Minnesota Journal of Business Law and Entrepreneurship

Volume 2026, No. 3

ISSN: 1540-3270

Criminal & Forensic Investigation with Artificial Intelligence & Their Effect on Privacy Rights: A Comparative Study of India and European Union

[1]Ms. Saloni Mishra, [2]Dr. Yamini Atreya, [3]Dr. Sumit Dalal

[1]Manav Rachna University, Faridabad, India

[2]Assistant Professor, School of Law, Manav Rachna University, Faridabad, India

[3]Assistant Professor, School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India

Abstract

Humans are living in the era of Technology and Artificial intelligence (AI) and the use of them by law enforcement and Forensic experts is not only able to solve unsolved mysterious cases but also becoming a threat to the individual's privacy. There are already some laws regarding Privacy since years such as Article 21 of Indian Constitution but with the growing global privacy concerns as AI and Technology are not limited to a certain territory, nations got alert and came up with their separate statutes to protect privacy such as DPDP Act of India, GDPR of European Union (EU) act, etc. This paper aims to identify how AI tools and Technology are beneficial for Law enforcement and other investigating agencies ultimately which will benefit the members of the society, thereafter how the privacy right of an individual got infringed due to excessive use of technology and AI by investigators, how legislature of India and European Union (EU) is trying to protect the privacy rights with the help of statutes or regulations, and finally to provide suggestions related to advanced technology and governance which will help to maintain the balance between a rightful investigation and privacy rights.

Keywords: Criminal, Investigation, Privacy, Rights, Artificial Intelligence, Technology, GDPR

1. Introduction

A human is just a body without rights, where the right to privacy is one of the most important rights of an individual.[1] There are numerous international legal frameworks, such as the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights, that recognize the right to privacy as a fundamental human right. It is essential for personal autonomy because it enables people to make choices free from outside influence. Today, privacy includes more than just personal space; it also includes anonymity, secrecy and defense against unauthorized monitoring. Concerns over privacy have grown as a result of technical breakthroughs, especially in the area of AI, since AI systems frequently need enormous volumes of personal data, including private information like biometric data. Technology can contribute to privacy protection but it also poses serious concerns, like data breaches and the abuse of artificial intelligence for spying or for investigation by police/law enforcement or Forensic teams.[2]

The 50th Chief Justice of India, Justice D.Y. Chandrachud, In a number of historic instances during his term, has broadened the definition of the right to privacy. He wrote a ruling in 2017 that upheld privacy as a basic right and

[1] Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 Harv. Int'l L.J. 81 (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485.
[2] Id.

connected it to individual liberty and human dignity. Since sexual privacy is a component of individual liberty, Justice Chandrachud was also instrumental in the decriminalization of homosexuality in 2018. In situations like Hadiya's, when the freedom to marry and make one's own judgments was maintained, he defended individual liberty. He also criticized the Aadhaar Act, claiming that by limiting a person's identity to a 12 digit number, it infringed upon their right to privacy. He upheld unmarried women's reproductive rights in 2022, acknowledging their autonomy over abortion. Justice Chandrachud has made sure that privacy is a solid foundation of individual liberties in India with his rulings.[3]

With significant rulings of Indian courts in cases like Gobind v. State of MP and PUCL v. Union of India establishing the groundwork for privacy rights, the acknowledgement of the right to privacy in India developed over time. According to the historic 2017 decision in Justice K.S. Puttaswamy v. Union of India, privacy is a fundamental right guaranteed by Article 21. The ruling also made clear that restrictions on privacy can be justified as long as they adhere to the requirements of necessity, proportionality and legality.[4]

Data security is a problem because of the numerous data breaches that have occurred in India in recent years, including those affecting MobiKwik and the CoWIN platform. To protect citizens digital data, the Digital Personal Data Protection Act 2023 was introduced. The law contains clauses pertaining to user rights, data consent and sanctions for infractions. It is still being improved, though, to handle fresh privacy issues.[5]

Legal frameworks are being put to the test as AI develops, especially with regard to accountability for AI driven activities and the effect on individual rights. Stronger privacy rules are necessary to address this rising issue and make sure that advancements in technology do not jeopardize basic human rights.[6] Countries like the EU and Germany have advanced data protection laws, with the EU's (European Union) General Data Protection Regulation (GDPR) setting a global benchmark. These laws emphasize individuals' rights to access, correct and erase personal data and they hold organizations accountable for misuse. Similarly, the U.S. is slowly moving towards stronger data protection regulations at the state level.[7]

