (repeat)	₹ 5 lakh → ₹ 10 lakh
67A	Publishing sexually-explicit material (non-child)	5 years → 7 years (repeat)	₹ 10 lakh (same for repeat)
67B	Child sexually-explicit material	5 years → 7 years (repeat)	₹ 10 lakh (same for repeat)
69A	Failure to comply with Govt blocking order (public-access info)	7 years	Fine (no statutory cap)

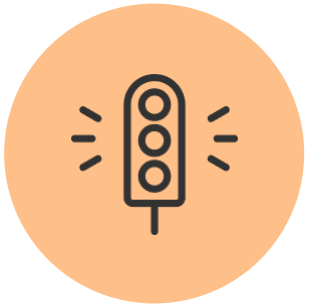
AI Voice-Clone Fraud: How It Works

3-step scam

Scrape voice → clone model → panic call for money

Real 2024 Pune case

Family nearly wired ₹50 k



Risk explodes with freely available tools

Easy access to voice cloning technology

The ease and availability of voice cloning technology has enabled a new type of scam, where attackers can impersonate victims and trick their friends and family into sending money. This poses a significant risk that engineers designing these systems must be aware of.

Sections Triggered by Voice Clones

Identity theft

Voiceprint counts as biometric under Section 66C

Cheating by personation

Cheating by personation via computer resource under Section 66D

Cheating (new penal code)

Cheating under Section 318 of the new Bribery and Corruption Act (BNS)

These sections of the IT Act and the new Bribery and Corruption Act carry significant penalties, with jail terms up to 3 years under the IT Act and up to 7 years under the BNS.

AI Deepfake Imagery: What & Why

Definition

Synthetic audio-visual record that impersonates, misinforms or sexually exploits

Buckets

Political fakes, non-consensual sexual, financial scams

Deepfake technology can be abused to create synthetic media that impersonates, misinforms or exploits individuals, leading to a range of malicious use cases that engineers need to be aware of and build countermeasures against.

Deepfake-Related Offences & Fines

Offence	Jail (Max)	Fine (Max)
Privacy breach	3 yrs	₹2 lakh
Obscene adult deepfake	5 yrs	₹10 lakh
Child deepfake	5–7 yrs	₹10 lakh
Platform non-removal	Lose S 79 safe harbour	36-hour rule under 2021 Rules

*Indian IT Act, 2000 (as amended 2008) + BNS/BNSS/BSA 2023

Engineering Counter-Measures

Voice

Use speaker-verification & out-of-band confirmation to prevent voice cloning attacks

Images

Utilize perceptual hashing, watermark AI output, and one-click reporting to detect and mitigate deepfake imagery

Evidence

Generate SHA-256 hashes and maintain immutable logs for tamper-proof evidence (BSA S 73 compliance)

ecure-by-design and strict logging are the best defences for future engineers to combat AI-powered cyber threats like voice cloni and deepfake imagery.

Key Take-Aways

66C, 66D are workhorses against AI voice scams

These sections of the IT Act are the primary legal tools to address identity theft and cheating via voice cloning scams.

Platforms have 36 h to act or lose immunity

Under the 2021 IT Rules, platforms must remove deepfake content within 36 hours, or risk losing their safe harbor protections.

