International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Bridging the Gap Between Digital Literacy and Cybersecurity Laws

Adv. Jayesh A Bhandekar

https://doi.org/10.55041/ijsmt.v2i5.584

Cite this Article: Bhandekar, A. J. A. (2026). Bridging the Gap Between Digital Literacy and Cybersecurity Laws. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.584

Abstract

There has been an explosion of digital technologies leading to an astounding contradiction. Right now we have more inter-connectedness than at any other time in history, but we also face a greater threat from advanced cybercrime threats. I am a Researcher at New Law College, Bharati Vidyapeeth University, Pune. This paper will explore how digital literacy and cybersecurity law work together in the Indian context, establishing the need to establish technical literacy as the basis for creating successful legal enforcement models. India's Information Technology Act, 2000 and recently passage of the DPDP Act, 2023 create enormous opportunities through the provision of remedies and regulatory protections; they are all premised on the false belief that everyday users have the ability to recognize digital risks and provide truly informed consent.By analyzing pivotal judicial precedents cases such as Poona Auto Ancillaries v. Punjab National Bank (2013), this article demonstrates how courts allocate liability based on idealized notions of user awareness, highlighting the severe practical consequences of systemic literacy gaps. Furthermore, a comparative look at international frameworks, including the Budapest Convention on Cybercrime and the European Union's General Data Protection Regulation (GDPR), underscores a global reliance on a digitally literate citizenry to achieve meaningful compliance.

This article examines the most significant structural impediments to cybersecurity such as complex legal terms; consistently low reported levels of cybercrime; and large, entrenched socio-economic gaps across generations; it proposes new ways to address these weaknesses and finds that one such way is by using a forward-thinking interpretation of the current judicial approach to digital literacy as part of the Right to Life and the Right to Personal Liberty found in Article 21 of the Indian Constitution; additionally, the article provides recommendations for progressive development of legislative reforms that create "privacy by default" designs, establish community-based "cyber clinics" for victims of cybercrime and require cyber laws to be integrated into all national level education systems; and finally, concludes by stating that cybersecurity is a shared responsibility because law is only an after-the-fact, reactive form of protection while digital literacy is a pre-emptive form of protection that must be put into place before a cyber-attack occurs. Therefore, the conclusion of this paper is to bridge these two gaps if we wish to develop a solid, secure, and equitable digital ecosystem.

1. Introduction: The Digital Paradox

We live at a time where we have the chance for profound changes brought about by the Internet, but at the same time we have unprecedented vulnerability to cybercrime. The new online world has developed so quickly that much of what we once referred to as human life has now been moved online. As a result, most people do not have the ability to defend themselves against cyber-attacks because many do not have the required skill set to work safely in this digital environment.

The law is supposed to be the means of holding those who cause harm through cybercrime accountable, deterring further attacks, and providing remedies for those who suffer losses resulting from cybercrime. The law cannot be enforced for damages when the injured parties do not have a fundamental understanding of how to operate safely in this new online environment. When we use the term digital literacy,the first though which comes to our mind is that being able to operate a computer/machine or send an email, or being able to use a smartphone. Digital literacy extends far beyond just these basic skills. [1]Digital literacy is an individual's ability to find, evaluate, and communicate information using digital devices or digital media platforms, as well as the ability to navigate, evaluate, create, and communicate information in digital environments. it includes using information and communication technologies to create, evaluate, and share information, and critically examining their social and political impacts.

Whereas, Cybersecurity law is in contrast to digital literacy.It defines the rules that govern the digital space and the rights and liabilities between users, businesses, and governments. Cybersecurity law also establishes what constitutes wrongdoing in the digital space .It prescribes a standard of care that must be followed by users and organizations. This article will make the argument that digital literacy is not just a social good, but is the foundational defense that will provide the basis for the practical enforcement of laws regulating cyberspace in real world. The law in general is reactive and designed to respond after an violation of rights occurs.The digital literacy empowers individuals proactively, with cognitive shields that can successfully mitigate threats before they develop into legal disputes or financial calamities.

