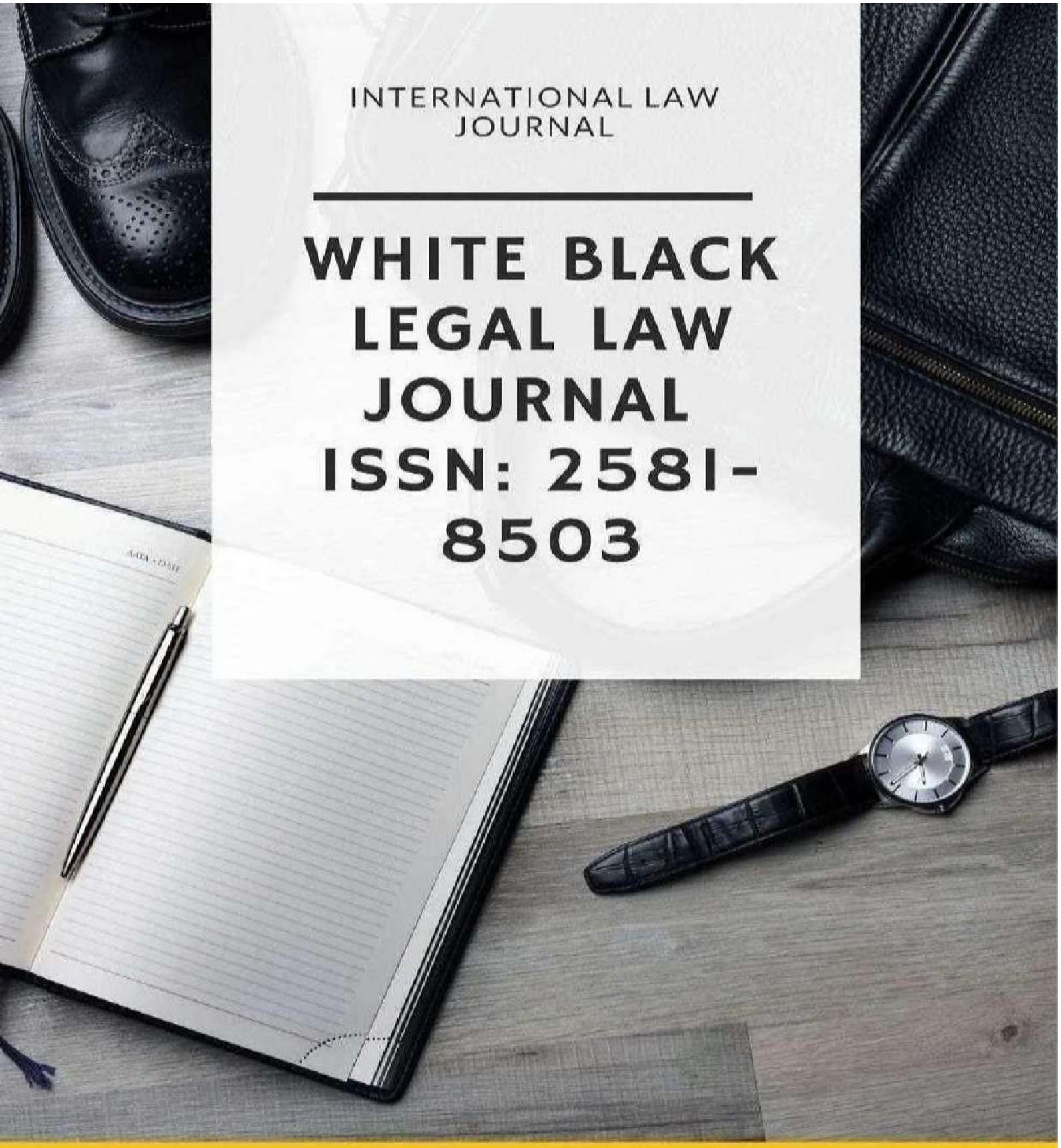

INTERNATIONAL LAW JOURNAL

# WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

## Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

## DISCLAIMER

# EDITORIAL TEAM

## Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

## Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

# Senior Editor

## Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

## Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

## Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

## Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

## Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

## Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

# *ABOUT US*

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

# THE DUAL ARCHITECTURE OF CYBER SOVEREIGNTY: ANALYZING INTERNATIONAL LEGAL TREATIES AND INDIA'S CYBERSECURITY FRAMEWORK

AUTHORED BY – ANKUSH SRIVASTAVA
(B.A LL.B 3RD YEAR)
STUDENT AT – BABU BANARASI DAS UNIVERSITY

CO- AUTHORED BY – DIVYANSHU KRISHNA
(B.A. LL.B 2ND YEAR)
STUDENT AT – BABU BANARASI DAS UNIVERSITY

## Abstract

The rapid expansion of digital networks has challenged the traditional notions of state sovereignty and international law. This paper explores the evolving dual structure of cyber sovereignty—balancing global cooperation in combating cybercrime and a nation's right to assert control over its digital space. By comparing the Budapest Convention (2001) and the United Nations Cybercrime Convention (2024), it evaluates how differing treaty models address cross-border enforcement, data access, and human rights safeguards. The study further examines India's domestic legal framework through the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, highlighting their intersection with international obligations. The research underscores key judicial pronouncements such as Shreya Singhal v. Union of India (2015) and Justice K.S. Puttaswamy v. Union of India (2017), which redefined digital rights within India's constitutional matrix. Ultimately, this analysis reveals that India's cyber governance emphasizes sovereignty and privacy protection but faces challenges in harmonizing global cooperation with national autonomy in cyberspace.