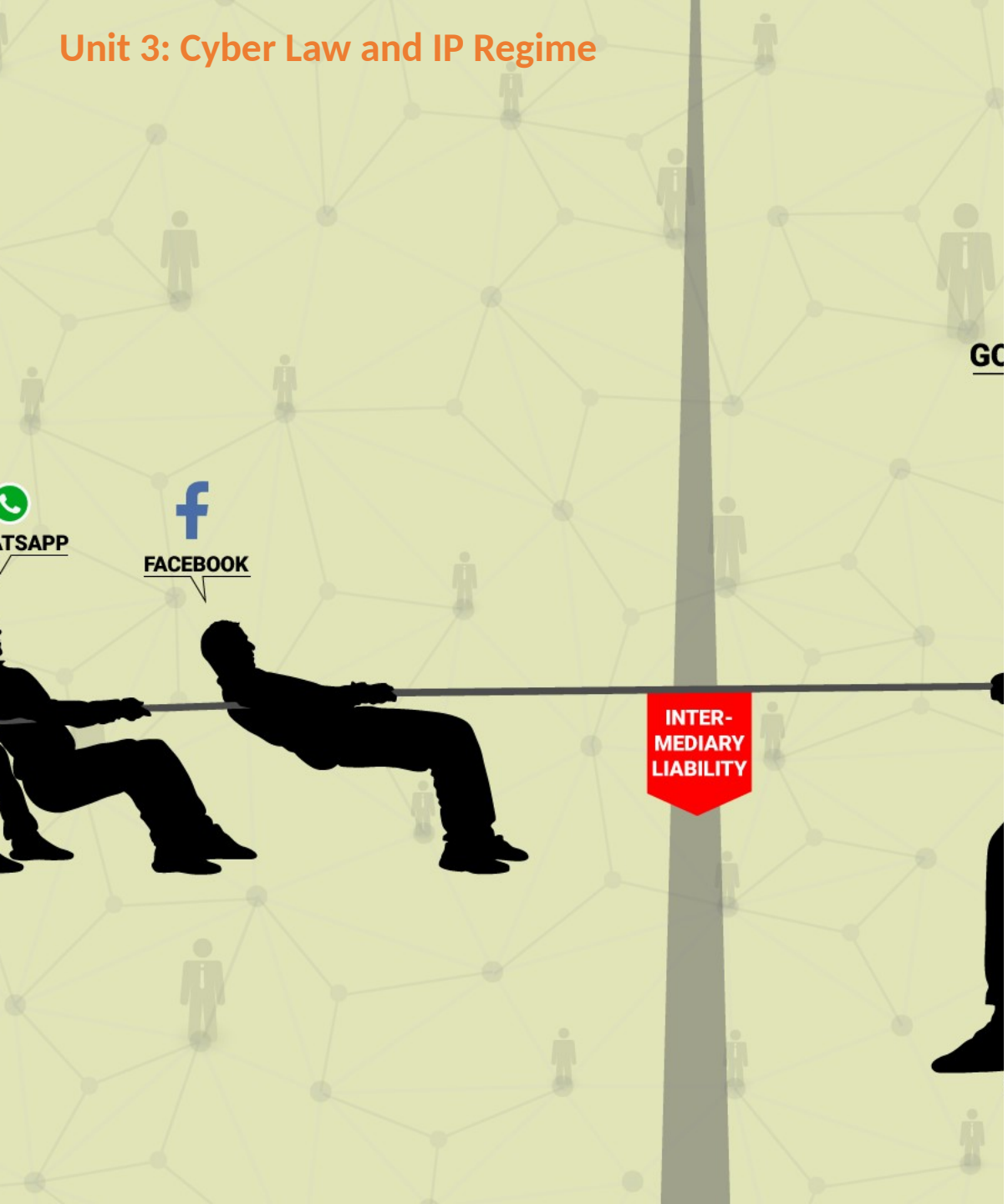
66E, 67, 67A/B cover the deepfake spectrum

The IT Act has provisions to tackle various forms of deepfake-related offenses, from privacy breaches to non-consensual sexual exploitation.

Secure-by-design + strict logging = best defence for future engineers

Designing systems with built-in security features and maintaining immutable audit trails are crucial to combat emerging AI-powered cyber threats.

The key takeaways highlight the critical legal sections, platform responsibilities, and engineering best practices to address the challenges posed by AI voice cloning and deepfake imagery. This knowledge equips future engineers to develop secure, ethical systems and navigate the evolving legal landscape.



Intermediary Liability & Platform Duties

An introductory overview of the legal framework, compliance requirements, and engineering best practices for online platforms in India to manage intermediary liability and safeguard their 'safe harbor' status.

