The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

END-TO-END ENCRYPTION: PRIVACY'S LAST LINE OR A LEGAL BLIND SPOT?

-Shivanshi Mishra

ABSTRACT

End-to-End Encryption (E2EE) stands at the intersection of digital privacy, cybersecurity, and modern law enforcement. By ensuring that only communicating users can access message content, it creates a digital "vault" protecting intimate conversations from intermediaries, corporations, and unauthorised surveillance. Yet this same architecture presents a legal challenge when investigators seek traceability or access to communications in serious offences. This paper examines India's constitutional and statutory framework, balancing privacy under Article 21 with legitimate State interests in security and investigation. It argues that privacy and security need not be adversaries, advocating targeted investigation, judicial oversight, metadata protection, and alternative investigative tools without weakening encryption itself.

INTRODUCTION

Imagine sealing a handwritten letter inside an unbreakable vault, handing it to a courier who is incapable of opening it, and allowing only the intended recipient to unlock it. Throughout the journey, countless individuals may carry the vault, inspect its exterior, or attempt to access it, yet none can decipher its contents.

End-to-End Encryption functions on a similar principle within the digital ecosystem. It converts readable information into unintelligible cipher text that can only be restored by the communicating users' devices, effectively preventing intermediaries—including service providers—from accessing private communications.

THE CONCEPT BEHIND THE IDEA

The Information Technology Act 2000[1] does not directly talk about E2EE, but Section 2(f)[2] describes an asymmetric crypto system as "a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature."

Section 2(x)[3] defines key pair as "in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key."

End-to-end encryption relies on asymmetric cryptography for secure key exchange. Naturally, each user has a public key and a private key. The public key is used to designate a secure session, while the private key, owned only by the recipient, decrypts the message. In practice, most systems also use symmetric encryption for the substantial message content, because it's faster.

E2EE is less a single algorithm and more a communication architecture built on asymmetric cryptography principles. And that distinction matters legally, because the law often regulates access or retention of data, rather than the underlying math.

End-to-end encryption isn't just a feature, it's a philosophy rather than an ideology that became practical in today's technological mindset. It guarantees that only the sender and the conscious recipient can read a message not the app, not the server, not even the corporation that built the platform. In technical terms, encryption keys live only on user devices, and intermediaries see only cipher text that are scrambled data which in conclusion is meaningless without the key to decipher the coded data text. The concept is that at its core, E2EE is deceptively simple the data is encrypted on the sender's device and can only be decrypted by the recipient's device. The service provider like WhatsApp, Signal, or iMessage never hold the keys. This design mirrors the confidentiality of a face-to-face conversation in a locked room even if someone intercepts the data in transit, without the keys, it remains unreadable.

The importance of this technological architecture prolongs beyond convenience. In an increasingly interconnected world, private conversations, financial records, medical histories, trade secrets, legal consultations, and political opinions travel through digital networks every

[1]Information Technology Act, No.21 of 2000, India Court (2000).
[2]Information Technology Act, No.21 of 2000, India Court (2000)§2(f).
[3]Information Technology Act, No.21 of 2000, India Court (2000).§2(x).

second. Without substantial encryption, these exchanges become vulnerable not merely to hackers but also to identity thieves, hostile governments, cybercriminals, corporate spies, and unlawful surveillance. Hence, encryption has become the invisible infrastructure upon which digital confidence is assembled.

INDIAN LEGAL POSITION: BALANCING PRIVACY, ENCRYPTION AND STATE INTERESTS

Privacy may be termed as a control that an individual has on his own life, especially related to his own personal information and having decisional autonomy on making the decision of what aspects of his life, he wants to keep private and which portions he wants to disclose to the world. India's legal framework on End-to-End Encryption (herein after E2EE) is unique because, while it strongly acknowledges the individual's right to privacy, it also entrusts the State to intervene where public safety, national security, and criminal investigations demand it. As a consequence, the legality of E2EE is shaped not by a single statute but by the interaction of constitutional principles and considerable legislative frameworks.

