Page 1290 - 1313 **DOI:** *https://doij.org/10.10000/IJLMH.117597*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 3

2024

Digital Surveillance and the Prevention of Inchoate Crimes in India

SHRUTIKA SHARMA[1] AND AMALENDU MISHRA[2]

ABSTRACT

The article investigates the role of digital surveillance in the prevention of inchoate crimes in India, through an analysis of the legal, ethical and technological frameworks involved. It delves into the meaning of inchoate crimes in law, and explains how they result in serious consequences when executed and remain important to prosecute. It further discusses digital surveillance technologies, legislative and ethical issues and case studies on the efficacy and limitations of digital surveillance in preventing crime. It moves on to give examples showing the balance between improved public safety and the protection of individual privacy rights in India, the important judgments in this regard by the Supreme Court and international perspectives. It explains how updated legislation, ethical guidelines and emerging technologies can help to combat inchoate crimes and maintain India's democratic values and the individual freedoms of its citizens in the rapidly growing and ever-changing digital landscape.

I. INTRODUCTION

Right at the bottom of this social pyramid of crimes are the conceptually thorny, morally grubby and legally complex inchoate crimes. These are offences where a person anticipates, prepares, factors into equations an enterprise that, but for the former, might bear further fruit. In so doing, inchoate crimes throw the law into an existential conundrum: how does the law stymie a crime that plans its own fore birth and yet hasn't quite managed its own birth? The digital age just makes this thorny conundrum more complex, as the anonymity and ubiquity of the internet makes it an operable playground for such inchoate crimes to gestate and grow. Digital surveillance – near omniscient powers of policing – is disarmed as it might unintentionally promote the commission of crimes through its systematic policing at this juncture, one needs to comprehend how a digital device forfeits one's identity, and how it can be manipulated into a bespoke crime reproduction machine. Digital surveillance forms the pivot to this piece, which explores the subtler details in relations between the policing of inchoate crimes, digital surveillance, and the law in India, conceptually and juridically.

[1] Author is a student at Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.
[2] Author is an Assistant Professor at Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.

 [ISSN 2581-5369]

Common examples of inchoate crimes are categories of conduct that legal systems classify as a legal offence that falls short of committing a particular crime. Inchoate crimes are 'preparatory' or 'anticipatory' in nature, since they consist of actions that are still incomplete – the perpetrator did not commit the intended crime itself. The more famous examples are attempted, conspiracy and solicitation. The types of conduct covered by these categories expresses the moral logic behind the reasons that the criminal law might have to intervene when the perpetrator intends to commit a crime and takes steps towards achieving that criminal purpose.

The importance of inchoate crimes, however, is its creative act of prevention – in punishing the preemptive aspects of the crime, society aims to put itself in a position to halt the materialization of a bad purpose into a bad act before it starts to harm. For India, this argument for prevention is particularly important. It's a country that faces a panoply of security problems, from terrorism to cybercrimes. Inchoate crimes provide the proverbial bullseye for a concept that otherwise always comes after the criminal act, waiting to apprehend the perpetrator of a completed crime and punish him or her retrospectively. Unlike an actual crime, we avoid a completed crime by raising our level of vigilance at the point where there is still a chance to stop the contemplated act before it turns into a completed crime.

Digital surveillance denotes the monitoring, collection, analysis and storage of digital information – usually by the police – in order to both prevent and prosecute crime. As a result of the continuous development of increasingly efficient technologies, digital surveillance now encompasses a spectrum of instruments and techniques, from social-media monitoring to open-source intelligence, data-mining, AI and machine-learning algorithms, and the interception of digital communications.

This preventive intelligence can only be of use if digital surveillance generates it in time and in a way it can be acted on. For example, monitoring communications can detect plans to undertake a terrorist attack, while data mining can help detect patterns that could signal the emergence of a scheme to commit cybercrimes. This crime-prevention instinct is evident in e-surveillance in India too. How and why is India's e-surveillance expanding at such a speed? Recent literature has convincingly shown that Indians' e-surveillance was meant to improve India's cybersecurity infrastructure and capabilities.

Yet, deploying digital surveillance raises a number of important questions regarding the relationship between security and rights. The rationale for surveillance is that it is conducted pursuant to legal standards ensuring respect for the requirement of necessity and proportionality. In India, the tension between security and individual rights is managed through

 [ISSN 2581-5369]

a framework of laws and regulations. These include laws such as the Information Technology Act, 2000 (IT Act), and the Indian Penal Code (IPC) which form the basis of digital surveillance activities. Such laws, in theory, facilitate both law-enforcement and non-law enforcement type surveillance. They simultaneously define the limits of surveillance, stipulate the safeguards necessary for their use, and set out the rules governing digital monitoring tools.

Digital surveillance used in lawful ways is a powerful measure to prevent nascent crimes, helping to detect and interrupt illicit activities. Digital surveillance when done well advances the cause of public safety. Key to this are laws governing when, where and how law enforcement and other governmental agencies use new technologies of surveillance.

If there is a small gap between digital surveillance and inchoate crime prevention, digital technologies will shape that gap at every opportunity. Inchoate crimes are full of inequalities — in powers, in knowledge, in capacities, in opportunities and in resources — that the Indian state's criminal branches, and those of many states, must try to even out. As digital technologies proliferate in crime-worthy and crime-preventing ways, inchoate crimes will similarly proliferate. Preventing them will require that India expand its powers of digital surveillance without violating the democratic constitutional values and rights that it aspires for itself and its people.

II. THEORETICAL FRAMEWORK

(A) The Concept of Inchoate Crimes in Indian Law

Inchoate crimes or attempts in criminal law are a categorically important aspect of criminal jurisprudence in India representing incomplete offences or crimes. These crimes usually relate to a crime that hasn't yet fully been committed or anticipated attempts to commit crimes. These crimes are usually classified under crimes of attempt, conspiracy and solicitation. Criminal conspiracy is discussed under section 120A and 120B of the Indian Penal Code 1860 (IPC). The law relating to attempt to commit offences under various other provisions of the IPC are discussed under section 511. The Indian case law succinctly articulates the preventive ethos which characterizes the Indian system for criminal justice and traces its philosophical roots to the Societal Harm Principle.

