DIGITAL ARREST: PRIVACY RIGHTS IN INDIA'S SURVEILLANCE ERA

Dr. Priyadarshini Samantray, Assistant Professor, Dhenkanal Law College, Dhenkanal, Odisha

ABSTRACT

This paper examines the paradoxical relationship between privacy protection and surveillance practices in contemporary India, focusing on two seemingly disparate yet interconnected phenomena: the epidemic of 'digital arrest' cybercrime scams and the expansion of state surveillance capabilities. While the Supreme Court's 2017 *Puttaswamy* decision established privacy as a fundamental constitutional right, implementation has been undermined by surveillance legislation that retains colonial-era executive powers and data protection laws riddled with government exemptions. The digital arrest scam epidemic—which has defrauded citizens of over ₹26 billion—exploits public trust in law enforcement through sophisticated impersonation, revealing how surveillance imagery can be weaponized by criminal networks. Simultaneously, revelations about Pegasus spyware deployment against journalists and activists demonstrate systematic abuse of legitimate surveillance tools for political monitoring. This research analyzes India's surveillance legal architecture, critiques the gaps between constitutional principles and statutory implementation, and argues that meaningful privacy protection requires comprehensive reform including judicial oversight, narrowed government exemptions, and accountability mechanisms for surveillance abuses.

Keywords: Privacy Rights, Digital Surveillance, Cybercrime, Constitutional Law, Data Protection, Telecommunications Act, Pegasus Spyware, Right to Privacy, India, Puttaswamy Judgment.

I. INTRODUCTION

How does a democracy protect its citizens when threats to privacy emerge from both criminal networks and the state itself? This question has become increasingly urgent in India, where two troubling developments are unfolding simultaneously. On one hand, sophisticated cybercriminals operating international fraud rings have perfected the art of 'digital arrest'—convincing ordinary citizens they face criminal charges through elaborate impersonation schemes. On the other, government agencies possess expansive surveillance powers with minimal oversight, as evidenced by the targeting of journalists and activists with military-grade spyware. These twin challenges reveal a fundamental crisis in how India balances security needs against individual privacy.

The irony is stark. India's Supreme Court delivered a historic ruling in 2017, declaring through *Justice K.S. Puttaswamy v. Union of India*[1] that privacy stands as a fundamental right protected by Article 21 of the Constitution. Yet seven years later, this constitutional promise remains largely theoretical. The legal infrastructure governing surveillance still bears the imprint of colonial-era controls,[2] while new legislation perpetuates rather than remedies the problem. Meanwhile, criminals exploit the very symbols of state authority—uniforms, courtrooms, official seals—to terrorize victims into surrendering their life savings. What connects these seemingly separate issues is that both represent failures to implement meaningful privacy protections in practice.

This paper argues that India's current approach creates a dangerous vacuum. Citizens lack robust protection from government overreach, yet they also remain vulnerable to criminal exploitation of surveillance imagery. The solution requires more than piecemeal reforms—it demands a fundamental rethinking of how privacy is conceptualized and protected in the digital age. By examining the digital arrest crisis alongside state surveillance practices, we can better understand why constitutional rhetoric has not translated into meaningful safeguards and what reforms might actually work.

[1]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[2]The Indian Telegraph Act, 1885, No. 13 of 1885, India Code (repealed 2023).

II. WHEN CRIMINALS WEAPONIZE SURVEILLANCE: THE DIGITAL ARREST EPIDEMIC

A. Anatomy of a Digital Arrest

A "digital arrest" refers to a form of cyber fraud in which offenders impersonate police officers or government officials through video calls and other digital platforms. The perpetrators often appear in police uniforms and use fabricated official settings to create an impression of legitimacy. Victims are falsely informed that they are involved in serious criminal activities, such as drug trafficking or money laundering, and are threatened with arrest, prosecution, or freezing of bank accounts. To avoid alleged legal consequences, victims are pressured into transferring money to so-called "secure government accounts" or converting their savings into digital assets. They are also frequently instructed not to disconnect the call or contact others during the supposed investigation. These tactics are intended to create fear, isolate the victim, and facilitate financial exploitation through psychological manipulation and deception.