After examining the domestic legal framework and international benchmarks, and noticing judicial trends, this study assesses the gap between what legislation assumes and what actually exists in the digital world in India and proposes a rights-based method for establishing digital education

2. The Current Legal Landscape: Domestic Framework

To see the gap between what lawmakers thought and what actually took place. First, we have to see the big laws that are changing the digital landscape of India.

2.1 The Information Technology Act, 2000

The Information Technology Act, 2000 (hereinafter "IT Act") serves as the bedrock of India's cyber-jurisprudence. Originally enacted to regulate electronic commerce and provide legal recognition to electronic transactions, further amnednments most notably in 2008 shifted its focus toward addressing an series of cybercrimes. Three specific provisions within this Act illustrate the heavy burden placed on user interaction and data management: Section 43, Section 66, and Section 72.[2]

Section 43: Civil Liability and Compensation for Unauthorized Access

Section 43 of the IT Act establishes a comprehensive civil liability framework for data protection, prescribing compensation for unauthorized access, data theft, or the introduction of malware. The statutory text states:

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,—

(a) accesses or secures access to such computer, computer system or computer network [or computer resource];

(b) downloads, copies or extracts any data, computer data base or information...

(c) introduces or causes to be introduced any computer contaminant or computer virus...

(d) damages or causes to be damaged...

(e) disrupts or causes disruption...

(f) denies or causes the denial of access...

(g) provides any assistance to any person to facilitate access...

(h) charges the services availed of by a person to the account of another person...

(i) destroys, deletes or alters any information...

(j) steals, conceals, destroys or alters...

he shall be liable to pay damages by way of compensation to the person so affected."[1]

The operational core of Section 43 turns entirely on the phrase **"without permission."** In an era dominated by advanced social engineering, phishing, and spoofing and other Cyber crimes. The conceptual boundary of "permission" becomes deeply obscured. When a user is tricked by a deceptive user interface into clicking a link that grants an external actor access to their system, the legal determination of whether "permission" was granted becomes highly problematic. The statute presumes a clear-cut binary between authorized access and forced entry, failing to account for situations where permission is extracted through technical manipulation from an uninitiated user.

Section 66: Criminalizing Dishonest Hacking

While Section 43 provides a civil remedy for damages, Section 66 introduces criminal culpability for identical acts if performed with specific criminal intent. It stipulates that if any person, **dishonestly or fraudulently**, commits any of the acts referenced under [34]Section 43, they shall be punishable with imprisonment for a term that may extend to three years, or with a fine that may extend to five lakh rupees, or both.[2]

Here, the prosecution must establish mens rea—the dishonest or fraudulent intent of the perpetrator. However, from the victim's perspective, the criminal process is often hindered by their own inability to recognize that a crime has been committed. A user lacking digital literacy may attribute a compromised system to a temporary technical glitch or user error, failing to preserve volatile electronic evidence or report the incident to law enforcement within the critical window required for digital forensics.

Section 72: Confidentiality and Privacy

Section 72 of the IT Act protects confidentiality and privacy by penalizing government officials or service providers who disclose electronic records without consent. It states that any person who, in pursuance of powers conferred under the Act or its rules, secures access to any electronic record, book, register, or document, and subsequently discloses such material to any other person without the consent of the concerned party, shall face imprisonment up to two years, a fine up to one lakh rupees, or both.3

[1] https://en.wikipedia.org/wiki/Digital_literacy

[2] Section 43, Information Technology Act, 2000 (Act No. 21 of 2000).

This section emphasizes the sanctity of **consent**, yet it assumes that the individual whose data is accessed possesses the awareness to monitor, track, and challenge unauthorized disclosures. In practice, without systemic transparency and user comprehension, provisions protecting confidentiality offer little recourse to individuals who remain entirely unaware that their personal records have been compromised or unlawfully disseminated.

2.2 The Digital Personal Data Protection Act, 2023 (DPDP Act)

The Digital Personal Data Protection Act 2023 marks the beginning of a new generation and for the first time in India there is consent-led structure for processing all forms of digital personal data within its borders.[5] The DPDP Act attempts to rectify the tension between the economic need for corporates to process individuals' personal data in accordance with law and the individual's right to manage their personal data.