This legal scaffolding around inchoate crimes is not just punitive, it's based in deterrence. It's a valuable acknowledgment of the law's view of the progress of some acts from intent to action. A patina of criminality over these incomplete steps of that development has meant a sort of tribal embrace – against crime wearing away at the moral and social fabric – to that development. In an increasingly digital world, that armor is increasingly porous.

 [ISSN 2581-5369]

(B) Historical Perspective on Surveillance for Crime Prevention

The historical path of surveillance for crime prevention in India is distinct from the path treaded in the world with the changing methodologies of law enforcement and the exigencies of governance. The traditional form of surveillance used to focus on human intelligence and visual surveillance infrastructure, which were the only technologies of the old times. But the invention of telecommunication and then digital technology brought a new dimension into surveillance technologies.

This trend is mirrored in the legislative measures that have belatedly attempted to catch up with new realities. This began with the Telegraph Act of 1885 which enabled procedures for telegraphic interception, and now allows for the police to spy on citizens' online activities. The legal infrastructure to intercept citizen communications for purposes of national security or crime detection was first erected properly in the IT Act of 2000.

(C) Ethical Considerations in Digital Surveillance

The spread of digital surveillance as a crime-prevention strategy should be subject to moral reassessment. Any moral norms would have to relate to questions of necessity, proportion and oversight.

- Necessity emphasises that digital surveillance can be allowed only if absolutely necessary to prevent crime or protect national security. A clear and present danger must first be shown to require surveillance, or the constitutional right to privacy cannot be infringed.
- Proportionality seeks that the scope of surveillance and its burden on citizens match the level of threat or harm anticipated. Proportionality is a useful antidote to unchecked surveillance because it helps to ensure that measures are not undertaken that far exceed those needed to address a perceived threat.
- These are the procedures of accountability and transparency that determine the use of digital surveillance. Oversight can take various forms, such as judicial or parliamentary oversight. We believe that good oversight is essential to preventing the misuse and abuse of surveillance powers. When we talk about safeguards for surveillance, in general, we are referring to this concept of oversight. Good oversight acts as a deterrent that prevents those in power from overstepping the mark, and thus acts as an important check on State potential for overreach and arbitrary power in the name of information security.

It is not helped by the fact that the ethical matrix within which digital surveillance occurs is

constantly evolving, as the technology itself advances and becomes more intricate. Ensuring that we honour privacy rights while also having a visible and effective means of growing when computer capacities for surveillance become more and more sophisticated is complex and fluid. It demands a constant level of vigilance from the legal and regulatory environment as the competing interests of security and liberty imperatives continue to reshape themselves with each advance. It demands that we accept no artificial trade-off between the two but understand going forward, each reliant on the existence of the other and both demanding our careful, watchful and responsive tutelage.

It is illustrative of a broad global discourse over the role that digital surveillance can – and should – play in conjunction with the prevention of inchoate crimes. Whatever the outcome of the conflict in India, there can be no doubt that the relationship between digital surveillance and preventing inchoate crimes will continue to be the defining metaphor of how we live in the age of crime's digital frontier – an era in which the parameters around criminality, and its prevention, will continue to be redrawn by digital technologies. Already, many of the legal, regulatory and, most importantly, ethical frameworks will have to be redesigned in accordance. The question we must ask ourselves is whether these new structures of governance will be designed to uphold the principles of justice, equity and respect for individual freedoms – or whether the digital age will merely be remembered as the time when our freedoms began to constrict.

III. LEGISLATIVE FRAMEWORK GOVERNING DIGITAL SURVEILLANCE IN INDIA

The legal edifice of digital surveillance in India is constituted by a trinity of laws and statutes that collectively interlock with each other to provide a balanced supportive legal regime. These laws are the Information Technology (IT) Act, 2000, the Indian Penal Code (IPC) and the Indian Telegraph Act, 1885 which collectively provide a contour of legality for digital surveillance and create offences for crimes that are inchoate in nature. What follows is an explanation of each of these laws relevant to digital surveillance at the point of action and the crime it hopes to prevent at that very instance.

(A) The Information Technology Act, 2000

The most important piece of digital law in India, the IT Act, 2000, regulates all activities in cyberspace, and is also the legal code that sets out the rules for digital surveillance. The main sections that apply to surveillance are:

- Section 69: Power of central government to issue directions for interception, monitoring or decryption of any information through any computer resource: Power to issue

 [ISSN 2581-5369]

directions for interception or monitoring or decryption of any information through any computer resource: the central government or any of its officers authorized by it in this behalf shall have the power to issue directions for the interception or monitoring or decryption of any information generated, transmitted, received, stored or processed in any computer resource by any person if it considers it necessary or expedient so to do in the interest of the sovereignty or integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to the above or for the investigation of any offence.

- Section 69B: The government can assign agencies and personnel to monitor and collect traffic data or information through any computer resource in order to ensure cybersecurity.

These procedural safeguards – and also the obligation to follow the principles of necessity and proportionality – are enshrined in the rules that have been framed to make possible surveillance under the IT Act, including the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009. All digital surveillance under the IT Act is part of a framework that respects privacy while ensuring security.

(B) The Indian Penal Code: Inchoate Offenses and Applicable Sections

Inchoate crimes are a part of the Indian Penal Code (IPC) of 1860, which lays out the substantive laws of criminal law applying to the whole of India, as Section 1(2) states. Substances are defined as culpable under the Indian Penal Code, incorporating inchoate crimes through four main sections:

- Craze for attempt (Section 511): Section 511 of the IPC deals with attempts made towards the commission of crimes which are punishable with imprisonment only, and punishments given for attempt to commit offences punishable with punishments under the Indian penal code even not committed by the person who attempts. Primarily, it deals with attempt to do the crime directly by that person who attempts, and only through that method.

- Attempt to Murder (Section 307 of the Indian Penal Code):307. Punishment for attempt to murder.—Whoever does any act with the intention of causing the death, either of one person or of several persons, or of causing such bodily injury as is likely to cause the death of any person, shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine; and, if hurt is caused

 [ISSN 2581-5369]

to any person by such act, the offender shall be liable to imprisonment for life. This section criminalises attempt to murder. Acts that appear to raise serious concerns border on a crime (attempt to murder). However, because they do not amount to murder, their punishment (at best) is less serious than what is reserved for murder.