This scenario has played out thousands of times across India in recent years. What makes these scams particularly effective is their psychological sophistication. The perpetrators don't simply demand money—they construct an alternate reality where the victim genuinely believes they are under criminal investigation. The statistics tell a disturbing story: roughly 40,000 reported incidents in 2022, swelling to 60,000 in 2023, then exploding to nearly 124,000 cases in 2024.[3] The financial toll has reached ₹26 billion, with government cybercrime portals documenting a tripling of complaints between 2021 and 2024.[4]

What's particularly troubling is the diversity of victims. These aren't just vulnerable elderly citizens or the technologically unsophisticated. Professionals—doctors, lawyers, bankers, even retired police officers—have fallen prey to these schemes. Some victims, unable to cope with the shame and financial devastation, have taken their own lives. The scammers demonstrate remarkable patience, sometimes keeping victims under "digital arrest" for days or even weeks, maintaining the psychological pressure until bank accounts are emptied.

[3]See Bloomberg Businessweek, Digital Arrests: India's Billion Online IDs Sparked Criminal Scam Bonanza (Dec. 5, 2025), available at https://www.bloomberg.com/features/2025-india-digital-scams/.
[4]National Cybercrime Reporting Portal, Ministry of Home Affairs, Government of India (2024).

B. The Psychology of Authority Exploitation

Why do educated, intelligent people fall for these scams? The answer lies in understanding how deeply authority bias runs in Indian society. We're conditioned from childhood to respect and obey those in uniform, to trust the symbols of government power. When someone appears to represent official authority, our critical thinking faculties often shut down. The scammers understand this perfectly, which is why they've gone to extraordinary lengths to create authentic-seeming environments—complete with fake courtrooms, actors in judge's robes, and even impersonations of India's former Chief Justice.[5]

Consider that surveys show 79 percent of Indians trust their government to do the right thing—substantially higher than trust levels in Western democracies. This isn't necessarily problematic in itself; healthy societies need some degree of institutional trust. But it creates vulnerabilities that sophisticated criminals can exploit. Moreover, India's cultural context includes a paternalistic view of government—the notion that state actions, even if restrictive, ultimately serve the greater good. This mindset makes it easier for scammers to convince victims that invasive 'verification procedures' or demands for financial transparency are legitimate exercises of state power.

C. Follow the Money: Transnational Criminal Networks

Digital arrest isn't some opportunistic individual crime. It's highly organized, transnational, and industrialized. The nerve centers operate from Southeast Asia—particularly Myanmar, Laos, and Cambodia—where weak governance and corruption create safe havens for cybercrime infrastructure. These operations employ hundreds of people, many of them Indian nationals recruited or trafficked to work in call centers that mimic police stations down to the smallest detail. The money laundering schemes involve thousands of mule accounts, cryptocurrency conversions, and complex layering designed to make funds untraceable.

What's perhaps most concerning is how these operations adapt and evolve. Government awareness campaigns briefly reduce victim numbers, but the criminals adjust their tactics. They study media reports about their own scams to refine their approaches. They monitor law enforcement responses to stay ahead of detection methods. This creates an arms race where

[5]Niti Aayog, Digital Arrest: The Modern-Day Cyber Scam (Apr. 2025), available at https://www.niti.gov.in.

traditional cybercrime prevention struggles to keep pace with increasingly sophisticated criminal innovation.

III. THE PROMISE OF PUTTASWAMY: PRIVACY AS A FUNDAMENTAL RIGHT

A. From Uncertainty to Constitutional Protection

For decades, Indian law remained ambiguous about whether citizens possessed a constitutional right to privacy. Earlier Supreme Court decisions had actually rejected this notion. The 1954 *M.P. Sharma* case and 1963 *Kharak Singh* ruling[6] both held that the Constitution did not explicitly protect privacy. This left a gaping hole in fundamental rights protection, particularly as India entered the digital age where personal data became increasingly valuable and vulnerable.