**KEYWORDS** –

**Sovereignty**

**Cybersecurity**

**International Law**

**Budapest Convention**

**UN Cybercrime Convention**

**India**

**Information Technology Act, 2000 (IT Act)**

**Digital Personal Data Protection Act, 2023 (DPDP Act)**

**Privacy**

**Free Speech**

**Digital Rights**

**Digital Evidence**

**CERT-In**

**Data Protection Board of India (DPBI)**

## I. Introduction: The Global Landscape of Cyber Law

The digital world doesn't play nice with traditional legal systems. We need adaptable rules that can handle cyber risks without stifling innovation. Cybersecurity isn't just tech stuff—it's deeply tied to human rights in our hyper-connected age. With data zipping across borders, we're stuck with a messy patchwork of national laws, tech standards, and voluntary agreements instead of a unified global rulebook.

### Why does this matter?

Cyber threats ignore borders. The UN's framework for responsible state behavior in cyberspace leans on voluntary norms, not hard laws. It pushes for capacity-building and protecting rights like privacy and free speech, but voluntary standards (like ISO or NIST) aren't cutting it against big cyber risks. Countries are now scrambling to replace "best practices" with enforceable laws backed by real penalties—forcing companies to overhaul compliance efforts.

Here's the tension driving everything: Countries need global cooperation to fight cybercrime (like through the Budapest or UN Conventions), but they're also doubling down on "digital sovereignty"—strong national laws like India's IT Act and Digital Personal Data Protection Act (DPDP Act). This clash defines how cross-border enforcement works today.

## II. Comparing International Cybercrime Treaties

Two major treaties show different approaches to global cybercrime fighting:

### A. The Budapest Convention (2001)

This Council of Europe treaty is the go-to framework, even for non-members. It requires

countries to criminalize core offenses like hacking and data tampering. Jurisdiction kicks in if the crime happens on a country's soil or its registered ships/planes.

**The big controversy?**

**Article 32**

It lets countries access data.. Critics (like India) say this tramples sovereignty—especially when foreign agencies want data from local servers.

**B. The UN Cybercrime Convention (2024)**

Adopted in 2024, this aims to be the first truly global treaty. It focuses on serious crimes (4+ year sentences) and tries to fix Budapest's gaps:

- Explicit sovereignty protections
- Rules for freezing assets and tech assistance
- A data protection article (Article 36) acknowledging modern privacy laws like GDPR[1]

But there's a catch: It relies on domestic laws for safeguards, which could mean weak protection in countries with poor human rights records.