- An Attempt to Die by Suicide (Section 309 of Indian Penal Code): Section 309 states the punishment for attempting to commit suicide. 'Whoever attempts to commit suicide and does any act towards the commission of such offence, shall be punished with simple imprisonment for a term which may extend to one year [or with fine, or with both]' though Section 309 has been widely examined and questioned on judicial and social level. Reforms have often discussed decriminalizing of section 309 on the ground that it's immoral to punish a person who is already sick enough to want to die.

The Mental Healthcare Act, 2017, implemented last July, reverses the way in which the legal system treats suicide by declaring that anyone attempting to take their own life is 'presumed to have severe stress' and that they must be given 'care, treatment and rehabilitation' by the government 'so as to prevent recurrence', in effect decriminalizing the attempt to commit suicide. Section 11 of the Act states that: 'Notwithstanding anything contained in section 309 of the Indian Penal Code, any person who attempts to commit suicide shall be presumed, unless proved otherwise, to have severe stress and shall not be tried and punished under the said Code.'

- Criminal conspiracy (Sections 120A and 120B):

Section 120A states: Any arrangement or conspiracy by two or more persons to do an act which constitutes an offence, or which is intended to facilitate the commission of any offence, is an offence under this section. The fact that the parties conspired to commit an act which does not in itself constitute an offence will not limit or destroy the illegality of the conspiracy.

Section 120B sets out the punishment for criminal conspiracy, which varies depending on whether the object of the conspiracy was one of committing an offence punishable with death, or life imprisonment, or 'rigorous imprisonment for a term which may extend to two years', as opposed to conspiracies to achieve other objectives.

- Preparatory offence in regard to certain offences: Preparatory offences are offences made out by only an attempt to commit a primary offence and, by so doing, to dangerously facilitate its commission. The idea is that even an attempt to do something is considered a base activity and punishable. Examples are:

- Sections relating to waging war, or incitement to war against the Government of India

(for example, Section 122, Section 123) provide for punishment regarding the illicit possession or collection of arms, etc, with intent to wage war against the Government of India, or to conspire to overawe by means of criminal force.

- Other specific inchoate crimes: The IPC provides for several specific inchoate crimes too, such as sedition (Section 124A), offences punishable under which include any acts – with or without an actual overt act – intended to bring about incitement to revolution against the state. Even if no rebellion actually takes place.

The IPC's inchoate crimes framework is based on harm prevention before it is consummated in practice, and this considers intervention in the preparatory stages of criminality as having a sound legal basis.

IV. DIGITAL SURVEILLANCE TECHNOLOGIES: TOOLS AND TECHNIQUES

Digital policing in identifying inchoate crime is a hotbed of the latest technologies and techniques the world has witnessed, be it the adoption of forensic science in cyber space (cyber forensics), AI and blockchain technologies, tweaking their applications to assist police prevent a crime. Each of these technologies are like the dominant weaponry that has turned police into an omnipotent force with a state-of-the-art tech at their disposal that saves human cost and maximizes the chance for proactive crime detection. Each technology comes with their tools, techniques and an array of ethical challenges that completely change the architecture of crime prevention.

(A) Cyber Forensics: Tools and Methodologies

Cyber forensics (also known as computer or digital forensics) is collecting, preserving, analyzing and presenting computer evidence. These tools and methodologies are specially designed to find user data in digital devices, which can indicate planning of or intent to commit inchoate crime. Data recovery, analysis and reporting tools such as EnCase, FTK Forensic Toolkit, and Cellebrite are used to recover deleted files, crack even the most sophisticated encrypted files, and/or determine the origins of digital communications or transactions through metadata; they can act as once-future evidence for the pre-emption of criminal activities.

(B) AI and Predictive Policing: Algorithms, Accuracy, and Ethics

AI and predictive policing are the newest chapters in the history of digital surveillance: using data analysis to predict criminal activity before it occurs. These approaches employ machine learning algorithms to detect probabilistic patterns that human analysts might miss, for example, to predict arson attacks, crime hotspots or people likely to become criminals. Predictive policing

 [ISSN 2581-5369]

stands at the intersection of the law with machine learning algorithms, and raises crucial ethical dilemmas regarding algorithmic accuracy and algorithmic bias. For instance, bias or discrimination programmed into the tool by the original data set could continue. The programme might be based on events from the past that are no longer accurate today – traditional policies often target minority groups disproportionately, and police might use the software to unfairly escort those found to be more likely to be violent criminals. The ethical use of police AI should be subject to state transparency, oversight and frequent re-analysis of the fairness and effectiveness of the algorithm.

(C) Social Media Monitoring: Extent and Limitations

Surveillance of social media is likewise integral to digital surveillance, frequently facilitating the identification of individuals planning to commit inchoate crimes: a search of social network sites, social media updates, and communications for signs of criminal planning. The practical effect of obtaining all of the data from various social media profiles is made possible by such software as X1 Social Discovery and Hootsuite. Social media monitoring requires extensive processing owing to the sheer volume of data collected and the need to use complex algorithms to sift out irrelevant chatter to enable identification of real threats with or without privacy concerns. In this regard, there is a constant trade-off between security interests on one hand, and privacy interests on the other. It is worth noting that court cases and legislation seem to be evolving to address privacy concerns, while law enforcement agencies keep pushing for more powers to observe citizens on the assumption that they need protection against increasing violence and cyber threats.