The 2017 *Puttaswamy* decision changed everything, at least in theory. A nine-judge bench unanimously reversed course, holding that privacy is indeed a fundamental right flowing from Article 21's protection of life and personal liberty.[7] Justice Chandrachud's opinion was sweeping in scope, recognizing multiple dimensions of privacy—informational, spatial, bodily, and decisional. The judgment explicitly stated that privacy constitutes 'the constitutional core of human dignity' and emphasized how privacy enables the exercise of other fundamental freedoms.[8]

This wasn't just legal doctrine—it reflected a philosophical commitment to individual autonomy. The Court recognized that in modern society, privacy enables people to make intimate personal choices, engage in political discourse without fear, and maintain control over their personal information. Without privacy, other constitutional rights become hollow. How can you exercise free speech if every communication is monitored? How can you freely associate if your movements are constantly tracked? The *Puttaswamy* judgment grasped that privacy isn't merely about keeping secrets—it's about maintaining the space for human flourishing.

[6]M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India); Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India).
[7]India Const. art. 21.
[8]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶ 127 (India).

B. THE THREE PILLARS: LEGALITY, LEGITIMACY, AND PROPORTIONALITY

Recognizing that no right is absolute, the Court established a framework for when privacy restrictions might be permissible. Any invasion must satisfy three requirements.[9] First, it must have clear legal authorization—not arbitrary executive action. Second, it must serve a legitimate state purpose like national security or criminal investigation. Third, and most importantly, it must be proportionate: the least invasive means necessary to achieve the legitimate aim.

The proportionality requirement is especially crucial for surveillance. It means government can't justify mass surveillance by invoking vague security concerns. Instead, they must show that the specific surveillance measure is genuinely necessary and that less intrusive alternatives won't work. Moreover, procedural safeguards must exist to prevent abuse—things like judicial authorization, time limits, and remedies for violations. This creates a demanding standard that, if actually applied, would prohibit most mass surveillance programs.

But here's the problem: establishing constitutional principles is one thing; implementing them through legislation and enforcement is quite another. The *Puttaswamy* decision created a legal foundation, but it required Parliament to actually reform surveillance laws and create enforcement mechanisms. As we'll see, that hasn't happened in any meaningful way.

IV. COLONIAL GHOSTS IN DIGITAL MACHINES: INDIA'S SURVEILLANCE LAWS

A. The Telecommunications Act: Old Wine in Digital Bottles

In late 2023, Parliament passed the Telecommunications Act,[10] ostensibly to modernize regulations for the digital era by replacing laws dating from British colonial rule. The government framed this as progress—finally updating nineteenth-century statutes for twenty-first-century technology. But if you look beneath the surface, what you find is essentially the same authoritarian framework with a fresh coat of paint.

Section 20 hands the government remarkably broad powers: they can intercept communications, take over telecommunications infrastructure, or suspend services entirely

[9]Id. at ¶ 180.
[10]The Telecommunications Act, 2023, No. 44 of 2023, India Code.

during 'public emergencies' or for 'public safety.'[11] The language is deliberately vague. What constitutes a public emergency? Who decides whether surveillance serves public safety? The Act provides minimal answers, leaving enormous discretion in executive hands. And critically, there's no requirement for prior judicial approval before interception begins.

Perhaps even more troubling is Section 19(f), which allows government to mandate 'standards and conformity' for encryption and data processing. This seemingly technical provision could become a tool for requiring backdoors into encrypted communications. If government can dictate encryption standards, they can potentially demand that companies build surveillance capabilities directly into their products. This fundamentally undermines end-to-end encryption, which is crucial for protecting everything from journalistic communications to business secrets to personal conversations.

Critics haven't held back in their assessment. Legal scholars have called the Act 'regressive and authoritarian,' arguing it perpetuates colonial-era state control rather than creating a framework suitable for a constitutional democracy. The timing of its passage—during a parliamentary session when nearly 100 opposition members were suspended—raises additional questions about the quality of democratic deliberation that produced it.