Why It Matters

Billions of user posts daily

Platforms face increasing demands for content takedown and user traceability

S 79 safe-harbour

Provides immunity only if platforms meet due-diligence requirements

Engineering decisions

APIs, logging, AI filters - all of these determine a platform's legal liability

Platforms must proactively manage their engineering and compliance efforts to ensure they can benefit from the safe-harbor protections under the law.

Who Is an "Intermediary"?

Receives, stores, transmits third-party data

Any entity that handles user-generated content falls under the definition of an 'intermediary'

Examples include telecoms, ISPs, clouds, social media, e-commerce, search

Intermediaries cover a wide range of online service providers and platforms

Significant Social-Media Intermediary (SSMI) threshold: > 5 million users (2021 Rules)

Platforms with a large user base have additional compliance obligations

The definition of an 'intermediary' is broad, encompassing any entity that handles third-party data. Platforms must understand their classification and the corresponding legal obligations to ensure compliance.

S 79 Safe-Harbour Essentials

Passive conduit

No initiation, no receiver selection, no content edit

Observe due diligence

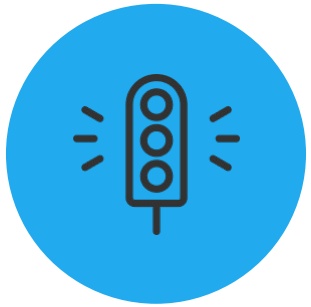
Follow Government guidelines

Immunity void

If platform "conspires, abets or aids" unlawful acts

To maintain safe-harbor protection, platforms must act as a passive conduit, observe due diligence, and refrain from aiding or abetting unlawful activities.

Losing Safe-Harbour



Actual knowledge & failure to act

Platforms lose safe-harbor immunity if they have actual knowledge of unlawful content and fail to take action to remove or disable it.

Active monetization or algorithmic amplification

Platforms that actively monetize or algorithmically amplify illegal content can be held liable, even if they didn't create the content themselves.

Repeat copyright or trademark notices ignored

Platforms must respond to repeated notices of copyright or trademark infringement, or else they risk losing their safe-harbor protection.

Platforms must carefully monitor their content and respond promptly to any indications of unlawful activity to maintain their safe-harbor immunity under the law.

IT Rules 2021 / 2023 — Core Platform Duti

- **Publish Terms, Privacy & "Users' Rights Charter"**

  Platforms must publicly disclose their policies and user rights charter.

- **T-36 h: Remove/disable unlawful content after govt / court notice**

  Platforms must remove or disable illegal content within 36 hours of receiving a government or court order.

- **T-24 h: Sexually explicit imagery takedown**

  Platforms must remove sexually explicit content within 24 hours of being notified.

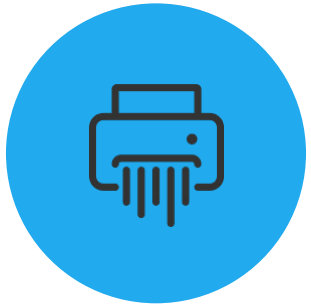
- **Appoint: Chief Compliance Officer, Nodal Contact, Grievance Officer**

  Platforms must appoint key personnel to ensure compliance and handle user grievances.

- **Monthly transparency & automated moderation reports**

  Platforms must regularly publish reports on their content moderation efforts and performance.

Extra SSMI Obligations & Fact-Check Amendments



End-to-end-encrypted SSMIs

require enabling originator traceability

2023 PIB Fact-Check Unit rule

(currently stayed by courts) would require removal of govt-labelled 'fake news'

Debate: privacy vs. accountability

Balancing user privacy and platform accountability is a key challenge

The slide highlights the additional obligations for Significant Social Media Intermediaries (SSMIs), including the requirement for enabling originator traceability in end-to-end encrypted platforms, as well as the ongoing debate around the 2023 PIB Fact-Check Unit rule and the need to balance user privacy and platform accountability.

CERT-In 2022 Directions (Synergy)

Report cyber-incidents within 6 hours

Platforms must report any cyber-incidents to the government within 6 hours of noticing them.

Retain logs for 180 days

Platforms must retain user activity logs for a period of at least 180 days.