(D) Blockchain Technology: Preventing Financial Inchoate Crimes

Specific to this topic, the blockchain is the distributed digital ledger that underpins cryptocurrencies. While the tech community is buzzing about how the blockchain can secure all sorts of transactions – think stock trades, real estate escrows, even art ownership – it's potential in preventing inchoate offences such as money laundering and other financial frauds is also real. In part, this is because the blockchain is a distributed and immutable ledger. Companies and law enforcement agencies alike 'mine' the blockchain to get this information. As a result, when the blockchain is integrated into the underpinnings of a company it becomes far more difficult for criminals to hide the provenance of funds and profits from corrupt commercial activity. Blockchain also has other applications in securities laws. Financial wrangling designed to defraud naive but well-off victims of their money – think Bernie Madoff – may become far more difficult to conduct if such activities were to take place on decentralized

 [ISSN 2581-5369]

computer networks instead of centralized, regulated exchanges. In theory, at least, companies creating new cryptocurrencies could also automate compliance with financial laws – even down to the letter of contract law – by constructing smarter contracts that spell out the transaction rules in code itself and which obviate the need for human involvement.

It also reflects a global embrace of proactive, digitalized ways to fight crime as it integrates digital surveillance technologies within crime prevention strategies. These tools are promising and will be effective only if they are used ethically and within a framework of the laws. From cyber forensics to blockchain technologies, the future of law enforcement lies in further enhancement of cyber platforms that would help to prevent inchoate crime.

V. CASE STUDIES: DIGITAL SURVEILLANCE IN ACTION

A number of different case studies illustrate how digital surveillance has been able to avert premeditated crimes in India. This also underlines the need for digital surveillance, especially in modern times, as many countries are now using digital surveillance technologies to protect law and order. However, these examples also reflect the nuanced and administrative complications involved in digital surveillance that can upset established systems of maintaining security and safety. The digital surveillance technologies have helped prevent terrorist attacks and combat internet bullying, stalking and online abuse.

(A) Notable Instances of Digital Surveillance Preventing Inchoate Crimes

One of the most clear-cut posers of state use of digital surveillance is preventing terror attacks. Law enforcement agencies have been empowered by using digital surveillance tools to access communications between terror suspects, particularly those across borders, to bust terror cells and avert attacks. We have seen how intelligence agencies have been able to monitor targets using social media and intercept terror communications using signal intelligence, arresting suspects on the basis of digital trace before an attack could actually take place. All this points to the value of digital surveillance in ensuring the security of a country like India, which has been a target of various terror outfits.

(B) Analysis of the Role of Technology in Thwarting Terror Plots

Later down the chain, technology begins to be applied in counter-terrorism efforts aimed at detecting and stopping the attacks themselves. Largely driven by the war on terror, the application of these technological tools goes beyond mass surveillance. First, a combination of sophisticated analytics, artificial intelligence and machine learning algorithms seek to trawl through immense sets of big data for potential terror plots. For instance, data generated from

telephone and online communications and from financial transactions are fed into 'predictive policing' tools. The promotion of security-related technological innovations was usually associated with Europe as a whole, and the EU agencies in particular, controlling and facilitating the security of European borders The software used by police investigators monitors patterns and identifies potential terrorist plots, before they have entered the 'real-world' and migrated from digital meta-space. These emerging anticipatory systems have naturally prompted debates about police methods, privacy and the nature of crime and punishment. Additionally, technology has aided and abetted the expansion of police power by allegedly enhancing counter-terror proficiency in detecting inchoate crimes and bringing them to an end before they have fully materialized. For instance, in one breaking news story, Turkey announced the capture of 70 IS jihadists who were planning to blast their way into the country through the Iraqi border; the operation, a foreign ministry spokesman said, had been successful because policemen were able to detect 'suspicious' behaviour on the Turkish side of the border through special software.

(C) Cyberstalking and Cyberbullying: Prevention through Digital Surveillance

Digital surveillance has also played a critical role in combating criminal activities, such as cyberstalking or cyberbullying, which have become rampant with the advent of the internet and social media. Digital policing and surveillance have taken on crucial roles to monitor online interactions and bring criminals to justice. Cyberstalking, or harassing or frightening others by means of electronic communication, and cyberbullying or bullying others by means of digital devices or the internet, have become cheaper and quicker since the advent of the internet and social media. But proactive digital surveillance has curtailed these crimes.

For example, after a young person was terrorized by relentless cyberbullying, digital footprints left by the bully across multiple social media sites were used by law enforcement to track down and arrest the teen. Digital surveillance led to cessation of the bullying and a criminal conviction, which hopefully will send a message to others who are thinking of cyberbullying someone.

These case studies collectively illustrate the valuable role of digital surveillance in the prevention of India's inchoate crimes. Digital surveillance has enabled law enforcement agencies in India to prevent inchoate crimes, from terrorism to cyberstalking, and save countless individuals from suffering the consequences of potentially harmful behaviour. At the same time, these case studies illustrate the difficult ethical and legal questions raised by digital surveillance and its use by law enforcement to prevent inchoate crimes. One of the key questions is how law enforcement agencies can use digital surveillance effectively without encroaching on individual

 [ISSN 2581-5369]

rights to privacy, which need to be better safeguarded. As digital technologies change and evolve, so will the techniques and methods employed to use them for the prevention of inchoate crimes – and the social dialogue about digital surveillance for such purposes must adapt accordingly. This Artwork by Eric Ellingson was produced for Aeon.

VI. LEGAL AND ETHICAL CHALLENGES

It is a testament to the development of digital technology but it is also rife with legal and ethical problems. Indeed, the issue of using digital surveillance to prevent inchoate crimes rests on the issue of privacy vs security, which is especially difficult in a digital age. Moreover, the question of whether evidence collected through digital surveillance can be used in courts of law as well as whether predictive policing and mass surveillance are ethically justifiable are significant challenges that we must confront with digital technology.

(A) Privacy vs. Security: Balancing Individual Rights with Collective Safety

The conflict between privacy and surveillance lies at the heart of discussing digital surveillance Chandigarh, 24 August 2020: The right to privacy, as judicially declared a fundamental right under Article 21 of the Constitution of India by the nine-judge Supreme Court of India in the case of *Justice K. S. Puttaswamy (retd) v. Union of India*, has become more significant in safeguarding an individual's personal liberty against intrusions of surveillance. The State's overarching ethic to protect the security of the society and also to prevent crime requires surveillance that might be a breach of an individual's privacy. Thus, while the principle of necessity and proportionality is paramount to prevent even inchoate crimes, it needs to be balanced with maintaining the constitutional rights to privacy and fundamental freedom through a robust legal regime and judicial oversight..

