08.11.2026—ToI Editorial--NCLT

The NCLT functions directly under the administrative control of the MCA — the very same Ministry that frequently appears as a principal petitioner. This does not tick any boxes with respect to transparency and accountability. There are two major issues of perspective here: the apparent lack of an arm's length distance between the Centre and the NCLT; and at a broader level, the need to ensure judicial independence and separation of powers as Constitutional principles — which explains the apex court's concern. The Tribunals Reform Bill, 2026 came into being on the premise of ensuring judicial independence and separation of powers. This was following a Supreme Court judgement a year ago in *Madras High Court vs Union of India* which takes a dim view on government interference in tribunals' processes. So, it is strange that the NCLT remains outside the ambit of the new law, even as NCLAT is included.

Be that as it may, only 67 of the 320 administrative posts are now filled at the tribunal, threatening a grinding halt to operations. Among judicial and technical members, 16 posts remain empty. . Administrative and budgetary control of the NCLT and NCLAT should be shifted entirely out of the Ministry of Corporate Affairs, placing it under an independent framework. The NCLTs must pivot away from benches with two or more members to single-member benches to double institutional disposal capacity. The current 62 positions were constituted for the Companies Act; the IBC was an immense additional responsibility. Recruitment processes should help ensure zero vacancy and those for administrative staff must begin on a war footing. Rules must welcome younger, but proven, professionals in the age group of 35 to 40 assessed for knowledge of basic economics, law, and policy, encouraging them to build careers of two decades or more in the tribunals.

08.11.2026— Income Tax Case

https://economictimes.indiatimes.com/wealth/tax/rs-48-lakh-in-cash-received-from-the-sale-of-two-properties-paid-capital-gains-tax-but-received-an-income-tax-notice-taxpayer-wins-the-case-in-itat-cuttack-for-this-reason/articleshow/135635284.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

According to the submission to the ITAT, Purushottam sold two of his properties for a total of about Rs 47.54 lakh, but he took the entire amount in cash for unknown reasons. In his income tax return (ITR), Purushottam declared the property sales and also paid the due capital gains tax on these sales

The AO's investigation found Purushottam guilty of accepting cash for his property sales. So, the AO invoked the provisions of Section 269SS (read with Sections 271D and 273D) and treated the sale consideration received by Purushottam in cash as liable for violation of the provisions of Section 269SS. Consequently, the AO imposed a penalty on Purushottam.

Purushottam won because the ITAT Cuttack treated the cash as consideration received on completion of the property sale, rather than an advance covered by Section 269SS. ITAT Cuttack therefore cancelled the Section 271D penalty, holding that Section 269ST and its corresponding penalty, Section 271DA, were the relevant provisions. These were penalty proceedings, not prosecution.

Pranshu says that the Income Tax Department can again start proceedings against Purushottam, this time with the correct Section, but doing do would need to factor in the complicance with Section 275 limitation period also.

Courts have differed on whether prior satisfaction during assessment is essential. Pranshu says that changing provisions cannot revive an expired limitation period. However, the ITAT Cuttack order does not disclose enough procedural dates to conclude that fresh proceedings are definitely time-barred.

Pranshu says that if you are selling a property and got the payments in cash then at once disclose the full sale consideration, correctly compute capital gains and pay the applicable tax and interest. Also check if you are still elgible to file a revise or updated income tax return for that year.

Even though disclosure and payment of tax do not erase a breach of the cash-receipt restrictions, but this accurate reporting avoids compounding the already existing problem i.e. taking cash for selling a property.

ITAT Cuttack said that when the facts of the case are clearly seen it shows that the provisions of Section 269SS does not apply in respect of the transactions on which the AO has attempted to levy penalty under Section 271D.

ITAT Cuttack ruled that the AO should have invoked Section 269ST but instead applied Section 269SS and thus the present penalty levied under Section 271D is cancelled.

Thus even though ITAT Cuttack cancelled the Section 271D penalty the ITAT did not declare the cash receipt exempt from all other provisions of the Income-tax Act.

08.11.2026—Income Tax Case

https://aniltikotekar4smedotcom.wordpress.com/wp-admin/post.php?post=141902&action=edit

The Income Tax Department has powers to recover unpaid taxes by attaching a taxpayer’s eligible assets. However, these powers are subject to certain legal exemptions. PPF is one such investment that enjoys specific protection against attachment. This means that even when a taxpayer has outstanding tax liabilities, money lying in a PPF account cannot automatically be attached to recover those dues.

The protection comes from the Public Provident Fund Act, 1968, read with provisions of the Civil Procedure Code and the income tax recovery rules. A Gujarat High Court case involving a taxpayer whose PPF savings were attached to recover tax dues explains how these provisions work.