Constitutional privacy in India flows from Article 21[4]. The constitutional foundation of digital privacy was firmly established in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[5], where a nine-judge Bench of the Supreme Court unanimously held that the right to privacy is a fundamental right under *Article 21* of the Constitution. The Court observed that privacy is ingrained to life, liberty, dignity, and individual autonomy. Keeping this in consideration it also clarified that this right is not absolute. Any restriction upon privacy must satisfy the three-fold test of legality, legitimate state purpose, and proportionality.The test of proportionality suggests that any action taken by the government should be equivalent with the needs of the situation. The concept of proportionality is also necessary so as to safeguard the individual interests of citizens and maintain balance against the public interest. In the context of End-to-End Encryption, this judgment becomes particularly substantial because it mandates the State to justify any attempt to access or weaken encrypted communications through constitutionally valid procedures rather than broad executive powers.

While the Constitution protects privacy, the *Information Technology Act, 2000* provides the statutory framework governing electronic communications. Interestingly, the Act does not

[4]INDIA CONST. art. 21.
[5]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

define or regulate End-to-End Encryption. But it recognizes the importance of secure electronic records and digital signatures while entrusting the Government under *Section 69*[6] to intercept, monitor, or decrypt information in specified circumstances such as national security, public order, sovereignty, or the investigation of cognizable offense.

The concept became more apparent with the introduction of the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*[7]*. Rule 4(2)*[8] requires significant social media intermediaries providing messaging services to identify the 'first originator' of information when ordered by a competent court or government authority for specific offences. Although the Rules expressly state that the contents of messages need not be disclosed, many technology companies argue that identifying the first originator on an End-to-End Encrypted platform may require changing the very architecture that guarantees user privacy.

India has also enacted the *Digital Personal Data Protection Act, 2023 (DPDP Act*[9]*)* to regulate the processing of digital personal data. The Act seeks to establish a framework based on lawful processing, informed consent, accountability of data fiduciaries, and protection of personal information. Though it does not specifically legislate End-to-End Encryption, its emphasis on safeguarding personal data indirectly supports the adoption of strong encryption as an effective cyber security measure. At the same time, the Act preserves certain exemptions that permit the State to process personal data for legitimate governmental functions, thereby reflecting the continuing attempt to balance privacy with governance and security concerns.

Another important legislation is the *Indian Telegraph Act, 1885*[10]*,* under which the Government own powers to intercept communications in situations involving public emergency or public safety. It was enacted long before the digital age, its surveillance provisions continue to influence India's interception framework alongside the Information Technology Act. Judicial decisions such as *People's Union for Civil Liberties (PUCL) v. Union of India (1997)*[11] emphasized that interception powers must not be exercised arbitrarily and

[6]Information Technology Act, No.21 of 2000, India Court (2000) §69.
[7]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, (India).
[8]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2) (India).
[9]Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[10]Indian Telegraph Act, No. 13 of 1885, India Code (1885).
[11]People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (India).

should be followed by procedural safeguards. These principles continue to guide contemporary debates concerning digital surveillance and encrypted communications.

Collectively, these constitutional and statutory developments demonstrate that India's legal position does not treat privacy and national security as mutually exclusive values. Instead, the law seeks to reconcile them through judicial oversight, procedural safeguards, and the constitutional doctrine of proportionality. As digital communication increasingly relies upon End-to-End Encryption, Indian courts and policymakers face the continuing challenge of ensuring that technological innovation strengthens both cyber security and constitutional freedoms without rendering legitimate law enforcement ineffective.

THE LAW ENFORCEMENT DILEMMA

There may be a possibility that the handwritten letter that was stored in that unbreakable vault contains illegal information that might lead to a crime if received. The investigator can see that the vault was sent, when, and between which individuals but not what was written. To police and intelligence agencies, this is a "going dark" problem: criminals are hidden in plain sight, behind locks that the state cannot pick.