VPS/VPN providers keep KYC for 5 years

Virtual private server (VPS) and virtual private network (VPN) providers must maintain user identity (KYC) records for 5 years.

Coordinate with platform abuse desks

Platforms must coordinate with government agencies during cybersecurity incidents and crises.

The CERT-In 2022 Directions establish a framework for enhanced cybersecurity cooperation between online platforms and the government, requiring rapid incident reporting, extensive data retention, and coordinated crisis response.

Deepfake & AI Content Advisories

Proactive detection of AI-generated deepfakes

Platforms must develop advanced AI/ML models to detect and identify AI-generated or manipulated media content.

Labeling and watermarking of deepfakes

Detected deepfakes should be prominently labeled or watermarked to inform users about the synthetic nature of the content.

Removal of impersonation/manipulated media

Platforms must remove any content that violates the

Visible policies and user education

Platforms should maintain clear and visible policies regarding deepfakes, and proactively educate users about the risks and identification of such content.

Effectively addressing the growing challenge of deepfakes and manipulated media requires a multi-pronged approach, including proactive detection, transparent labeling, swift removal, and comprehensive user education. Platforms must remain vigilant and continuously adapt their technical and policy frameworks to maintain compliance and protect their users.

Engineering Checklist & Key Take-Aways

Takedown Clock

Build a 36-hour and 24-hour takedown clock into the ticketing system to ensure compliance with content removal timelines.

Hash-log Uploads

Hash-log every user upload to maintain a tamper-evident audit trail as evidence (BSA S 73).

Automate Detection

Automate the detection of prohibited content, but maintain a human review loop to ensure accuracy and prevent over-censorship.