Does this mean all your savings are safe from tax recovery?

No. The protection available to PPF should not be confused with a blanket exemption from income tax recovery.

The Income Tax Department can still initiate recovery proceedings against eligible assets of a taxpayer. Bank deposits, shares and other financial assets may be attached in accordance with the applicable law and prescribed procedure.

08.11.2026—ET—DPDP Act and the Rules

https://aniltikotekar4smedotcom.wordpress.com/wp-admin/post.php?post=141900&action=edit

(DPDPA), 2023, and the rules notified in November 2025 are intended to give citizens greater control over their personal information and impose clearer responsibilities on organisations that collect and process it

But the success of the framework, expected to go live in May 2027, will depend on more than just legislation. It will be tested by how banks respond when customer records appear on the dark web, how digital-certification companies handle cryptographic failures, and whether organisations can prevent personal information from being copied, forwarded or stored indefinitely.

Organisations must know where personal data sits, who can access it, why it is being processed and what happens when a breach is detected

Draft standards in works with DPDPA Forum

Standard / framework	Relevant section(s)	What it covers
Consent Notice Framework	Section 5	Notice content, plain-language requirements, availability in scheduled languages, timing and record-keeping
Consent Lifecycle Framework	Section 6	Obtaining, managing and withdrawing consent; affirmative action, purpose specificity, equal ease of withdrawal and consent records
Reasonable Security Safeguards Baseline	Section 8	Security safeguards scaled according to the volume and sensitivity of data; access control, encryption, logging and vendor/processor controls
Breach Notification Protocol	Sections 8(6) and 36	Reporting personal-data breaches to the Board and affected Data Principals; severity classification, notification content, timelines and breach registers
Significant Data Fiduciary Obligations Framework	Section 10	Additional obligations, including officer appointment, periodic data audits and impact assessments
Data Protection Governance Framework	Sections 8 and 10	Internal accountability structures, roles and ownership, policy hierarchy, training and review cycles

Source: DPDPA Forum

ETPrime

For Ramsunder, data protection is an operational discipline requiring repeated practice, clear ownership and tested systems. “That is not only a legal problem, it is an operational one,” he said. “And operational problems are solved the way soldiers solve them, by drill.”

The episode –SBI--illustrates a central principle of data protection: a breach is not only a question of whether an organisation’s main database was hacked. It is also about where copies of information travel, who can access them, how third-party systems are monitored and how quickly the organisation can establish the chain of custody.

That requirement becomes difficult in large institutions with multiple vendors, legacy systems, e-mail archives, printed reports and data stored in informal channels. The most secure central database cannot compensate for a sensitive report sent to the wrong inbox or a customer document photographed on a personal phone.

The eMudhra case is significant because it shows that data protection cannot be separated from the security of the systems that authenticate websites, encrypt communications and establish digital identity. Even when no customer database is stolen, a weakness in the trust chain can create the possibility of impersonation, credential theft, financial fraud and sensitive-data exposure.

It also demonstrates why security standards, audits and incident-response procedures must be backed by technical competence and transparent disclosure. A certificate authority does not merely store information; it helps determine whether users can trust the digital environment in which information is exchanged.

Key penalties under India's DPDP Act, 2023

Non-compliance	Relevant provision	Maximum penalty
Failure by a Data Fiduciary to implement reasonable security safeguards to prevent a personal-data breach	Section 8(5)	Up to INR250 crore
Failure to notify the Data Protection Board of India and affected Data Principals about a personal-data breach	Section 8(6)	Up to INR200 crore
Breach of additional obligations relating to children's data	Section 9	Up to INR200 crore
Breach of additional obligations applicable to a Significant Data Fiduciary	Section 10	Up to INR150 crore
Breach of duties applicable to a Data Principal—for example, providing verifiably authentic information or not filing false/malicious complaints	Section 15	Up to INR10,000
Breach of any other provision of the Act or rules	General provision	Up to INR50 crore
Breach of a voluntary undertaking accepted by the Board	Section 32	Up to the penalty applicable to the underlying breach

Source: DPDP Act, Meity

ETPrime

Meaning of consent

For citizens, however, privacy risks are often much more ordinary. They arise when a hotel photocopies an identity document, when a retailer demands a mobile number for a bill, when a small business retains documents after a transaction or when a service provider shares information with multiple vendors.

At a recent conclave organised by the Forum, Parveen Goribidnur, a data and AI-governance expert, argued that India's privacy framework must be designed around the lived experience of the ordinary citizens. Recalling the difficulties faced by a farmer during biometric verification, she said digital policy must prioritise "ease of access, true inclusion, and dignity for every citizen".