These encrypted messages create difficulty for the government when doing an act of seeking information that provides justice. since the messages are unknown, the traceability of the originator of that message becomes quite tricky. Because all that can be perceived by the agencies is the encrypted message, which is unknown to them since they do not hold the deciphering key. The issue of traceability is a very essential issue since it helps in finding the actual culprit behind the illegal actions. The government may force the platform to find the first originator of that message, but it will be hard for the platform itself because it's just an intermediary between the sender and the recipient.

E2EE system makes it difficult for parents to keep an eye on the messages sent by their infants. This concept of system leaves no space for parental control over the use of language and matter that are coming in contact with their children as well as those that are sent by them.

Governments have responded with proposals that range from the subtle to the drastic. Security experts warn that each of these approaches weakens encryption for everyone. A backdoor that suggests that each platform must have a key of their own that can be used to encrypt any, and all messages sent by its users which was initially created for "good guys" can be discovered,

stolen, or misused by bad actors. Traceability, while aimed at curbing misinformation, can undermine anonymity and chill free speech.

The government's claim that this unbreakable vault of E2EE systems hinders justice and security questioning whether E2EE privacy's final fortress, or a legal blind spot shielding the unseen?

BEYOND THE BINARY: A THIRD WAY?

The "privacy vs. security" framing is seductive but misleading. It indicates a zero-sum game where more privacy means less safety, and vice versa. In reality, the choice is between targeted, lawful investigation and mass, systemic vulnerability.

A finer approach would:

- Preserve E2EE by default. Treat strong encryption as the bottom line for digital communication, not a peculiarity.
- Invest in alternative investigative tools. Enhance abilities in metadata analysis, financial tracking, human intelligence, and device forensics methods that do not require breaking encryption.
- Strengthen judicial oversight. Ensure that any extraordinary access is narrowly tailored, time bound, and subject to robust judicial authorization, not blanket mandates.
- Protect metadata. Even if content is encrypted, metadata reveals who spoke to whom, when, and for how long. Legal frameworks must lengthen privacy protections to metadata, not just message content.
- Promote transparency and accountability.Require platforms to publicize transparency reports on government requests, and administrations to disclose the scope and success of decryption efforts[12].

This is not a compromise, it is a recognition that security and privacy are not opposites, but mutual prerequisites of a free and safe digital society.

CONCLUSION: THE LAST LINE WORTH HOLDING

[12]Elec. Frontier Found., Defending Encryption in the U.S. and Abroad: 2025 in Review (Dec. 27, 2025), https://www.eff.org/deeplinks/2025/12/defending-encryption-us-and-abroad-2025-review.

End-to-end encryption is not perfect. It does not protect metadata, it cannot stop malware on a compromised device, and it is not an elixir for all digital harms. But it is the closest thing we have to a private conversation on a surveilled planet. To break it is to invite not just criminals, but corporations and states, into the most intimate corners of our lives.

Imagine that same unbreakable vault so secure that not even its manufacturer can open it. Inside lies a single, handwritten letter which is sealed in an envelope, addressed from one person to another. No photocopy exists. No digital scan. Only the sender and the recipient hold the key. This vault is end-to-end encryption. Now imagine a government knocks on the manufacturer's door and demands a master key. "There are criminals inside," they say. "We need to read that letter." The manufacturer replies: "We cannot. The design ensures that no one but the intended recipient can open it."

The State has two choices:

•Accept that some doors cannot be opened without breaking the vault itself and with it, the trust of every person who ever placed a letter inside.

•Or force the manufacturer to build a backdoor, knowing that once it exists, it will be copied, stolen, and misused-until no one's letter is safe again.

Encryption is not a legal blind-spot. It is the modern equivalent of that unbreakable vault. The law must learn to investigate crime without demanding that every vault be made breakable. Encryption is not the enemy of justice; it is the ground of trust in a digital society. If we lose it, we do not gain safety. We lose the last line.

Other References-

1.PRIVACY INT'L, SECURING PRIVACY: PI ON END-TO-END ENCRYPTION (2022).

2.IBM, How Does End-to-End Encryption Work? (Sept. 21, 2021).