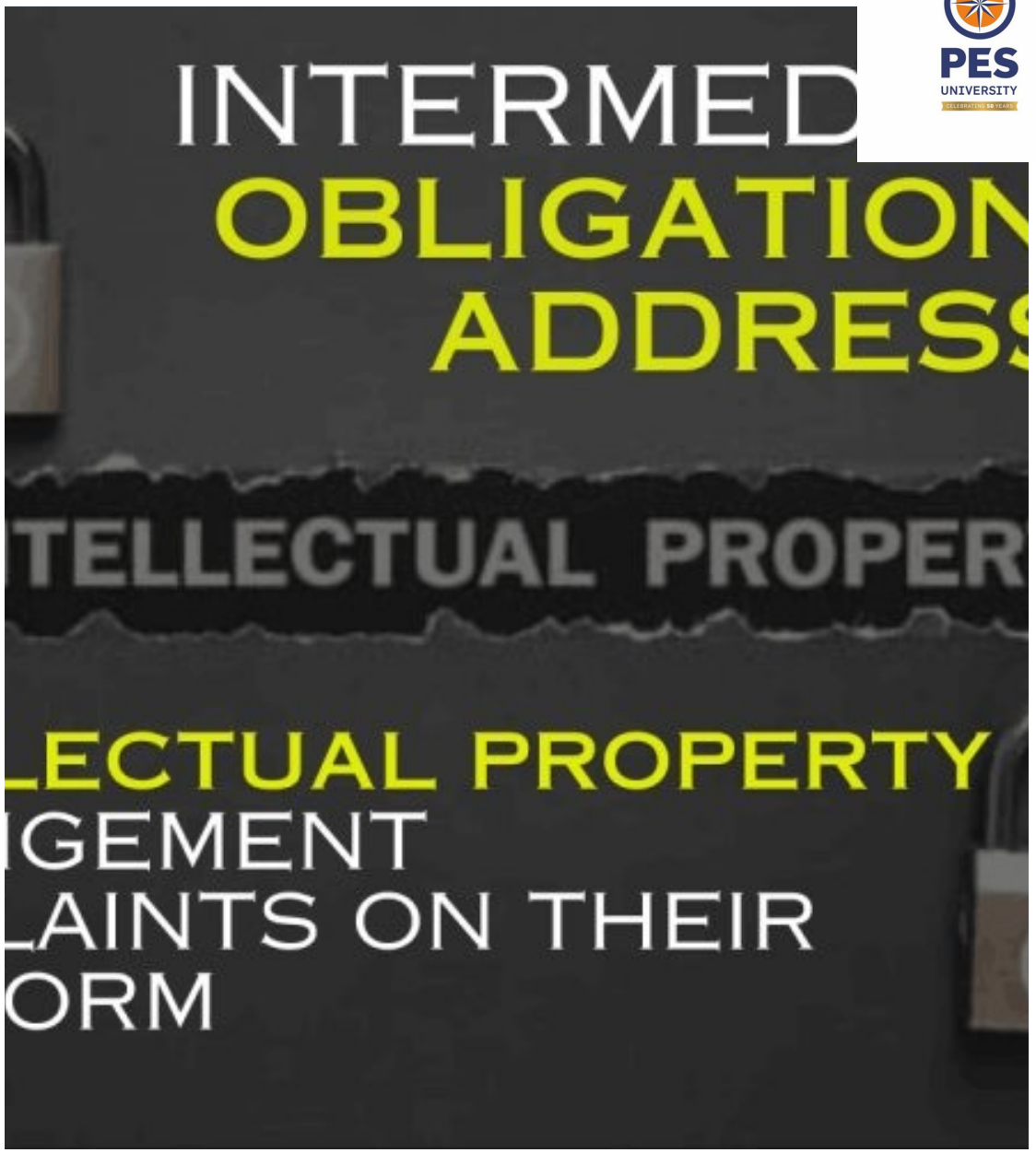
Compliance as a DevSecOps Task

Safe-harbor is not a blanket shield, and compliance is an ongoing, evolving DevSecOps task that requires continuous monitoring and adaptation.

The engineering checklist emphasizes the need for a proactive, technology-driven approach to platform compliance, while maintaining a balance between automation and human oversight. Ultimately, effective platform governance requires a deep understanding of the evolving regulatory landscape and a commitment to continuously refining the platform's engineering and operational practices.

Intermediary Liability & Platform Duties

The presentation provides a comprehensive overview of the legal framework and compliance requirements for online platforms in India. It highlights the critical importance of adhering to safe-harbor provisions, meeting due diligence obligations, and implementing robust engineering solutions to ensure platform liability is effectively managed. The key takeaways emphasize the need for a proactive, dynamic approach to platform governance, as the regulatory landscape continues to evolve to address emerging challenges like deepfakes and misinformation.



vacy in India :

d Laws

anch of data management that deals
al data in compliance with data
lations, and general privacy best

Sensitive Personal Data & India's New Data-Protection Regime

An introductory overview of the evolving data privacy landscape in India, including the existing SPDI Rules 2011 and the upcoming Digital Personal Data Protection Act 2023.

What Is "Sensitive Personal Data/Informati (SPDI)?

Definition from IT (Reasonable Security Practices & SPDI) Rules 2011

The IT (Reasonable Security Practices & SPDI) Rules 2011 define SPDI as personal information relating to

Examples of SPDI

- Passwords - Financial information - Health records - Biometrics - Sexual orientation

Contrast: Ordinary Personal Data

Ordinary personal data includes information like: - Name - Email address - IP address

Key Difference

SPDI requires stronger protection and consent mechanisms compared to ordinary personal data.

SPDI	Non-SPDI
✓ Aadhaar number	✘ office e-mail
✓ fingerprint	✘ favourite colour
✓ mental-health report	✘ college roll-number
✓ bank account details	✘ home address
✓ sexual orientation	✘ date of birth

SPDI Rules 2011: Core Obligations

- **Obtain written/opt-in consent before collecting SPDI**

  Organizations must obtain explicit, written consent from individuals before collecting their sensitive personal data.

- **State clear purpose, retention period; no secondary use**

  The purpose and retention period for collecting SPDI must be clearly communicated, and the data cannot be used for any secondary purposes without additional consent.

- **Implement ISO 27001-level security; audit every 12 months**

  Organizations must maintain robust security measures for SPDI, in line with the ISO 27001 standard, and conduct regular audits to ensure compliance.