**C. India's Stance and the Geopolitical Split**

India never joined Budapest. Why? Three reasons:

1. It wasn't in the room when the treaty was drafted.
2. Article 32's data access felt like sovereignty overreach.
3. It didn't align with India's priorities (like intellectual property rules).

India backed the UN Convention instead—even proposing criminalizing "harmful information" (disinformation). But even if India ratifies it, conflicts loom with India's strict data localization rules under the DPDP Act. For now, India handles cross-border requests through old-school Mutual Legal Assistance Treaties (MLATs) and domestic IT Act powers.

## III. India's Cyber Foundation: The IT Act (2000)

India's digital rulebook started with the IT Act in 2000. It had two goals:

1. Enable e-governance and digital transactions
2. Punish cybercrimes

[1] IT ACT 2000
2 CONVENTION ON CYBER CRIME, BUDAPEST 2001, COUNCIL OF EUROPE, ETS 185.

**Key Features:**

- Section 66: Criminalizes hacking, data theft, and fraud (up to 3 years jail + fines).
- Cyber Terrorism (Section 66F): Life imprisonment for attacks threatening national security.
- Critical Infrastructure Protection: National agencies like NCIIPC guard systems that, if hacked, could cripple India (e.g., banks, power grids).

The Landmark Twist: In 2015, the Supreme Court axed
Section 66A (which criminalized "offensive" online messages) for violating free speech. A warning shot: Laws can't override constitutional rights.

## IV. The Privacy Revolution: DPDP Act (2023)

The old data rules (Section 43A) were weak. After the Supreme Court declared privacy a fundamental right (2017's *Puttaswamy* case), India got the DPDP Act in 2023.

What Changed?

- Consent is King: Companies need clear permission to use your data (or fall under "legitimate uses").[2]
- Your Rights: Access, correct, or delete your data. But you also have duties—like not filing fake complaints.
- Big Fines, New Cop: The Data Protection Board (DPBI) can hit companies with penalties up to ₹250 Crore. No more "prove negligence" lawsuits—this is strict liability.
- Data Borders: Rules for sending data abroad are still fuzzy. Critics worry this gives the government too much discretion.

## V. The Compliance Nightmare

India's cybersecurity agency, CERT-In, demands **6-hour breach reporting** for incidents like hacks or data leaks. Meanwhile, the DPDP Act gives companies 72 hours to report privacy breaches to the DPBI.

Why the Clash?

- CERT-In cares about national security: Its 6-hour rule helps stop attacks fast.
- DPBI cares about your privacy: Its 72-hour rule lets companies assess harm to users.

[3] DPDP ACT (2023)
[4] United Nations Cybercrime Convention, 2024, General Assembly Resolution A/RES/78/267.

**Penalties:**

- Ignore CERT-In? Up to 1 year jail or ₹1 Crore fine.
- Violate DPDP Act? Up to ₹250 Crore fine.

## VI. New Tech, New Headaches

AI in Cybersecurity:

- Bias in AI tools could lead to discriminatory targeting.
- No clear rules yet for transparency or ethics.
- Companies must juggle AI innovation with DPDP Act compliance.

IoT Security:

- Devices need "security by design" (unique passwords, encrypted storage).
- Old liability rules (Section 43A) are gone—now DPDP Act fines apply for insecure gadgets.

## VII. Courts and Evidence

Key Rulings:

- Shreya Singhal (2015): Killed Section 66A, protecting online speech.
- Puttaswamy (2017): Made privacy a fundamental right.
- Crypto Ban Lift (2020): Forced RBI to regulate digital assets fairly. [3]

[4]Digital Evidence Rules:

- Section 65B Evidence Act: Requires a certificate proving digital evidence (emails, logs) wasn't tampered with.
- Miss this step? Your evidence gets tossed in court—a huge hurdle for cybercrime caseS.