The DPDP Act permits a data Principal (the individual) to consent to the processing of his/her personal data only if the data Principal provides that consent, which is clear, adequate and informed. Nevertheless, there is a significant flaw in the ascribed behavioral premise on which the DPDP Act's operational success is predicated: specifically, the assumption that the typical consumer has sufficient understanding of the extensive, complex and potentially long-term ramifications of agreeing to policies or terms of service. In reality, today's digital providers utilise convoluted contractual language, terms of service that are extremely difficult to read or comprehend, as well as lengthy disclosure statements. On occasion, the sheer volume of densely packed text creates a level of "consent fatigue", whereby users treat consent mechanisms as an obstacle, hindering their ability in accessing products and services. In many cases, users simply click the "I Accept" button without fully reviewing or understanding the extent of the data they are agreeing to have harvested, how the data will be used to develop profile information, and with whom their data will ultimately be shared.

3. International Benchmarks - A Comparative Study

It is not only in India that there is a problem when trying to match legal compliance level of users with how competent they are. An investigation into other major international frameworks has shown that the worldwide data protection and cybercrime systems rely on their citizens having a certain amount of digital literacy in order to be effective.

3.1 The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime by the Council of Europe, is an international agreement aimed at harmonising national laws, improving investigative techniques and facilitating international cooperation and coordination against those who participate in the unlawfulness associated with the activities of cybercrime.[6]Furthermore, a list of substantive offences committed through cybercrime, such as illegal access, interference with data and interference with systems, have been defined; additionally, the Convention has provided the foundation of the legal tools required for the preservation and interception of electronic data. While the Budapest Convention places a strong emphasis on international law enforcement cooperation and the capabilities of states, the enforcement mechanisms for the Convention rely on the ability of domestic populations to have the necessary technological skills to cooperate with their law enforcement authority.

2. Section 66, Information Technology Act, 2000 (Act No. 21 of 2000).

3. Section 72, Information Technology Act, 2000 (Act No. 21 of 2000).

[5] . Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

For international cooperation to be effective, victims/person in a local jurisdiction will need to identify technical breaches of their rights, preserving relevant electronic evidence and filing a formal complaint with law enforcement agencies. However, the citizens of a country do not have the functional knowledge to differentiate between an internal network failure and an externally initiated cyber attack, the international investigative channels created through the Convention will lack practical application, and will be structurally dislocated from the crimes that are occurring in the jurisdiction on the ground

3.2 The General Data Protection Regulation of the European Union.

The General Data Protection Regulation (GDPR), enacted by the EU, is the apex of global Statue on the protection and privacy of personal data of the users. In contrast to older legislation designed to protect data and privacy rights, the GDPR expressly identifies the inherent cognitive disadvantage that data controllers have in comparison to the cognitive advantage that data users have. Pursuant to Article 7 of the GDPR, to obtain valid consent, data controllers must provide a data subject with specific, informed, unambiguous, and voluntary consent must be accompanied with an affirmative act that evidences the intent of the data subject to consent. Further, the European Data Protection Board (EDPB) has advised that data subjects must be provided privacy information in a manner that uses plain and clear language, makes access to the information as simple as possible and clearly differentiates the privacy information from the general conditions of use of the data controller.

Legislative Framework	**Core Mechanism**	**Presumed User Standard**	**Practical Vulnerability**
IT Act, 2000 (India)	Unauthorized access remedies (Sec. 43) & criminal penalties (Sec. 66)	Rational actor capable of recognizing technical breaches and securing evidence.	Users misidentify attacks as system glitches, resulting in a loss of volatile forensic data.
DPDP Act, 2023 (India)	Explicit, unconditional, and informed consent framework.	Autonomous individual capable of evaluating long-term data processing risks.	"Consent fatigue" leads to blind acceptance of terms, turning consent into a superficial hurdle.
EU GDPR	Freely given, specific, and unambiguous consent via plain language.	Informed citizen supported by mandatory clear disclosures and structural design.	Despite high baseline literacy, subtle manipulative design patterns (dark patterns) still bypass intent.