- **Appoint a Grievance Officer with 1-month response time**

  Organizations must designate a Grievance Officer to address any concerns or complaints from individuals regarding the handling of their SPDI, with a maximum response time of one month.

AI Profiling & The 2011 Limits

Rule 5: Collection Limited to Necessary Purpose	Rule 6: Prior Consent for Third-Party Disclosure	Rule 8: Privacy-by-Design and Audit Logs	Engineering Tip: Anonymize or Aggregate Before Model Ingestion
Prohibits unlimited model training by limiting the collection of SPDI to only what is necessary for the stated purpose.	Requires obtaining prior consent before disclosing SPDI to any third-party AI vendor or service provider.	Mandates the implementation of privacy-by-design principles and the maintenance of audit logs for any automated decision-making processes involving SPDI.	Recommends anonymizing or aggregating SPDI before using it to train AI models, in order to comply with the data minimization and purpose limitation principles.

Digital Personal Data Protection Act 2023 (DPDPA): Bird's-Eye View

Repeals S 43A liability once fully notified

The DPDPA replaces the existing patchwork of data protection regulations under the IT Act's Section 43A.

Introduces Data Fiduciary & Data Principal roles

The DPDPA establishes the roles of Data Fiduciary (entity handling data) and Data Principal (individual whose data is collected).

Cross-border transfers allowed to whitelisted jurisdictions

The DPDPA allows for cross-border data transfers to countries or sectors deemed 'whitelisted' by the government.

Oversight: Data Protection Board of India (DPBI)

The DPDPA introduces the Data Protection Board of India as the regulatory authority to oversee and enforce the new data protection framework.

The Digital Personal Data Protection Act 2023 (DPDPA) represents a significant shift in India's data protection landscape, introducing new roles, cross-border data transfer guidelines, and regulatory oversight to ensure comprehensive privacy safeguards for individuals.

Seven Foundational Principles (DPDPA S 4)

#	Foundational Principle (DPDPA S 4)	Plain-English Meaning
1	**Lawful, Fair & Transparent Use**	Collect and handle personal data only for legitimate purposes, in a clear and honest manner.
2	**Purpose Limitation**	Use the data strictly for the purpose stated to the Data Principal (or a compatible one).
3	**Data Minimisation**	Gather only the personal data that is necessary—nothing excessive.
4	**Accuracy**	Keep data correct and up-to-date; promptly rectify inaccuracies.
5	**Storage Limitation**	Retain personal data no longer than needed to fulfil the stated purpose or legal duty.
6	**Reasonable Security Safeguards**	Protect data against unauthorised access, breach, or loss with appropriate technical and organisational measures.
7	**Accountability**	The Data Fiduciary is responsible for demonstrating compliance and answering to the Data Protection Board.

Rights of Data Principals (Students, Users, \

- **Right to Access**

  Individuals have the right to access a summary of how their personal data is being processed.

- **Right to Correction & Erasure**

  Individuals have the right to request correction of inaccurate data and erasure of redundant or unnecessary data.