## VIII. Where Do We Go From Here?

The Big Picture:

India chose sovereignty over global treaties. Its layered laws—IT Act for security, DPDP Act for privacy—aim to control the digital space. But conflicts like the 6-hour vs. 72-hour reporting gap create chaos.

[5] www.supremecourtofindia.com
[6] Information Technology Act, 2000 (Act No. 21 of 2000), Ministry of Law, Justice and Company Affairs, Government of India.

Fix-It List:

1. Harmonize Reporting: Split alerts into "urgent security triage" (to CERT-In in 6 hours) and "privacy impact report" (to DPBI in 72 hours).
2. Regulate AI: New laws must set ethical guardrails for AI in cybersecurity.
3. Train Investigators: Cops and lawyers need better skills to handle digital evidence (that pesky Section 65B certificate).

India's gamble? That strict homegrown rules will make it a digital heavyweight—without crushing rights like free speech. The next test: Making the DPBI effective without drowning businesses in red tape.

## MORE INFORMATION ABOUT THE ACTS

1. The Information Technology Act, 2000 (IT Act)

Passed back in October 2000, this is India's main law for anything digital. It basically does two big things:

- Makes government services easier to access online
- Punishes cybercrimes to keep the digital world safer

Quick breakdown of what it covers:

- Legal Recognition (Sections 4, 5, 10A):

Makes digital signatures and electronic records legally valid – super important for stuff like online contracts or e-gov services.

- Cybercrime Penalties (Sections 65-78):

Defines and punishes core cyber offenses (all grouped under "Offences").

- Computer-Related Offenses (Section 66):

If you hack, steal data, or mess with systems *with bad intent*, you could face up to 3 years in jail, a ₹5 lakh fine, or both.[5]

- Cyber Terrorism (Section 66F):

[7] Digital Personal Data Protection Act, 2023, Ministry of Electronics and Information Technology, Government of India

Using computers to threaten national security? That's the most serious offense here – carries the heaviest punishment.

- Identity Theft & Privacy (Sections 66C, 66D, 66E):

Stealing identities, impersonating people, or leaking private images? Straight to jail (plus fines).

- Data Protection Liability (Section 43A - phasing out):

Companies handling sensitive data used to owe compensation if they were negligent about security. *Note: This part's getting replaced by the new DPDP Act.

2. The Digital Personal Data Protection Act, 2023 (DPDP Act)

This is India's shiny new privacy law (came out August 2023), sparked by a 2017 Supreme Court ruling that said privacy is a fundamental right.

What it does:

- Scope & Consent:

Covers all digital personal data. Now you gotta give clear, explicit consent for your data to be used – no more sneaky fine print.

- Regulatory Shift:

Creates the Data Protection Board of India (DPBI) as the main watchdog. Companies now face strict fines for breaking rules, moving away from the old "oops, our bad" compensation model.

- Breach Notification:

If your data gets leaked, companies must tell both you and the DPBI ASAP. Draft rules suggest they've got just 72 hours to report it.

3. The Indian Evidence Act, 1872 (Section 65B)

This old-timer (updated by the IT Act) decides how digital evidence like emails or call records can be used in court.

Key bit:

- To use any digital record as evidence, you must include a Section 65B(4) certificate. Somebody responsible has to sign off confirming:
  - The computer/system was working right
  - The info was properly fed into it
  - No funny business happened

Landmark Court Cases That Shaped These Laws:

- Puttaswamy v. India (2017):
  SC declared privacy a fundamental right – the push that got the DPDP Act made.
- Shreya Singhal v. India (2015):
  SC killed Section 66A of the IT Act (which criminalized "offensive" messages) for being too vague and violating free speech.

- Anvar P.V. v. Basheer (2015):
  SC ruled that Section 65B certificates are *mandatory* for digital evidence – no certificate, no evidence.
- Internet and Mobile Association v. RBI (2020):
  SC overturned RBI's ban on crypto trading, shaking up digital finance laws.