Even with strict laws and rules governing how cookies operate.How much personal information companies can collect from their customers.The studies conducted in the EU indicate that people still have difficulty understanding how to deal with cookie consent (the consent form that asks for permission from a customer before using their data) and algorithmic profiling (i.e., using computers to analyze and categorize characteristics about a person based on the information collected). This reality is important information for India because while educated and technologically literate individuals living in Europe are at risk for having their data exploited, those living in a country with significant less knowledge about the Digital literacy and their rights regarding their data will be at an even higher risk for abuse. Legal protections cannot ensure privacy unless there are some type of awareness campaigns to educate individuals about their rights regarding data collection.

[6] . Council of Europe, Budapest Convention on Cybercrime, European Treaty Series - No. 185 (2001; updated 2025).

4. The "Reasonable Man" Problem in Cyberspace

There may be subsequent losses that are treated legally as occurring because of the user's actions. Under the reasonable person standard, the assumption is that the reasonable person would have acted similarly as the user in that instance. A reasonable person would not leave their house open with the keys at home but rather lock the doors, take the keys, and not have them available outside. If we transfer the standard of a reasonable person from the physical world to the digital world, it becomes problematic, especially when an everyday individual experiences phishing tactics and identifies as a rational individual.
For example, phishing is an ongoing threat to users.

A user when receives an email from their bank. Thinking it to be genuiene that appears to be authentic based on text, logos and showing urgency in that mail and need to update their personal bank credentials by clicking an "Fraudulent link" button. Therefore, the email appears to be authentic to the user. However, when the email is analyzed by a cybersecurity professional, the expert quickly identifies the email is fraudulent due to the sender's email address, and an incorrect hyperlink in the button for the user to click on. So, when the user clicks on the fraudulent button and then enters their credentials into the fraudulent email, they will potentially suffer loss as a direct result of their actions as a result of being legally deemed the reasonable person.

Phishing is a very widespread threat. You get an email designed to look like the one your banking institution would send you. It has all the correct corporate logos, the right type face and you have an urgent security alert. There is a prominent button that says "Update Now" or "Verify my Account Credentials." As a cybersecurity expert, you can very easily notice the fraudulent indicators such as the email coming from a suspiciously different address, the page doesnot open with secure protocol i.e HTTPS where S stands for secure, and the hyperlink destination not matching what it says. To the average user, the interface looks 100% authentic. As soon as the user clicks on that button and enters his/her credentials and submits them, they have not willingly surrendered their data nor consented to a security breach.

They have been manipulated through "dark patterns" that purposefully manipulated the design of the user interface through their use of cognitive biases and human blind spots.
To argue that such coerced or manipulated interactions fall within the definition of
"permission" or "consent" under either section 43 of the IT Act or section 6 of the DPDP bill is to deny the psychological and technical characteristics of digital deception. The common law "reasonable man" is effectively blind in cyberspace. Unless the reasonable man possesses specialized knowledge in this area, he is unable to exercise his capacity for reason because the technical asymmetries render the reasonable man's ability to reasonably consent to digital transactions an impossible myth.

5. Judicial Trends and Case Law Analysis

The loss that is caused from digitally illiterate users is documented in many cases throughout India's documented case law. Indian courts and adjudicating officers are regularly called upon to divide financial responsibility between negligent parties and the victim.

5.1 Poona Auto Ancillaries v. Punjab National Bank Case (2013)

A foundational precedent addressing user awareness and institutional liability is Poona Auto Ancillaries Pvt. Ltd. v. Punjab National Bank case.[7]In this case, the company fell victim to a very sophisticated phishing attack, resulting into unauthorized transfer of funds of ₹80.10 lakh from its corporate bank account through fraudulent electronic funds transfers which the attackers engineered a fake and misleading interface that closely replicated with the bank's portal, securing the M D official authentication credentials.

The Adjudicating Officer, acting under the powers of the Information Technology Act, supervised an extensive analysis of the security protocols implemented by the financial institution alongside the conduct of the user. The investigation revealed that while the bank had failed to implement adequate two-factor authentication and real-time fraud monitoring systems and constituting a clear systemic loop hole ,the MD also like a layman showed his lack of digital literacy and clicked on unauthentic email link leading to compromising the system and leading to fraudulent fund transfer.