- **Right to Grievance Redressal**

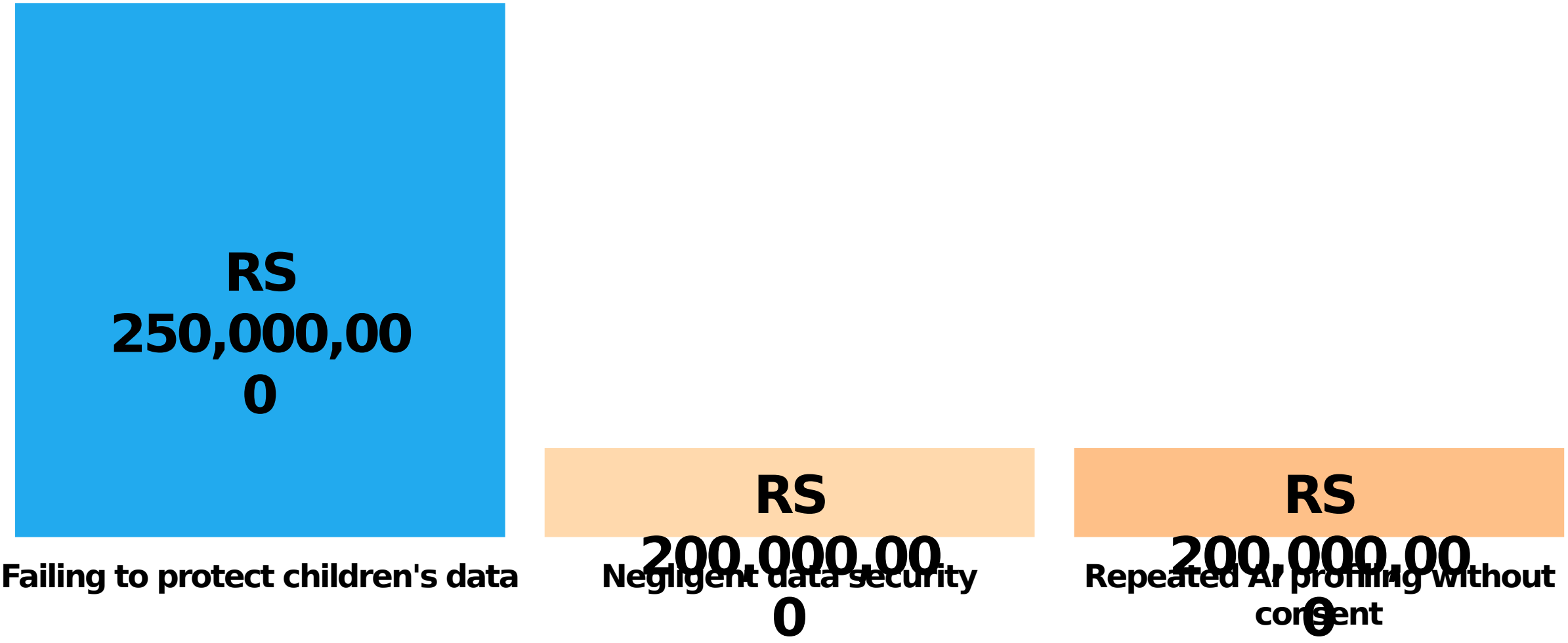
  Individuals have the right to file a grievance with the data fiduciary within 7 days, and escalate to the Data Protection Board of India if necessary.

- **Right to Nominate**

  Individuals have the right to nominate a trusted person to exercise their rights in case of their incapacity.

Remedies & Penalties (DPDPA Ch. VIII)

Potential fines for violations of the DPDPA



Key Take-Aways

SPDI Rules 2011 still apply until DPDPA fully operational

Existing regulations continue to govern sensitive personal data handling until the new law is fully implemented.

DPDPA grants users strong rights—design products to honor them by default

Incorporate data principals' rights, such as access, correction, and grievance redressal, into product design from the outset.

AI profiling without explicit, informed consent risks multi-crore penalties

Strict limits on AI-based data processing and decision-making without user's clear approval can lead to hefty fines.

Privacy-by-design is not optional; it's your competitive edge

Proactively building data protection safeguards can enhance customer trust and provide a strategic advantage.

The key takeaways emphasize the need to stay compliant with existing and upcoming data protection regulations, empower users with their rights, and adopt a privacy-focused approach as a competitive advantage. By understanding and addressing these critical points, organizations can navigate the evolving data privacy landscape in India effectively.

Sensitive Personal Data & India's New Data-Protection Regime

The presentation provides a comprehensive overview of the evolving data protection landscape in India, highlighting the existing SPDI Rules 2011 and the upcoming Digital Personal Data Protection Act 2023. It emphasizes the importance of understanding and complying with these regulations to safeguard sensitive personal data and avoid significant penalties. The presentation encourages organizations to adopt a privacy-by-design approach and empower individuals with the rights granted under the new data protection framework. By staying informed and proactively addressing data privacy concerns, companies can build trust with their customers and maintain a competitive edge in the digital landscape.