- Cyber Harassment Judgments (2023):
  SC ordered cops to set up special cyber cells to tackle online stalking/harassment faster, especially for vulnerable folks.

## MORE DETAILS OF LANDMARK JUDGEMENT

1. **Upholding Digital Free Speech: Shreya Singhal v. Union of India (2015)**

So back in 2015, the Supreme Court basically killed off Section 66A of the IT Act. That law was wild – it made it a crime to send anything "grossly offensive" or false online if it annoyed or inconvenienced anyone. The court called it out as super vague and over-the-top, saying it crushed free speech rights under Article 19(1)(a). This ruling's a big deal because it protects people from laws that could shut down legit criticism online.

2. **Privacy Became a Fundamental Right: Justice K. S. Puttaswamy Case (2017)**

In 2017, nine Supreme Court judges unanimously agreed that privacy [6]is a fundamental right tied to our right to life (Article 21). This wasn't just symbolic – it forced the government to finally create proper data laws. That's why we got the Digital Personal Data Protection Act in 2023, India's first real data privacy law.

3. Digital Evidence Rules Got Strict: Anvar P.V. v. P.K. Basheer (2015)

This case made digital evidence way harder to use in court. The Supreme Court said any electronic records – like emails, call logs, or copied files – need this special Section 65B certificate. Some official has to vouch that the device worked properly and the data's legit. No certificate? The evidence gets tossed. It's meant to stop tampering but makes prosecuting cybercrimes a headache.

4. Crypto Got Legal (Sort Of): Internet Association vs RBI (2020)

Remember when RBI banned crypto trading? The Supreme Court overturned that in 2020. Suddenly, crypto was legal-ish, forcing the government to scramble for regulations. Recent rulings (2024) keep pushing for tighter rules to stop scams though.

## SOME LAWS FOR BETTER UNDERSTANDING

1. Cracking Down on Online Abuse

- Cyber Harassment (2023): Courts ordered every state to set up special cyber cells to handle online stalking ASAP, especially protecting women and kids.
- Misinformation (2022-2024): Social media platforms got told: Cooperate with Indian cops investigating fake news and hate speech, no matter where your servers are. Follow our laws.

Cybercrimes Under the IT Act (The Shortlist)

Here's the cheat sheet for what'll get you in trouble:

- Section 66: Hacking or messing with systems fraudulently → Up to 3 years jail / ₹5 lakh fine
- Section 66B: Keeping stolen computers/devices → Up to 3 years / ₹1 lakh fine
- Section 66C: Stealing someone's digital ID (passwords/signatures) → Up to 3 years / ₹1 lakh

[6] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[7] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[8] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

fine.

- Section 66D: Scamming people with fake profiles → Up to 3 years / ₹1 lakh fine.
- Section 66E: Creepshots – sharing private pics without consent → Up to 3 years / ₹2 lakh fine.
- Section 66F: Cyber terrorism (threatening national security) → Life imprisonment.
- Section 67: Posting obscene stuff online → Up to 5 years / ₹10 lakh fine.

**Precautions**

Preventing cyber incidents and making courts actually enforce legal standards isn't about one magic bullet. It's a mix of companies stepping up their game, regulators getting their act together, and courts handling digital evidence properly. Courts aren't just there to punish hackers – they set the tone for how seriously everyone takes digital rights and privacy.

Stopping Cyber Incidents Before They Blow Up:

To keep cyber messes from turning into full-blown disasters, companies need to actually follow the rules laid out in India's IT Act and the newer Digital Personal Data Protection Act.

1. Stop dragging your feet on reporting breaches

India's rules are clear: if something bad happens to critical systems, you shout about it FAST. Companies – especially service providers and data centers – have to report serious incidents (like data leaks or system hacks) to CERT-In within *six hours* of finding out. This isn't bureaucracy; it's about shutting down threats before they spread.