The Adjudicating Officer ordered Punjab National Bank to pay ₹45 lakh in compensation to the complainant. Also, the court reduced the total liability of the bank and citing contributory negligence on the part of the firm's executive management. The tribunal reasoned that as a business entity managing substantial financial portfolios, the complainant was bound by a higher standard of care and should have possessed the sufficient digital awareness to verify the authenticity of the communication .

Poona Auto Ancillaries clearly shows that the Indian legal system does provide justice. It does not hesitate to impose financial penalties on victims of cybercrime if they fail to exhibit a basic level of digital awareness which is must if you hold key position in society. This case underscores a harsh legal reality: a lack of digital literacy can directly result in the loss of substantive legal remedies, leaving individuals and small businesses to bear the financial losses of cyber attacks.

5.2 The Rise of "Digital Arrest" Scams and Privacy Violations

In more recent years, Indian courts have had to grapple with increasingly coercive fraud v most notably **Digital Arrest** scams.In these cases, the fraudsters pose an agents or officer of government agencies like CBI , Narcotics , Income Tax and Police Officials where they try to convince the victims that they have been accused of some illegal activity and are being arrested online as their information has reached the enforcement agencies office.The Video usually consist of a person sitting in his government office in uniform and creating a situation of panic which doesn't allow the victims to think and ask them to follow their procedures strictly which includes sharing their Sensitve information leading to a major Financial fraud.

When these matters eventually reach the judiciary, they highlight an alarming enforcement gap. The Supreme Court of India, in various modern interpretations of cyber hygiene, has noted that technical illiteracy directly enables state-level and non-state coercion.[8] In Justice K.S. Puttaswamy V. Union of India (2017), the apex court specifically recognized informational privacy as a fundamental right under Article 21. It said that real privacy cannot be envisaged in an environment where citizens do not know how to protect their digital spaces or how to protect themselves from digital intrusion and fraud. From Poona Auto Ancillaries to the digital arrest scams of today, the judicial journey shows greater awareness in the judiciary that the law cannot protect a citizen who is completely powerless in the face of technological deception.

[7] . Poona Auto Ancillaries Pvt. Ltd. v. Punjab National Bank, Complaint No. 4 of 2012, Before the Adjudicating Officer, Information Technology Act, Maharashtra (2013).

[8] . Sajjad Husain Law Associates, Cybersecurity Laws in India: Legal Framework and Emerging Challenges, 3rd edn. (New Delhi: Legal Publications, 2025), pp. 112-115.

6. Identifying the Structural Barriers

To create effective legal and social solutions, we must first remove the structural barriers preventing the integration of digital literacy and cybersecurity enforcement. This systemic disconnect is driven by three major challenges: the complexity barrier, the enforcement gap and the socio-economic digital divide.

6.1 The Complexity Barrier: Legal Jargon vs. Technical Reality

One structural barrier relates to the use of legalise in both corporate and statutory privacy policies. For example, the average user is exposed to a far-reaching regulatory regime via long difficult "Terms & Conditions" which create a contract of adhesion, so-called "take it or leave it," in which users have zero ability to negotiate. The legal profession recognizes this and has long pointed out this disparity. The contracts created by the corporate legal community are intended to protect the corporation from risk of liability, not to provide clarity to consumers. Therefore, if a user were to read every privacy policy on every application they downloaded, they would spend hundreds of hours each year deciphering complex legal documents drafted by law experts. Since users skip this information entirely, their consent to data collection is authorized smartly under law, but not legitimate under democratic theory.