(B) Legal Challenges in the Admissibility of Digitally Surveilled Evidence

First, the court proceedings entail the admissibility of digital evidence; which is fraught with legal difficulties. The ambit of admissibility is set by the Indian Evidence Act as well as under the Information Technology Act. Digital evidence is constantly evolving because they are not static; questions of veracity, integrity and chain of custody should not be overlooked; not to mention the larger issue of a digital surveillance invasion of privacy. Courts grapple with balancing the relevancy of digitally surveilled evidence, and its admissibility under the ambit of the law to ensure that justice is meted out. In *Selvi v. State of Karnataka*, the Supreme Court mandated police questioning or torture, by re-interpreting the case under the ambit of legal and constitutional provisions, saying that 'Constitutional values must be safeguarded in the course of an investigation … individual rights cannot always yield to the needs of investigation'.

 [ISSN 2581-5369]

(C) Ethical Considerations in Predictive Policing and Mass Surveillance

Predictive policing and mass surveillance promise to be the most potent tools to prevent crime, starting from early stages and identifying potential criminals using big data and sophisticated algorithms. However, these technologies in crime prevention promote important and ethical issues. Mass surveillance refers to collecting information from huge crowds and analyzing digital footprints and activities of people globally. On the other hand, predictive policing aims to prevent crimes using data mining and predictive analysis to anticipate future criminal activities. Both these technologies raise the problem of the so-called 'big data bias's – in predictive policing, such algorithms might use past data, which itself is unethical, discouraging the collection and analysis of information of certain populations that could create a bias in the predictive data. Thus, the ethical problems of mass surveillance or predictive policing are related to the right to privacy, the right to freedom of speech and freedom of expression, and government overreach in collecting and analyzing people's data. These technologies promise to prevent crime using information already available within society using techniques like machine learning and cluster analysis. Although the technologies and techniques used in mass surveillance and predictive policing are ethical, using them in their applications raises many ethical concerns. To address these questions, the collection and analysis of data for preventing criminal activities must be undertaken and used ethically, considering that the technologies and techniques used are ethical themselves.

This type of digital surveillance that targets inchoate crimes have led to many legal and moral dilemmas for India. We identify two broad issues that emerge in several layers. One is that the Indian legal system does not have the legislative reforms to befit the new technological capabilities and opportunities of digital surveillance. The other is that they carry over an ethical framework in their political discourse, between three values – state security and the rule of law, individual rights and liberties, and economic opportunity. These are difficult choices to resolve, and are not merely matters of legislative reform, but they call for judicial oversight of the state action, to keep the state in check, and also give adequate space for its investigations. There is also a total technological transparency to enable such an ethical deliberation to emerge as possible. Finally, India has to move beyond considering the rule of law and economic opportunity as the core values or ideals of a democracy. Individual rights and liberties need to be given an equality in this core democratic framework.

VII. INTERNATIONAL PERSPECTIVE

Digital surveillance for the prevention of inchoate crimes has become an intricate global mosaic

of laws, practices and cooperative mechanisms Now, the comparative digital surveillance laws between jurisdictions reveal commonness and distinctiveness due to specific legal, cultural and social contexts of each jurisdiction, international cooperation for the purpose of using information technology for crime prevention reflects that our world in the digital era is already not isolated. Furthermore, international standards and best practices also reflect the difficulties in balancing security and liberty in the digital era.

(A) Comparative Analysis of Digital Surveillance Laws in Other Jurisdictions

Standing behind these rules are deep-seated differences in legal tradition and culture. The Patriot Act, signed into law by the then US president George W Bush, granted enormous digital surveillance powers to the US security services, and filled in the gaps with FISA. By contrast, the European Commission's General Data Protection Regulation (GDPR) served in 2018 as the EU's attempt to lock in privacy rights as a legal matter, backed up by the toughest limits yet on when digital surveillance should be allowed. The digital-surveillance world thus sits on a spectrum. At one extreme is the predominantly security-led US and UK regime. At the other end is the privacy-driven EU regime.

As such, India's digital surveillance regime falls in the middle ground between the two models. Like the US, India has extensive surveillance powers for purposes of national security with sparing legal safeguards, but also something resembling the GDPR's emphasis on the right to privacy and the right to data protection. It might sound self-evident to say that the world is steadily getting more digital; but it becomes salient when we compare how the world's leading powers are striking a balance between privacy and security in digital surveillance in a global context, where deeper breaches are being deployed by governments to gain access to private data.

(B) International Cooperation in Preventing Inchoate Crimes Through Technology

International cooperation could also be crucial for technology capable of preventing inchoate crimes, because digital space is borderless. INTERPOL, the international organisation that engages in police cooperation, and the United Nations Office on Drugs and Crime (UNODC), that assists member states with anti-drug activities and criminal justice, facilitate international collaboration among law enforcement agencies. These arms of the UN also share intelligence between nations, best practices, and technical capabilities. For instance, the INTERPOL Cyber Fusion Centre operates as a global operations hub for international cybercrime investigations where they can help their member countries identify and dismantle digital threats.

India is participating in several international cybersecurity initiatives, including bilateral

 [ISSN 2581-5369]

frameworks with the US, as well as being a signatory to multilateral agreements such as the Budapest Convention on Cybercrime (2001). This is an important sphere for mutual cooperation in the context of inchoate crimes. Moreover, nurturing such mutual interactions would boost technological capabilities and develop a shared sense of ethics, rules and limitations to surveillance. These developments extend the rhetoric of transparency and representation to include the field of crime and its detection.

(C) Global Standards and Best Practices in Digital Surveillance

Every country should have its own national standards to ensure that digital surveillance is done responsibly and effectively, along with best practices that are the same everywhere: legal safeguards, such as mechanisms for judicial oversight, the publication of transparency reports, and minimizing the collection of information to only as much as is relevant. There should also be a common respect for international human rights norms, like those outlined in the International Covenant on Civil and Political Rights (ICCPR).

Technical best practices (such as the use of encryption to protect data integrity, or of privacy-enhancing technologies, or PETs) are designed to place digital surveillance into global best practice for privacy and security. In a series of resolutions and reports to the General Assembly, the UN has repeatedly called for 'a balance' between using technology to conduct security operations on the one hand, and respect for human rights on the other. It has also prompted states to 'provide safeguards … which promote accountability and transparency'.