B. Information Technology Act: The Surveillance Parallel Track

Telecommunications aren't the only avenue for digital surveillance. The Information Technology Act provides another legal pathway through Section 69, which permits government agencies to intercept, monitor, or decrypt any digital information for purposes including sovereignty, security, public order, and criminal investigations.[12] While the accompanying 2009 Rules supposedly provide procedural safeguards—authorization requirements, review committees, and so forth—these protections have been characterized by experts as 'paper-thin.'[13]

The fundamental problem is structural. Executive officials authorize surveillance; executive committees review those authorizations. There's no independent check on this power. Judges don't evaluate whether surveillance requests meet constitutional standards before they're

[11] Id. § 20(2)(a).
[12] The Information Technology Act, 2000, No. 21 of 2000, India Code § 69.
[13] Chinmayi Arun, Paper-Thin Safeguards and Mass Surveillance in India, 26 Nat'l L. Sch. India Rev. 105, 105-114 (2014).

implemented. Citizens don't receive notice that they're being monitored, so they can't challenge the surveillance in real time. The grounds for surveillance are defined so broadly—'public order,' 'security'—that they could justify monitoring almost anyone.

Moreover, there's zero transparency. The government doesn't publish statistics on how many surveillance orders it issues, who gets targeted, or how often. This makes meaningful public accountability impossible. We literally don't know the extent to which Indian citizens are being monitored by their own government. And without transparency, we can't assess whether surveillance practices satisfy the *Puttaswamy* requirements of necessity and proportionality.

V. DATA PROTECTION IN NAME ONLY: THE DPDPA'S FATAL FLAW

A. A Framework for Privacy Protection

The Digital Personal Data Protection Act, passed in 2023 and operationalized in 2025,[14] represented India's first serious attempt at comprehensive data protection legislation. On paper, it looks quite progressive. The Act establishes clear rules about how organizations can collect and use personal data. It requires explicit consent before data processing. It gives individuals rights to access, correct, and delete their information. It mandates breach notifications. It creates a Data Protection Board with enforcement authority. These are all positive developments that bring India closer to international standards.

The Act also shows some sophistication in addressing modern data challenges. It includes provisions about data localization—requiring that Indian citizens' data be stored domestically or only transferred abroad to countries with adequate protections. It establishes penalties for violations that are substantial enough to deter corporate misbehavior. And it attempts to balance various interests: protecting privacy while enabling beneficial data uses, creating obligations for data processors while keeping compliance burdens reasonable for small businesses.

B. The Government Exemption: Swallowing the Rule

But there's a massive exception that threatens to undermine the entire framework. Section 17(2) exempts government data processing from most of the Act's requirements when undertaken for purposes including 'prevention and investigation of offenses,' 'maintenance of public order,'

[14]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code.

and 'sovereignty or integrity of India.'[15] These categories are so expansive that they effectively exclude most government surveillance from meaningful regulation.

Think about what this means in practice. A private company that wants to collect your data needs your explicit consent, must explain how they'll use it, can only keep it for necessary periods, and faces penalties if they misuse it. But a government agency investigating 'public order' (whatever that means) can collect the same data without consent, without transparency about usage, without time limits, and without meaningful oversight. This creates a double standard where citizens have substantial protection against corporate data misuse but minimal protection against government surveillance.

Civil society groups have been vocal in their criticism, and rightfully so. The exemptions don't require that government demonstrate their data processing satisfies *Puttaswamy*'s constitutional standards. There's no showing of necessity, no assessment of proportionality, no meaningful oversight mechanism.[16] The result is that the very entity with the greatest power to invade privacy—the state—faces the weakest constraints. This isn't just poor policy; it's arguably unconstitutional given the Supreme Court's clear requirements for any privacy invasion.

VI. PEGASUS: WHEN SURVEILLANCE BECOMES WEAPONIZED

A. The Scandal Unfolds

In 2021, an international journalistic investigation raised concerns regarding the possible use of Pegasus spyware in India. Pegasus, a sophisticated surveillance software developed by the Israeli company NSO Group and reportedly marketed primarily to government agencies, was alleged to have been used to target the mobile devices of certain Indian citizens. The forensic evidence was damning: over 300 Indian phone numbers appeared in a leaked database of potential surveillance targets.[17]

Pegasus is terrifying in its capabilities. Once installed—which can happen without any user action, no clicked link or downloaded file needed—it gives complete access to a device.

[15]Id. § 17(2) (providing broad exemptions for government processing of personal data).
[16]The Digital Personal Data Protection Rules, 2025, Ministry of Electronics & Information Technology Notification (Nov. 13, 2025).
[17]See Amnesty International, India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists (Dec. 28, 2023), available at https://www.amnesty.org.