6.2 The Enforcement Gap: Under-Reporting and Forensic Destruction

An operational barrier affects law enforcement agencies in obtaining the necessary evidence to investigate digital crimes. The firing of someone who has limited knowledge as to how to use technology and is also a victim of cyber crime (online fraud, identification theft, ransomware) typically does not know how to preserve structured evidence when they locate their account or the device used in the crime. Often these victims will delete from their system or factory reset their device or un-install the app being used to try to remove the cyber crime and can destroy critical evidence, such as volatile logs, cache data, and malicious source code, making it almost impossible for the cyber cells to conduct a forensic investigation. In a country like India, where cyber crime is under-reported, due to the stigma attached to the crime, individuals not being aware of national portals where cyber crimes can be reported, and general dissatisfaction with the law enforcement agencies' ability to resolve technical crimes, the overwhelming majority of cyber crimes are never reported and as such, the true extent of crime is significantly understated and supports the criminal behavior of these bad actors.

6.3 The Social Divide.

The ultimate barrier is the unequal access to digital education . India's move to digital india has been rough and was majoritively during covid times with stark differences between rural and urban areas and between generations.

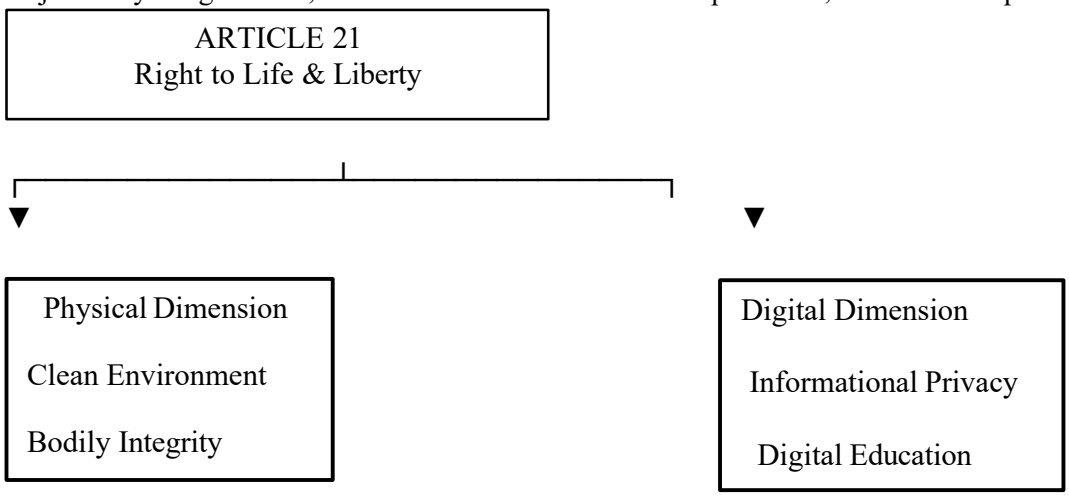
While city youth can be highly functional and skilled with smartphones and social media applications, their awareness in backend data security, encryption and phishing indicators is dangerously low which helps us to understand that how prone are they for falling prey to cyber crimes.

The risk is even more acute in rural areas, where millions of first-time internet users entered the digital market through cheap mobile data with no prior knowledge of cyber safety and digital literacy . Similarly, the old age group is disproportionately targeted by financial criminals because they are not familiar with the modern digital bank interfaces and multi-factor authentication systems. This uneven landscape means that a single, standardized legal presumption of the "reasonable user" cannot be applied fairly across a population with such disparate levels of technical competence.

7. Digital Literacy as a Fundamental Legal Right

Against the backdrop of statutory protections being perpetually challenged by systemic literacy gaps, the article proposes a progressive constitutional solution – the explicit recognition of the Right to Digital Education and Literacy as a part of the Right to Life and Personal Liberty under Article 21 of the Constitution of India.

The Supreme Court of India has in the past, widened the ambit of Article 21 by reading into it various socio-economic rights necessary for a dignified life, such as the Right to Education (Mohini Jain v. State of Karnataka) and the Right to Clean Environment (M.C. Mehta v. Union of India). In the modern age where access to majority service which include government services, Financial institutions including banking sector, healthcare and employment is almost entirely through digital platforms and social media applications, an individual/user who lacks basic digital literacy is effectively secluded from the mainstream society. He/She is stripped of their dignity which is majoritively a digital one , is left vulnerable to economic exploitation, and unable to protect their privacy.