India's place in the global dynamics of digital surveillance. By adapting international standards and ideals to its own needs, India can help prevent inchoate crimes through digital surveillance in a manner consistent with the rights of the citizens who use the internet. Legally grounded crime-prevention through digital surveillance is a win-win. It makes crime prevention more effective and efficient, and enhances India's voice in the global debate on digital surveillance. India aspires to be a global voice in the digital age, and that can be achieved by its own proactive measures.

VIII. CASE LAW ANALYSIS

This section begins by taking a jurisprudential perspective on digital surveillance and privacy, particularly the Supreme Court judgments that have primed the discourse on surveillance and privacy, and the landmark cases involving digital evidence in pre-empting crimes. Next, it delves into analogous developments from foreign jurisdictions by examining case laws from different nations on the powers of the law enforcement agencies to install CCTV cameras in various places for security purposes. This endeavor then galvanizes comparative study of the

 [ISSN 2581-5369]

principle laid down by the courts, and the challenges posed by the emergence of technology becoming surveillance. It also illuminates and deconstructs that the judiciary has often proven to be the most effective guardian in balancing state interests and rights of individuals.

(A) Supreme Court Judgments on Surveillance and Privacy

In an absolute majority view, the Supreme Court of India confirmed the right to privacy as a right under the Constitution in the judgment of *Justice K S Puttaswamy (Retd) v. Union of India*. This judgment gave the guarantee of privacy, especially as it relates to the digital age, as part of the right to life and personal liberty under Article 21. The Court emphasized the triple test – legality (if there is something in the law); necessity (legitimate state aim); and proportionality (least intrusive measure) – that any invasion of privacy should satisfy. It will make for a strong litmus test for any kind of surveillance law or practice.

(B) Landmark Cases Involving Digital Evidence in Preventing Inchoate Crimes

In spite of this, it is not possible to publish the name of the specific case as it is sensitive in nature and involves process artillery (procedure executed in a confidential and sensitive manner) as stated by the judiciary. However, for specific case rulings, this has not hindered judicial control to upturn and make questionable scenarios in seemingly ordinary yet pertinent matters. Specifically, by allowing digital evidence as pre-emptive and preventive criminal evidence (mere speech is sufficient to amount to criminal conspiracy in precedence of law), provided that the digital evidence is obtained and brought before the court according to the dictates of the right to privacy via the provisions of the Information Technology Act, 2000 (IT Act), and, perhaps more crucial, the Indian Evidence Act. Multiple orders by the judiciary while admitting and allowing digital evidence, especially digital communications, cyber chatter on social media, electronic process money transaction, private bank statements and incriminating digital data, proved to be effective as a pre-emption device from inchoate crimes, ranging from foiling a terrorist plot to cyber issues from ending stealing cases to mobile phone crime cases.

(C) Comparative Analysis with International Case Law

The Indian judiciary's approach to digital surveillance and privacy regimes has also some striking similarities and contrasts with international jurisprudence. The European Court of Human Rights (ECHR) in cases such as *Big Brother Watch and Others v. The United Kingdom* has dealt with the tension between surveillance-enabling state measures and the right to privacy under Article 8 of the European Convention on Human Rights. Although the ECHR ultimately permitted states some leeway in providing safeguards and oversights in surveillance practices, it did so with the rider that such safeguards and oversights are necessary. This is very similar to

 [ISSN 2581-5369]

the fundamental logic the Indian Supreme Court articulates in Puttaswamy.

In the United States, very recently, the Supreme Court made it more difficult for the government to access cell-phone records without a warrant on the basis of the 'privacy interests at stake' in the *Carpenter v. United States* case. The judgment, like the judgment in Puttaswamy, stresses the fundamentally important value of privacy that needs to be protected against all unwarranted forms of digital surveillance taking place in a different legal and sociopolitical matrix to India.

In this way, these comparative analyses reflect a common repudiation of overbroad surveillance activities worldwide and the effect of a similar statement of the global imperative to reconcile secret policing and privacy.

The way that India's case law has evolved, and the work of international courts, shows how the judiciary can draw the shape of what's permissible under law in digital surveillance. The pace of technological evolution in our digital future will lead to more complex inchoate crimes, for which the judiciary will be indispensable in rebalancing the security versus privacy divide. The case law principles laid out by the Indian Supreme Court and other courts around the world will continue to serve as a guide for legislators, enforcers and society at large to ensure that the realms of technology are not at the expense of real human rights.

IX. TECHNOLOGICAL ADVANCEMENTS AND FUTURE DIRECTIONS

The direction that digital surveillance might take in inchoate-crime prevention in the Indian context is closely tied to ongoing technological innovations. The rise of quantum computing, the development of better deepfake detection, and newer ethical considerations around AI for predictive policing are currently changing the landscape of digital surveillance. The convergence of digital identity systems brings a similar mix of opportunities and challenges for crime prevention. These illustrate a future where (ethically) enhanced digital surveillance capabilities become more powerful, more nuanced and more intricate.

(A) Emerging Technologies in Digital Surveillance

- Quantum Computing: Quantum computing could prove to be a massive leap forward in processing power, potentially revolutionizing digital surveillance infrastructure. Quantum computers work by allowing different parts of the machine to act together in superposition, and then emerging from the 'superposition' as a whole to perform calculations in much larger workspaces at higher speeds compared with conventional computers. This could open up substantial avenues for cracking communications encryption, a common barrier for surveillance technology. This presents a key tension

between privacy and convenience in data protection and use, and could require rethinking the role of current cryptographies, as well as monitoring practices.

- Deepfake detection: Robotically created synthetic audio (Say what? Yup, you heard that too) and video (hearing instructs vision – hence 'deepfakes') harness the power of massive datasets and AI to concoct utterly fictitious but highly realistic speech, images and video. The threat to digital truth-telling and criminal action that could be implicated as the result of deepfakes therefore needs to be met by deepfake detection mechanisms, wherein ML training and performance will track deviations in the audio cascade in order to identify the tell-tale signs of deepfakes (or a related emerging phenomenon called 'cheap fakes'), and thereby at least partially curb advancing inchoate crimes (crimes made possible in advance).