The provided paper examines the significance of privacy rights both domestically and globally, concentrating on a number of legal frameworks and seminal instances. The right to privacy is protected as a fundamental right under Article 21 of the Indian Constitution, which upholds individual liberty and dignity. However, in some circumstances, such as those involving national security, this privilege might be restricted. The Digital Personal Data Protection Act, 2023, which governs the processing of personal data in India and guarantees that people's data is secure and their consent is acquired, is covered in the text. It also draws attention to Europe's General Data Protection Regulation (GDPR), which gives EU individuals stringent privacy rights. In order to demonstrate how the Indian judiciary understands private rights, pertinent court cases are also reviewed, including Vineet Kumar and Kharak Singh v. State of Uttar Pradesh as well as how the EU's judiciary is taking care of Privacy Rights with the help of case laws such as Österreichische Post Case[8] and Bridges v. South Wales Police.[9] In general, the text highlights the necessity of striking a balance between state objectives and privacy protection, particularly in the digital age.

---

[3] Thyagarajan Narendran, *Privacy: A Recurring Theme In Justice Chandrachud's Landmark Judgments*, SC Observer (Oct. 22, 2022), https://www.scobserver.in/journal/privacy-a-recurring-theme-in-justice-chandrachuds-landmark-judgments/.

[4] Khushi Chopra & Surya Pratap Kasaudhan, *From Constitutional Rights to Data Protection: Article 21 and Comparative Perspectives on Privacy*, Manupatra (July 2, 2024), Manupatra.

[5] Id.

[6] Geraldine Mbah, Data Privacy in the Era of AI: Navigating Regulatory Landscapes for Global Businesses, 13(2) INT'L J. SCI. & RES. ARCHIVE 2040, 2040–2058 (2024), https://doi.org/10.30574/ijsra.2024.13.2.2396.

[7] Supra Note 4, at 2.

[8] Case C-300/21, UI v Österreichische Post AG (ECLI:EU:C:2023:370).

[9] \(R\) (on the application of Bridges) \(v\) Chief Constable of South Wales Police [2020] EWCA Civ 1058.

1.1. Contributions of the Study

- The significance, reach and development of privacy rights are thoroughly examined theoretically and constitutionally in present study, especially in light of artificial intelligence and technologically assisted criminal investigations.
- It examines critically how privacy rights are impacted by AI tools like facial recognition, predictive policing, DNA analytics, big data profiling and digital surveillance systems, emphasizing both practical advantages and threats to civil liberties.
- A practical grasp of technology deployment and its legal ramifications is made possible by the paper's inclusion of empirical examples of AI assisted criminal investigations.
- In order to provide unified insights for regulatory development, it compares the privacy regimes in India, Europe (GDPR) and other countries.
- In order to place AI surveillance within the framework of constitutional protections, the study critically assesses the Indian Supreme Court's privacy jurisprudence, including significant decisions.
- The paper offers a thorough doctrinal analysis of the DPDP Act, 2023, with a focus on consent exceptions, law enforcement processing and surveillance supervision.
- It examines due process standards, necessity tests, proportionality theories and procedural safeguards that apply to AI driven investigations.
- The article proposes governance principles for AI decision making systems and extends the conversation on algorithmic transparency, explainability, accountability and auditability.
- It points out that India's current regulatory environment has poor enforcement models, oversight mechanisms lacking, institutional capability shortages and legal ambiguities.
- In order to incorporate human rights principles into AI governance, the study incorporates ethical issues such as widespread surveillance, profiling, discrimination, chilling effects and erosion of autonomy.
- It evaluates AI generated evidence's forensic integrity, chain of custody, admissibility and dependability critically for use in criminal proceedings.
- The report provides well organized institutional, legal and policy suggestions for guaranteeing privacy preserving AI research systems in India.

1.2. Significance of study

There are two opposing aspects to privacy and investigation using AI and technology. One is discussing limiting privacy in order to provide victims and society with justice and the other is discussing keeping private the possessions of specific individuals. This paper will discuss the importance of privacy rights in the modern world and the role that technology and artificial intelligence play in research. In addition, which laws and cases exist to safeguard and limit the right to privacy. And how the rights and the inquiry should be balanced.

2. Literature Review

The proposed study aims to review the various legislations and research papers related to Privacy Rights and Investigation. The objective of the Literature Review is to collect findings and gaps from various legislation or statutes, books, reports, decisions and articles published in various magazines and journals, which are referred to as the leading sources of information. Author name, year of publication, paper title, study aims, outcomes, years of references and research gaps are among the headings of the literature review table (see table 1). The legal and human rights implications of artificial intelligence are covered in the first paper; legal responsibility in the age of AI is defined in the second; data privacy in the AI era is covered in the third; using AI for data privacy is covered

in the fourth; artificial intelligence and its implications for data privacy is covered in the fifth; and challenges related to artificial intelligence and data privacy are covered in the sixth and final paper.