That principle is particularly important for consent. Ashok Yende, advocate and Supreme Court empanelled mediator, said consent must be active, informed and linked to a clearly explained purpose. "Consent should be very active consent," he said. Citizens should understand what they are agreeing to, what data is being collected

and what the consequences may be. “They should know what are the consequences of the consent,” Yende added.

The problem is that consent notices are frequently long, technical and difficult to understand. In practice, many users click “Accept All” because they have no realistic alternative or because the service is designed to make refusal inconvenient.

AI raises the stakes

AI increases both the value and the risk of personal data. AI systems can profile individuals, infer sensitive attributes, automate decisions and reproduce errors at scale.

M Nagarajan, a Gujarat cadre IAS officer and cybersecurity expert, said regulators were often forced into a “catch-up game” because technology was advancing faster than governance systems could understand and regulate it.

But he argued that regulation should not be seen solely as a restriction on innovation. The more important question was whether the right technology was being deployed in the right context.

“Innovation is not just about novelty, but application of the right technology in the right context,” Nagarajan said.

India’s opportunity

India’s size and digital infrastructure give it an opportunity to build privacy systems at scale. Ritesh Jain, former digital head at a foreign bank, described data protection as more than a compliance exercise. Organisations must first understand their data through data lineage and then build controls around it. “You can only protect what you know,” he said.

Rashmi M Oza, a human-rights jurist, cautioned that technological progress cannot come at the cost of individual rights. Privacy must be balanced with development, innovation and public interest through legality, proportionality and minimal intrusion.

That balance will be tested repeatedly. The DPDPA’s larger promise will be realised only when these principles become routine: collect less, explain more, retain only what is necessary, secure every transfer, maintain a human check on high-impact decisions and make accountability visible at every stage.

08.11.2026-- HbA1c reading

But there is a catch: sometimes, the HbA1c reading itself can be misleading.This matters because HbA1c is one of the most commonly used tests to diagnose and monitor diabetes. Yet, despite its importance, it does not tell the complete story of a person's blood sugar control.

When glucose circulates in the bloodstream, some of it attaches to haemoglobin, the protein inside red blood cells that carries oxygen. This process is called glycation. The HbA1c test measures the percentage of haemoglobin that has glucose attached to it.An HbA1c level of 6.5% or higher falls in the diabetes range, while 5.7% to 6.4% indicates prediabetes. A result below 5.7% is generally considered within the normal range

Even when the test is accurate, it has another limitation: it does not show how blood sugar behaves throughout the day.A person could have frequent spikes after meals and episodes of low blood sugar at night, yet their average glucose reading may appear relatively stable

This is because the test captures an average rather than the individual highs and lows.

"HbA1c is a measurement of blood glucose that shows average levels for about three months but does not report daily activities or processes. There are no findings of drastic rises after meals, instances of being low in blood sugar, or highs and lows during the night. In such cases, monitoring of blood glucose is essential."This distinction matters particularly for people taking insulin or medicines that can cause hypoglycaemia (low blood sugar). An average reading alone may not reveal how frequently their glucose levels are dropping or rising.The Centers for Disease Control and Prevention (CDC) also points out that HbA1c cannot capture sudden, temporary changes in blood sugar. Readings from the past 30 days influence the result more heavily, but individual fluctuations can still remain hidden.The larger message is that diabetes management cannot always be reduced to one number on a laboratory report. HbA1c remains a valuable tool, but its accuracy depends partly on the health of the red blood cells carrying the haemoglobin.

Japan on Friday announced an emergency cybersecurity package that includes the use of artificial intelligence and cyber rescue teams after a wave of massive data breaches hit major companies and government agencies.

The emergency package comes after dozens of companies and government agencies were hit by unauthorized access to their systems and leaks of client data, prompting uneasiness across Japan.

"At this very moment, cases of unauthorized access and data breaches are occurring, causing a major impact on daily lives of the people and corporate activities," Takaichi said. "Let us increase the response capability across Japan by devoting all government resources."

Measures in the 10 billion yen ($63 million) package are designed to build a resilient society in which the public and private sectors share information, provide swift assistance to the affected and recover from damage.

It aims to acquire one of the world's highest levels of cybersecurity.

The government will enhance its capability to access servers used by hackers as a preemptive measure known as "active cyber defense," which was legalized in October.

Under the measures in the package, a "top gun" team of cybersecurity experts will be set up by the Ministry of Economy, Trade and Industry by the end of November. Team members will use AI to counter hackers and detect weaknesses in network systems. They are to cooperate with technology companies and advanced AI developers of friendly nations to keep Japan's security expertise up to date.

There will also be a "cyber rescue team" of experts from the public and private sectors to provide initial responses to companies affected by cyberattacks. A separate team will help vulnerable companies to strengthen their defenses.