Messages, emails, contacts, photos, even live audio and video through the microphone and camera. It's essentially carrying a spy in your pocket who sees and hears everything.

B. Accountability Deferred, Justice Denied

Faced with these revelations, concerned citizens and journalists filed petitions with the Supreme Court demanding an independent investigation.[18] Their argument was straightforward: if true, Pegasus deployment would represent a flagrant violation of the fundamental right to privacy the Court had so eloquently defended in *Puttaswamy*. It would also chill freedom of expression and association—how can journalists protect sources if their communications are monitored?[19]

The government's response was revealing. They refused to confirm or deny Pegasus procurement, claiming national security prevented disclosure. But this created a this created a tension between national security confidentiality and judicial accountability: if surveillance is too secret to acknowledge, how can it ever be challenged or reviewed? The Supreme Court appointed a technical committee, led by retired Justice Raveendran, to investigate. In August 2022, the committee reported finding malware on some examined phones, though they couldn't definitively confirm it was Pegasus. Crucially, the Court noted that government agencies 'did not cooperate' with the investigation.

The full committee findings haven't been made public. No accountability measures have been implemented. And the surveillance has continued—forensic investigations documented fresh Pegasus attacks on journalists as recently as October 2023.[20] The message sent by this inaction is clear: those with power can deploy invasive surveillance against critics without facing consequences. The constitutional right to privacy, so stirringly articulated in *Puttaswamy*, remains more aspiration than reality.

VII. THE PARADOX: TWO THREATS, ONE INFRASTRUCTURE

Digital arrest scams and state surveillance appear to be opposite problems: criminals impersonating authorities versus authorities potentially abusing their power. But they're

[18] Manohar Lal Sharma v. Union of India, Writ Petition (Civil) No. 637 of 2021

[19] Human Rights Watch, India: Spyware Use Violates Supreme Court Privacy Ruling (Aug. 27, 2021), available at https://www.hrw.org.

[20] See Paranjoy Guha Thakurta, Indian Supreme Court's Silence on Pegasus Legitimizes Spying on Critics, Center for the Study of Organized Hate (Dec. 9, 2024).

actually two sides of the same coin, both exploiting weaknesses in India's privacy protection framework.

Digital arrest scams operate effectively by exploiting public perceptions of institutional authority and compliance. The increasing normalization of intrusive surveillance practices and immediate obedience to purported law enforcement directives has contributed to an environment in which individuals are more likely to comply without questioning procedural legitimacy or judicial authorization. Fraudsters capitalize on this climate by imitating the appearance and methods of official agencies, thereby creating a false sense of legal compulsion. In this manner, such scams derive credibility from broader structures of authority and the public's expectation of unquestioned compliance with state power, particularly in contexts where surveillance mechanisms function with limited transparency and accountability.

Moreover, excessive government surveillance may actually make citizens more vulnerable to criminal exploitation. When people know that surveillance is pervasive and arbitrary, when they understand that privacy protections exist more in rhetoric than reality, they become desensitized. The boundaries between legitimate and illegitimate exercises of authority blur. If real police can intercept your communications without judicial warrants, why would fake police doing the same seem implausible?

The government faces genuine security challenges that require some surveillance capacity. Terrorism exists. Organized crime is real. Cybercrime—including digital arrest scams themselves—demands investigation. Nobody seriously argues for abolishing all surveillance powers. But there's a vast difference between targeted, proportionate monitoring of actual threats and mass, indiscriminate surveillance of lawful activity. The current framework fails to make this distinction adequately.

Ironically, robust privacy protections would actually strengthen security in the long run. When citizens trust that law enforcement only monitors people for legitimate reasons, with proper oversight, they're more likely to cooperate with investigations and report suspicious activity. They can distinguish between real authorities and imposters because real authorities follow transparent, accountable procedures. Conversely, when surveillance is secretive and unaccountable, it breeds cynicism and undermines the very trust that effective law enforcement requires.

VIII. A PATH FORWARD: SURVEILLANCE REFORM THAT ACTUALLY WORKS

Fixing these problems won't be easy, but the necessary reforms are actually quite clear. They just require political will to implement them.