Table 1: Literature Review

Author	**Year**	**Title of the Paper**	**Objectives**	**Findings**	**Years of references**	**Research Gap**
Rowena Rodrigues	2020	Legal And Human Rights Issues Of AI: Gaps, Challenges And Vulnerabilities	Determine the legal and human rights concerns, gaps and solutions related to AI; map weaknesses to build resilience.	Concerns about privacy and autonomy are raised by AI; there are some restrictions in place but vulnerability mapping is required.	Primarily 2016 to 2019	Lacks depth on particular concerns, such as AI studies; limited vulnerability analysis from a broad perspective.
Ashish Chaturvedi	2023	Defining Legal Responsibility In The Age Of AI: Addressing Gaps In Data Privacy Regulation	Fill up the privacy gaps in AI data and use framework analysis to determine legal responsibility.	Current laws, such as the CCPA and GDPR, are insufficient for AI, moreover they require ethical revisions.	emphasis on the previous five years.	There is a lack of clarity on AI's legal responsibility for improper treatment of privacy.
Geraldine O Mbah	2024	Data privacy in the era of AI: Navigating regulatory landscapes for global businesses.	to examine the privacy implications of AI based investigations, real world case studies, regulatory protections, governing legal frameworks and changing judicial interpretations around the world.	While AI based investigations increase efficiency, they also increase privacy dangers, necessitating stricter legal oversight, regulatory protections, ethical application and accountability systems.	The majority of the existing literature covers the years 2018 to 2024.	Few empirical studies combine privacy harms, judicial responses, regulatory efficacy and AI research methods into cohesive comparative legal frameworks.

Kelly D. Martin, Johanna Zimmermann	2024	Artificial intelligence and its implications for data privacy	Use the process outcome continuum to categorize AI; relate it to ownership and privacy calculus.	Calculus, ownership and influence are all changed by process or outcome AI, which also raises privacy concerns.	Recent article from 2024; references to privacy and AI ecosystem research	There are few research on the junction of AI and privacy for morally sound, long term regulation.
Arokia Sushma, Dr. Ranjit Oommen Abraham, Dr. R. Haritha Devi	2025	Artificial Intelligence And Data Privacy Challenges: A Legal Perspective	Analyze India's AI privacy issues and suggest countermeasures like audits.	DPDPA 2023 is insufficient for AI monitoring; privacy is at risk from prejudice and profiling.	Visits until 2025 (DPDPA, 2023; Puttaswamy, 2017).	Despite the misuse of facial recognition by Delhi Police, there are no sector specific AI regulations.

Moreover in Table 2 there is a more specific discussion over table 1. The titles of the tables provide an explanation of the analysis and comparison of the research literature. "Focus on Data Privacy" indicates whether or not privacy rights are the study's primary topic. "Span (in Years)" denotes the time frame that the evaluated material covered. The number of sources examined is indicated by "# Articles Reviewed," demonstrating the breadth of the study. "Multi Jurisdiction Coverage" refers to the study of laws from many nations. "# Key Legal Issues Discussed" represents the number of significant legal issues that are looked at. "Legal Frameworks" are the laws and constitutional clauses that have been examined. Moral issues like justice and decency are highlighted in "Ethical Issues." "Regulatory Gaps" highlights flaws in current legislation. "Applications" refers to the practical applications of technology and artificial intelligence. "Policy Recommendations" offer recommendations for changes to the law and regulations. Here in table ✓ means Discussed in Detail, **δ** means partially discussed , ✗ stands for not discussed and ≅ means approximately (see table 2). In addition to this at last there is a clear indication of the present research work and how it is different from other papers. In present study data privacy in the context of artificial intelligence and technology based criminal investigations is the main topic of the current study (2026). It examines scholarly and legal advancements from 1963 to 2026, demonstrating how privacy rights have changed in tandem with technology advancement. To guarantee thorough and impartial coverage, the study examines over forty reliable sources, including research papers, statutes, court rulings and policy reports. By analyzing Indian, European and international legal frameworks, it takes a multi jurisdictional perspective. About 10 major legal topics are examined, including the legitimacy of AI driven surveillance, the right to privacy guaranteed by Article 21 of the Constitution, data protection obligations, algorithmic responsibility and evidential difficulties. With an emphasis on consent, lawful processing and purpose limitation, the article examines important laws such as the Indian Constitution, the Digital Personal Data Protection Act, 2023 and the General Data Protection Regulation. Along with identifying regulatory inadequacies, it also discusses ethical issues and the dangers of mass surveillance, profiling and prejudice. The report offers policy oriented proposals to improve privacy protection while permitting the ethical use of AI in criminal justice systems by looking at real world applications and case studies.