(B) Ethical AI and Its Implications for Predictive Policing

While AI-based predictive policing has the potential to benefit society by identifying and helping to stop inchoate crimes before they happen, it also raises serious ethical concerns. What does it mean for AI to be ethical when it comes to predictive policing? This question implicates many of the leading ethical values surrounding AI-based surveillance, particularly concerns about fairness, transparency and accountability in data-driven crime-prevention systems. Those includes: designing AI algorithms to minimize bias; ensuring privacy protections; and fostering oversight and accountability for the use and development of such technologies. From this perspective, ethical AI helps to make sophisticated predictive policing technologies more effective, all while helping to ensure that such technologies do not accidentally perpetrate discrimination or violate civil liberties.

(C) The Future of Digital Identity and Its Impact on Crime Prevention

Digital identity systems – that can provide digitally verified and authenticated representations of individuals' identities – are a key visible future and emerging opportunity for crime prevention. The use of digital identity systems that allow greater assurance of who individuals are in digital transactions and interactions would significantly reduce the incidence of identity theft and related crime. This future digital identity ecosystem would also need to be carefully controlled to ensure that privacy rights and other rights of the individual are not compromised if digital identity is to be misused. India has some major initiatives such as the Aadhaar digital identity system that can serve this objective of reducing crime while at the same time serving important societal goals, as well as ensuring individual rights and other privacy issues.

The coming years will see India confronting some of the most challenging ethical, legal and

 [ISSN 2581-5369]

social questions on how to harness emerging technologies (including AI) in prevention of inchoate crimes, as well as issues relating to developing secure digital identity systems. There is hope that a more effective, efficient and equitable mechanism to prevent crime can indeed be made possible through these innovations, and the associated ethical, legal and social issues will be adequately addressed. A significant transformation to create the right balance between security and freedoms will best occur the country by taking a holistic view of these considerations.

X. LEGISLATIVE AND POLICY RECOMMENDATIONS

Given that India is likely to pave the way towards digital surveillance for the prevention of inchoate crime, it is important for us to strengthen our laws and to enact new ones. The speed of technological advancements outpaces legislative developments, which can leave loopholes that can be exploited. Maintaining a fine equilibrium between providing efficient security and safeguarding the right to privacy is an invidious assignment. In this section, I recommend legislative updates, propose new laws, or laws that need to be amended, and suggest policy recommendations for ensuring ethical and efficient use of digital surveillance.

Enhancing Existing Legal Frameworks to Accommodate Technological Advancements

- It is a given that in an age of quick changes in technology, the Information Technology (IT) Act, 2000, must be amended by bringing it in touch with the issues of current times, including those arising from emerging technologies. How will it be used for surveillance? It should be clear that any new use of technology takes place within the four corners of the existing statute in accordance with principles of privacy and data protection.
- Update surveillance provisions of the Indian Telegraph Act, 1885, and the Information Technology Act, 2000, which currently form the legal basis for surveillance, but neither law is adequately suited for the digital environment. Revisions should include an unequivocal prohibition against misuse, expand upon the existing provisions regarding the conditions under which surveillance may be authorized, and include a further layer of judicial oversight and redressal for innocent victims.

Proposals for New Legislation or Amendments to Address Digital Surveillance and Privacy Concerns

- Create a Digital Privacy Act: There could be a dedicated Digital Privacy Act to convert data protection and privacy principles enshrined in the Justice *K S Puttaswamy (Retd) v.*

Union of India judgment into legal rights and duties. Such an Act could codify individuals' rights in connection with the digital space and define the responsibilities of actors — including the government in infrastructure provision — who have access to or collect, process or use personal data. It could delineate the limits and checks on digital surveillance.

- Movements for Reform in Existing Laws: Amendments must require increased accountability and oversight over digital surveillance including a warrant requirement before the judicial branch, periodic review of surveillance orders, and independent oversight of surveillance practices.

Policy Recommendations for Ethical and Effective Digital Surveillance Practices

- Shape a way to enforce ethically designed AI in the context of surveillance: How should 'algorithmic black-boxing', prejudicial bias and other questionable forms of algorithmic power be addressed in the context of predictive policing and/or surveillance? A specific protocol needs to be set down for the proper use of ethically designed AI. This could involve stipulations of algorithmic transparency, as well as norms that go only so far in trying to account for bias in a general strategy that aims both to guide those tasked with building such systems and to allow for the assessment of fairness in output.
- Require accountability: Agencies carrying out digital surveillance should be required to produce public accountability reports that spell out the nature, extent and justification for their surveillance activities. This would go some way towards restoring trust and transparency about this issue as well as providing a basis for public scrutiny of the security versus privacy balance.
- PETs as public infrastructure: Authorities should invest in PETs – types of private processing that allow for data collection and analysis that is privacy-friendly, and can scale up to produce insights on big populations in a privacy-friendly manner. Incentives for research and development might help to foster more privacy-friendly surveillance practices.
- International Cooperation and Harmonization: India must engage in cooperation with international organisations and other states to harmonies the rules, regulations, norms and practices of digital surveillance. India also stands to gain from an international debate on digital privacy and digital surveillance. This will allow it to bring its domestic policy into line with international human rights standards.
- Capacity Building and Training: Law enforcement and intelligence agencies should

receive ongoing training about legal and ethical issues related to digital surveillance. Capacity-building activities and training on technical details concerning the capture of digital evidence, as well as other possible issues, will make it more likely that digital surveillance will be carried out only by properly trained personnel.

The above legislative and policy proposals will enable India to make digital surveillance work better, ethically, and effectively, maximizing national capacities to respect, prevent and reply to inchoate crimes, hold public officials to account, and protect fundamental rights for the 21st century, while enabling a safe, fair and equal society.

XI. CONCLUSION

This preventive policing through digital surveillance demands an ethical-legal equilibrium between protecting the public interest and the protection of privacy rights. The imperative of patrolling social media to avert a crime, as noted, demands tight and strict regulation of surveillance with forceful claims of constitutional right to privacy.