Juggling two timelines: Here's the headache: CERT-In wants that super-fast tech report (6 hours), but the Data Protection Board gives you 72 hours for the full privacy impact assessment. Smart companies plan for both – triage the tech mess first, then figure out who's affected privacy-wise later.

Keep your logs! Seriously, hold onto system logs (like firewall records) for at least 180 days. If something goes sideways, you'll need them to figure out what happened. No logs = no proof.

2. Build security in from the start (especially for IoT)

If you're making internet-connected gadgets, security isn't an afterthought – it's baked into the design. That means unique passwords for every device, locking down sensitive settings, and pushing out secure updates reliably. The rules demand this now.

The DPDP Act bites hard: Forget the old IT Act loopholes. Under the new DPDP rules, sloppy security that leads to breaches can get you fined up to ₹250 Crores. That's a massive

incentive to get your security house in order.

Courts Setting the Bar: Protecting Rights & Demanding Proof

Courts play a huge role reining in government overreach and making sure digital laws actually protect people, not just power.

1. Guarding your digital rights

Free Speech Wins: Remember Section 66A of the IT Act? It was so vague it let cops arrest people for annoying Facebook posts. The Supreme Court killed it dead in 2015 (Shreya Singhal case), shouting loud and clear that free speech online matters just as much as offline.

Privacy is Fundamental: The huge Puttaswamy ruling in 2017 was a game-changer. The Court said privacy is a core right protected by the Constitution. That decision basically forced the government to finally pass the DPDP Act – showing how courts can kickstart real change.

2. No shortcuts with digital evidence

Proof needs proof: Digital evidence is easy to fake or mess with. The Supreme Court (Anvar P.V. case) laid down the law: if you want to use emails, chats, or server logs in court, you must have that special Section 65B certificate proving it's legit. No certificate? It probably gets tossed out. This forces cops and investigators to do things by the book.

Pushing cops to level up: When courts consistently demand this high bar for evidence, it pressures police forces to actually train their cyber units properly and document every step of the evidence chain – from seizure to courtroom.

Tackling new nastiness: Courts aren't stuck in the past. Orders to set up dedicated cyber cells across states show they're pushing the system to handle modern horrors like cyberstalking and online harassment, especially protecting vulnerable groups.

Bottom line: Courts act as a crucial check. They make sure tough laws meant for national security (like CERT-In's powers) don't trample your rights, while also demanding rock-solid proof to actually convict cybercriminals. It's about balance and making the rules stick.

## SOME NEWS ARTICLES RELATED TO TOPIC

India is on the brink of implementing one of its most consequential digital regulations – the Digital Personal Data Protection Act, 2023 (DPDPA), and its accompanying rules. As the

country inches closer to operationalizing this framework, there is a growing sense of urgency across the tech ecosystem. The era of soft compliance is over. Data has emerged not only as a currency for innovation but also as a growing liability, and the new regime reflects the government's sharpened focus on accountability, transparency, and regulatory control.

At its core, the DPDPA is a principles-based legislation. The draft rules currently under consultation provide a closer view of what real-world compliance will demand—particularly in areas such as consent, retention, data erasure, and breach notification. This is where the criticality of data governance truly comes into focus—not just as a question of digital infrastructure, but as a matter of strategic economic and legal consequence.

Data compliance vs practicality

The draft rules under should adopt a more risk-based and proportionate approach to age verification and parental consent. As it stands, the requirement for verifiable consent—regardless of a data principal's self-declared age—could impose disproportionate burdens on data fiduciaries, often compelling them to collect excessive data and implement rigid mechanisms that may violate principles of data minimisation. International standards like the EU-GDPR and COPPA offer a more balanced path by allowing entities to take "reasonable efforts" to verify age and parental consent, depending on the nature of the service and risk involved. The DPDPR should follow suit by clarifying that stricter age assurance measures be applied only where high-risk processing of children's data is involved, while permitting flexibility for low-risk use cases. This not only prevents unnecessary operational hurdles for businesses but also aligns better with both child protection goals and practical feasibility.