Table 2: Comparison Checklist

Reference	Focus on Data Privacy	Span (in years)	# Articles Reviewed	Multi Jurisdiction Coverage	#Key Legal Issues Discussed	Legal Framework	Ethical Issues	Regulatory Gaps	Applications	Policy Recommendations
Rodrigues (2020)	✓	2005-2019	≅60	✓	≅12	✓	✓	✓	δ	✓
Chaturvedi (2023)	✓	2012-2022	≅45	δ	≅8	✓	δ	✓	✗	✓
Mbah (2024)	✓	2012-2023	≅70	✓	≅11	✓	✓	✓	δ	✓
Martin & Zimmermann (2024)	✓	2015-2023	≅85	✓	≅10	✓	✓	δ	✓	✓
Sushma, Abraham & Devi (2025)	✓	2015-2024	≅60	✓	≅10	✓	δ	✓	✗	✓
Present Study	✓	1963-2026	≅40	✓	≅10	✓	✓	✓	✓	✓

3. AI Based Investigation's Impact on Privacy

This section of research will focus on the importance of Right to Privacy, how AI and Technology are contributing to investigation and what is the impact of Right to AI and Technology over Right to Privacy.

3.1. Right to Privacy: The right to privacy is the most basic right of an individual. In a world where surveillance is increasing, the right to privacy is crucial for preserving individual liberty and dignity. It guarantees legal supervision, keeps governments from over monitoring and shields people from power abuse.[10] As seen by

[10] Emmaline Soken-Huberty, *10 Reasons Why Privacy Rights are Important*, Human Rights Careers, https://www.humanrightscareers.com/issues/reasons-why-privacy-rights-are-important/ (last visited May 9, 2026).

significant data scandals, privacy regulations also prevent businesses from exploiting personal information for manipulation or financial gain. Robust legislative safeguards guarantee responsibility for data breaches and offer victims remedies.[11] By enabling people to make decisions about their personal lives without fear or coercion, privacy protects individual autonomy. By granting people authority over their personal information, it facilitates secure use and informed consent. By shielding independent thought and avoiding self censorship, privacy promotes freedom of expression. By preventing the spread of inaccurate or damaging information, it protects reputations. Privacy enhances trust in the economic, social and healthcare systems by guaranteeing data protection.[12] Last but not least, it fortifies democracy by safeguarding the rights to association, belief and protest while shielding people from excessive surveillance and technological abuse.[13] (see figure 1).

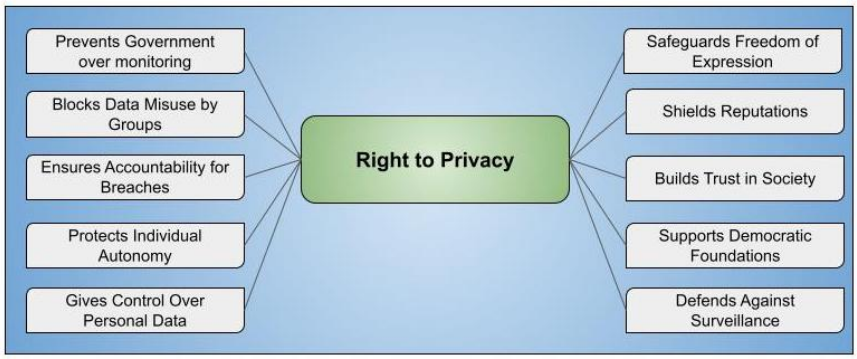

Figure 1: Importance of Privacy Rights

Out of 194 countries 137 countries have the right to privacy in their provisions. Among all countries 71% countries are with legislation regarding privacy rights, 9% with draft legislation and 15% countries with no legislation over privacy and there are also countries with no data and they are 5%.[14]

Many international legal frameworks, including Article 12 of the 1948 Universal Declaration of Human Rights and Article 17 of the 1966 International Covenant on Civil and Political Rights, recognize the right to privacy as a basic human right. This right, which permits people to make their own decisions without outside intervention, is essential to individual autonomy. Maintaining secrecy, protecting one's dignity and avoiding unjustified state surveillance are all aspects of privacy.[15]

Privacy now encompasses secrecy, anonymity and seclusion in addition to limiting access to oneself. In the modern world, technology is crucial for maintaining privacy but it also raises significant risks, like data breaches and AI driven problems like deepfakes. As a result, national and international legislation to protect personal data has been developed (Chopra & Kasaudhan, 2024).