First and most importantly, India needs real judicial oversight of surveillance. Both the Telecommunications Act and Information Technology Act should be amended to require prior judicial authorization for interception. Not rubber stamps—actual adversarial hearings where judges evaluate whether surveillance requests satisfy constitutional requirements. Authorizations should be specific about targets, time-limited, and subject to periodic review. This isn't radical; it's how most democracies handle surveillance powers.

Second, the grounds for surveillance must be narrowed and precisely defined. Vague terms like 'public order' or 'sovereignty' can justify virtually anything. Surveillance should require showing probable cause that the target is involved in serious criminal activity, with 'serious' defined by reference to specific offenses carrying substantial penalties. National security surveillance should have separate procedures with heightened safeguards given the potential for abuse.

Third, the government exemptions in the Digital Personal Data Protection Act need to be dramatically narrowed. Any government processing of personal data that implicates privacy rights should satisfy the same necessity and proportionality tests that bind everyone else. There can be specific procedures for sensitive investigations, but blanket exemptions are incompatible with constitutional privacy protections. Government agencies should be subject to the same oversight by the Data Protection Board as private entities.

Fourth, transparency is essential. The government should publish annual statistics on surveillance: how many orders were sought and granted, for what purposes, targeting how many individuals. Aggregate data can be released without compromising specific investigations. This enables public oversight and allows assessment of whether surveillance practices align with stated policies. It also helps the legislature evaluate whether surveillance laws are being used as intended or need revision.

Fifth, there must be real accountability for surveillance abuses. The Pegasus technical committee findings should be fully disclosed. If government agencies deployed spyware

against journalists and activists for political purposes, those responsible should face consequences. Without accountability for past abuses, legal protections remain theoretical. Future surveillance requests should be evaluated by judges who understand that approving unjustified surveillance carries professional consequences.

Finally, combating digital arrest scams requires more than just cybercrime enforcement. It requires rebuilding trust in institutions through genuine privacy protections. When citizens know that legitimate law enforcement follows transparent procedures, obtains judicial warrants, and faces oversight for misconduct, they can better identify imposters. Public awareness campaigns should emphasize not just scam warning signs but also what legitimate police procedures actually look like—precisely because those procedures should be standardized, transparent, and lawful.

IX. CONCLUSION: CONSTITUTIONAL PROMISES DEMAND LEGISLATIVE ACTION

India finds itself at a crossroads. The Supreme Court delivered a landmark judgment establishing privacy as a fundamental right, articulating beautiful principles about human dignity and individual autonomy. Yet the infrastructure of surveillance remains largely unchanged from colonial times, updated with modern technology but not modern democratic values. Meanwhile, sophisticated criminal networks exploit this very surveillance apparatus, stealing billions from citizens who've been conditioned to defer to authority without question.

The digital arrest epidemic tells us something important: privacy violations harm people regardless of whether perpetrators wear uniforms or operate from call centers in Myanmar. A citizen whose life savings are stolen through psychological manipulation suffers real injury. A journalist whose communications are monitored by spyware experiences real chilling effects on their ability to report freely. Both represent failures of privacy protection, just through different mechanisms.

What's needed now isn't more eloquent judicial rhetoric about privacy rights—we already have that in *Puttaswamy*. What's needed is the political courage to implement those principles through concrete legislative reform. Judicial oversight of surveillance. Narrow, precise grounds for interception. Transparency about surveillance practices. Accountability for abuses. These aren't radical demands; they're basic requirements for a constitutional democracy that takes

privacy seriously.

The question isn't whether India has the legal framework to protect privacy—the Constitution provides that. The question is whether the political system has the will to translate constitutional promises into statutory reality. Will Parliament reform surveillance laws to require real oversight? Will courts hold government accountable when surveillance violates constitutional standards? Will the public demand meaningful privacy protections rather than accepting invasive monitoring as inevitable?

India deserves better than a surveillance state dressed up with privacy rhetoric. The world's largest democracy should have a surveillance framework worthy of that designation—one that respects human dignity, enables legitimate security while constraining abuses, and protects citizens from both criminal fraud and governmental overreach. Whether India achieves this vision will determine not merely how well privacy is protected, but what kind of democracy India becomes in the twenty-first century. The constitutional promise exists. Now comes the harder part: making it real.