Further, the consent under section 6 of the DPDP Act is valid only if based on an informed choice. From a constitutional standpoint, "informed consent" is not valid unless the citizen has the basic capacity to understand the terms being offered to them. When the state does not provide its citizens with basic digital literacy, but simultaneously moves essential public infrastructure onto electronic platforms, it creates systemic vulnerability. Thus, promoting digital literacy as a constitutional right and not as a policy goal would oblige the State to develop substantive and structural educational models so that every citizen has the cognitive tools to navigate the digital world in a safe manner and to assert his/her legal rights.

8. Recommendations: Bridging the Gap

To bridge the gap between digital literacy and cybersecurity law, India must move away from reactive enforcement and adopt a proactive, multi-layered strategy that integrates legislative reform, community infrastructure, and educational mandates

8.1 Legislative Reform: Mandating Privacy-by-Design

The legislature must go beyond the demand for consent to regulating the method of obtaining it. Future amendments to the DPDP Act and its implementing rules should require "Privacy-by-Design" and "Trust-by-Design" architectures for all di**gital consumer platforms.**[9] The legal system should require software developers to create user interfaces that reduce barriers to literacy.

This can be done by replacing dense text-based privacy policies with standardized, color-coded visual icons (such as a green shield for local data storage, a red arrow for third- party data sharing) and short, multilingual audio summaries. By making disclosures more transparent. The law can prevent companies from taking advantage of user and enable less techinically sound users to make more explicit, informed choices about their data.

[9] George N. Taylor, 'Legal Aspects of Cyber Security in India and International Perspectives', International Journal of Research in Law and Management, vol. 14, no. 2 (2026), pp. 45-67.

8.2 Community Infrastructure: Establishing Local Cyber Clinics

India needs to be proactive to bridge the enforcement gap and help victims of cybercrime by setting up a national network of community-based "Cyber Clinics" and local digital legal aid cells. These cells could be run by law universities and technical institutes in co-operation with state cyber police departments, like traditional clinical legal education programs and public health centres.

These clinics could be established in rural panchayats and urban neighborhoods alike as free and accessible resource centers where citizens can walk in to verify suspicious digital communications, learn basic device security settings and get immediate assistance in preserving evidence and filing formal complaints on the national cybercrime portal in case an exploit occurs.

8.3 Educational Mandates: National Cyber Law Curriculum

Fixing the digital literacy gap will require a reconstruction of our education system. The Ministry of Education and the Ministry of Electronics and Information Technology (MeitY) should work together to make cyber safety and digital law modules compulsory, easy to understand and age-appropriate in school and other curricula across the country.

This education should go beyond the simple application of software skills and should be inculcated with essential digital safety skills such as recognizing cues of social engineering , knowing rights of data privacy, practicing safe and using Strong passwords and understanding the legal outcomes of online misconduct. Cyber hygiene should be so deeply woven in the very soul of our educational systems that it produces a generations of digitally resilient citizens who can proactively protect themselves and their communities online and upgrade themselves with the demand of time[10].

9. Conclusion

India's fast digitalisation provides tremendous opportunities for socio-economic growth. It also poses many security challenges that cannot be addressed by legislation alone. As this article has shown, the Effectiveness of the IT Act, 2000 and the DPDP Act, 2023 is intrinsically limited by a growing digital literacy gap. The legal fiction of the "reasonable man" cannot survive the sophisticated realities of modern cybercrime and makes the principle of informed consent an impossible standard for millions of first-time internet users facing vast information on every second basis due to exposure through smart gadgets.

At the end of the day, cybersecurity will have to be understood as a shared responsibility of the State, business and each of us as citizens. But law , it comes after the harm has occurred, to punish the bad guys and assign civil liability which can be stated as reactive in nature rather than preventing the crime. Digital literacy, on the other hand, acts as a pre-emptive shield, arming people with the critical consciousness to avoid exploits before they occur.

Statutes and security literacy are the two pillars of true digital resilience. India can bridge this vast gap by recognizing digital literacy as a fundamental constitutional right and by implementing systemic, community-based educational reforms. This transformation will elevate Indians from passive recipients to empowered stakeholders in a safe and inclusive digital future and will help them to tranform from being just users to informed users.