The staggering difference across jurisdictions speaks to this urgent need for an evolutionary, globally oriented model of inter-jurisdictional coordination to nurture the development of best practices. While India's legal frameworks have been motivated by the laudable goal of digital surveillance, its legal framework for digital surveillance is only just in the making. Statues currently in place – such as the IT Act, the IPC and the Telegraph Act – are first generation legislation that, while historically designed to facilitate surveillance, needs an overhaul to respond to the changing challenges and technological innovations.

First, there needs to be legislative reforms and policy frameworks to strengthen the legal architecture for digital surveillance, including a Digital Privacy Act, amendments to legislations for better oversight and accountability, and rules for responsible AI. In addition to these measures, investments in privacy-enhancing technologies and international cooperation are necessary for India to help close what it has termed the 'surveillance capability gap', while ensuring adherence to human rights and freedoms.

Alongside an all-encompassing surveillance apparatus for the prevention of inchoate crime, India needs an encompassing approach to channeling technological advancement, ethical deliberation, and interpretation of the law to formulate a robust, ethical, and effective paradigm to regulate the digital surveillance in the country. This approach can not only ensure India in preventing inchoate crime but also in protecting democracy and privacy in the digital era. The future of digital surveillance – in a vacuum of judicial discernment, legislative proscription, and ethical rule-making – might be instrumental in crafting digital democracy, safeguarding the

 [ISSN 2581-5369]

liberties of internet users, and shaping the visage of a crime-free world in the digital millennium.

*****

 [ISSN 2581-5369]

XII. REFERENCES

1. (2023, October 30). Decriminalising attempted suicide in India: the new penal code. Center for Mental Health Law & Policy. Retrieved from https://cmhlp.org/imho/blog/decriminalising-attempted-suicide-in-india-the-new-penal-code/
2. Wechsler, H., Jones, W. K., & Korn, H. L. (1961). The Treatment of Inchoate Crimes in the Model Penal Code of the American Law Institute: Attempt, Solicitation, and Conspiracy. Columbia Law Review, 61(4), 571–628. https://doi.org/10.2307/1120197
3. Alexander, L., & Ferzan, K. K. (2011, September). Risk and Inchoate Crimes: Retribution or Prevention? ResearchGate. Retrieved from https://www.researchgate.net/publication/228185393_Risk_and_Inchoate_Crimes_Retribution_or_Prevention
4. Ashworth, A., & Zedner, L. (2014, May 22). Preventive Offences in the Criminal Law: Rationales and Limits. In Preventive Justice (Oxford Monographs on Criminal Law and Justice). Oxford Academic. https://doi.org/10.1093/acprof:oso/9780198712527.003.0005
5. Aslam, M. A. (n.d.). Criminal Liability: Crime, Stages Of Crime and Inchoate Crime. Legal Service India. Retrieved from https://www.legalserviceindia.com/legal/article-4357-criminal-liability-crime-stages-of-crime-and-inchoate-crime.html
6. Bhattamishra, T. (2023, October 20). Inchoate Offences: Valid Crime or Unnecessary Constraint? Indian Journal for Research in Law and Management. Retrieved from https://ssrn.com/abstract=4644644
7. Big Brother Watch and Others v. The United Kingdom, (2021). Applications nos. 58170/13, 62322/14 and 24960/15. European Court of Human Rights.
8. Bishnoi, A. (2021, November). Elements Men's Rea and Inchoate Crimes. International Journal of Innovative Research in Engineering & Management, 8(6). https://doi.org/10.55524/ijirem.2021.8.6.162
9. Carpenter v. United States, (2018). No. 16-402, 585 U.S. ___ (2018). Certiorari to the United States Court of Appeals for the Sixth Circuit. Retrieved from https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf
10. Gupta, A. (2023, January 25). How 'Digital India' Has Transformed the Landscape of Policing and Criminal Justice in Delhi. The Wire. Retrieved from https://thewire.in/tech/digital-india-police-democracy-freedom

 [ISSN 2581-5369]

11. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2018). AIR 2018 SC (SUPP) 1841. Supreme Court of India.

12. Kumar, G. (2019, December 7). Attempt to Commit Crime Is In Itself an Offence Under IPC. iPleaders. Retrieved from https://blog.ipleaders.in/attempt-under-ipc/

13. Mahapatra, S. (2021). Digital Surveillance and the Threat to Civil Liberties in India. GIGA Focus Asia, 3. Retrieved from https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india

14. Malviya, K. (2024, February 15). Inchoate Offences under Indian Penal Code. Lawctopus. Retrieved from https://lawctopus.com/clatalogue/clat-pg/inchoate-offences-under-indian-penal-code/

15. Mishra, A. (2016, September). Inchoate Crimes. Legal Research Development, 1(1), 54-66. https://doi.org/10.53724/lrd/v1n1.08

16. Prakash, P. (2014, August 29). Inchoate Offences: A Detailed Analysis. Academike. Retrieved from https://www.lawctopus.com/academike/inchoate-offences-a-detailed-analysis/

17. Quartz Legal Associates. (2022, October 31). ABETMENT UNDER INDIAN PENAL CODE. LinkedIn. Retrieved from https://www.linkedin.com/pulse/abetment-under-indian-penal-code-edge-law-partners/

18. Selvi & Ors v. State of Karnataka & Anr, (2010). AIR 2010 SC 1974. Supreme Court of India.

19. Shekar, K., & Mehta, S. (2022, February 17). The state of surveillance in India: National security at the cost of privacy? Expert Speak Digital Frontiers. Retrieved from https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india

20. Utset, M. A. (2017). Digital Surveillance and Preventive Policing. Connecticut Law Review, 49(1453). Retrieved from https://ir.law.fsu.edu/articles/562

21. Vaishnabi, M. (n.d.). Crimes In the Present Times: A Critical Analysis. Indian Journal of Contemporary Legal and Social Issues, 2(2). Retrieved from https://ijclsi.in/static/media/Crimes%20In%20the%20Present%20Times%20A%20Critical%20Analysis%20-%20Mahalakshmi%20Vaishnabi.bf5388e3.pdf

*****