What's more, the DPDP Act also does not currently allow for "legitimate interest" as a legal basis to process data—something that other jurisdictions like the EU recognize. This could make basic business activities like internal audits, AI training, and even due diligence for M&A transactions unnecessarily difficult.

Breach reporting framework

One of the more stringent aspects of the draft rules is the breach notification framework. Data fiduciaries are required to notify both the Data Protection Board and the affected data principals of every data breach, irrespective of the perceived level of risk or harm. While a more extended window of 72 hours (or longer, subject to the Board's discretion) has been proposed for

submitting a detailed report to the Board, the timeline for notifying affected data principals is notably tighter—requiring disclosure "without delay." In addition, a preliminary breach report must also be submitted to the Board without delay, containing essential initial details. Given the varying levels of detail and specificity expected in these "without delay" notifications to the Board and data principals, there may be differing interpretations of the timeline and its practical implications.

This structure, though well-intentioned, raises concerns about the resulting desensitization of both users and regulators. In practice, most breaches require internal triage: identifying the breach, scoping its impact, initiating remediation. Reporting too early without adequate clarity could expose companies to unnecessary reputational and legal risks. Worse, it could distract from mitigating actual harm.

A more pragmatic approach would involve the introduction of a severity threshold, distinguishing minor from major breaches, and re-calibrating reporting timelines, to ensure meaningful compliance rather than mechanical disclosure.

MSMEs and the risk of overregulation

Another critical concern is the asymmetry of impact. While large corporations may struggle with scale, it is smaller businesses that will feel the heat of non-compliance most acutely. The framework as it stands does not adequately differentiate obligations by the size, scale, or risk profile of the fiduciary.

As seen in other sectors, overly burdensome compliance can stifle MSME growth. Risk-based regulation—where the extent of compliance is proportionate to the sensitivity and volume of data—needs to be institutionalised.

Governance beyond compliance

What the DPDP regime ultimately signals is the institutionalization of data governance in India. The legislation is not just about data protection. it is about shaping the way organizations think about trust, risk, and accountability. This is not merely a legal challenge—it is an organizational transformation. Policymakers must continue to listen—to industry, to civil society, and to

consumers—so that implementation is guided by dialogue rather than dictate.[7]

India has a unique opportunity to set the gold standard in digital governance—not just by protecting personal data, but by enabling the responsible unlocking of its economic value. But to achieve this, the DPDP Rules must evolve: from ambiguity to clarity, and from theory to real-world feasibility.

Five key areas to make the DPDP law more effective:
Adopt a risk-based approach to age verification and parental consent—aligned with global best practices and avoid one-size-fits-all mandates that may lead to over-collection of data and create compliance burdens.

Add "legitimate interest" as a basis for data processing—especially for due diligence in M&A and Investment activities and internal operations.

Introduce a severity-based breach reporting system and reconcile reporting timelines to avoid false alarms and regulatory fatigue.

Clarify the language requirements for user notices—especially for backend or automated services.

Differentiate compliance for MSMEs to ensure ease of doing business isn't compromised.
Encourage industry-led self-regulation under the oversight of the Data Protection Board.

## Conclusion

The digital age has transformed sovereignty into a shared, contested, and constantly evolving concept. India's cyber framework—anchored by the IT Act and DPDP Act—embodies a strong assertion of national control while seeking to uphold constitutional freedoms. However, fragmented reporting obligations, limited investigative capacity, and inconsistencies between security and privacy objectives hinder effective enforcement. The coexistence of international conventions like the Budapest and UN Cybercrime treaties demonstrates the difficulty of achieving universal norms without infringing on state autonomy. Moving forward, India must

[9] TIMES OF INDIA

focus on policy coherence, capacity-building, and international collaboration to ensure that its digital sovereignty does not become digital isolation. Establishing ethical standards for artificial intelligence, strengthening cross-border cooperation, and enhancing cyber forensic capabilities will be crucial to building a secure, rights-respecting digital future.