3.2. AI & Technology in Investigation: AI enables law enforcement organizations to operate more efficiently, intelligently and precisely, it is becoming increasingly significant in contemporary criminal investigations. AI tools make it easier to identify suspects, trace movements and review evidence since they can quickly evaluate vast amounts of data. Investigators can swiftly and accurately identify people thanks to technologies like automatic

[11] Id.

[12] Daniel J. Solove, *10 Reasons Why Privacy Matters*, TeachPrivacy (Jan. 20, 2014), https://teachprivacy.com/10-reasons-privacy-matters/.

[13] Vajiram & Ravi, *Right to Privacy, Evolution, Significance, Challenges*, Vajiram & Ravi (Jan. 5, 2026), https://vajiramandravi.com/upsc-exam/right-to-privacy/.

[14] UN Trade & Dev. (UNCTAD), *Global Cyberlaw Tracker: Summary of Adoption of E-Commerce Legislation Worldwide*, https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide (last visited May 9, 2026).

[15] Supra Note 11, at 7.

fingerprint identification, facial recognition, iris scanning and license plate recognition.[16] By utilizing biometric analysis and sophisticated pattern recognition, these systems decrease human error and increase accuracy. By managing complicated data that might normally take months to process manually, AI also boosts productivity. This enables investigators to efficiently handle increasing workloads and solve cases more quickly.[17] AI also helps predictive policing by seeing crime trends and possible threats and it enhances forensic analysis by improving the inspection of evidence. Despite all of AI's benefits, there remain privacy, bias and civil rights issues that call for strict regulation and ethical application. The necessity to strike a balance between innovation and moral protections is emphasized by the U.S. Department of Justice. All things considered, if AI is applied cautiously and openly, it has the potential to revolutionize criminal investigations by enhancing identification, expediting procedures and enhancing public safety.[18]

3.3. Impact of AI & Technology over Right to Privacy: Because AI in investigations allows for continuous, covert surveillance that frequently eschews legal protections like warrants, privacy hazards have increased.[19] People are tracked online and in public by technologies like facial recognition and predictive policing, which generate "pre crime" profiles without good cause. Minorities may be unfairly singled out by biased algorithms, which could result in needless investigations and privacy violations.[20] Additionally, without the required consent, AI systems gather and retain vast amounts of personal data, increasing the possibility of abuse and illegal access.[21] Opaque decision making which is acting like “Black Box Decision” makes it impossible for people to question automated processes.[22] Constant surveillance stifles protest and free expression.[23] Growing speech, movement and emotion biometric tracking progressively encroaches on identification and personal life.[24] Thereafter, the issue of responsibility for AI driven actions and robotics are another two major legal issues raised by AI. Currently, existing frameworks do not allow for the legal responsibility of robots, which are composed of hardware, software and algorithms. There is no appropriate legal position for robots, as evidenced by debates about whether they belong in the category of objects, animals, or legal beings. Furthermore there is still uncertainty about the consequences of robots picking up dangerous behaviors, getting compromised, or inflicting harm.[25] These changing issues force academics, legislators and investigators to reconsider legislation and get ready for the social role of AI. Under present legal frameworks, robots that combine hardware, software and algorithms are not now liable. The lack of a suitable legal position is highlighted by debates about whether robots belong in the category of objects, animals, or legal entities. The consequences of robots picking up dangerous habits, getting compromised, or committing harm are also still up for debate. Researchers, legislators and investigators are urged by these changing difficulties to reconsider legislation and get ready for the role of AI in society[26](see table 3).

---

[16] Hadijat Ijaiya, Harnessing AI for Data Privacy: Examining Risks, Opportunities and Strategic Future Directions, 13(2) INT’L J. SCI. & RES. ARCHIVE 2878, 2878–2892 (2024), https://doi.org/10.30574/ijsra.2024.13.2.2510.

[17] Id.

[18] Council on Criminal Justice, DOJ Report on AI in Criminal Justice: Key Takeaways, COUNCIL ON CRIMINAL JUSTICE, Apr. 2025, https://councilоncj.org/doj-report-on-ai-in-criminal-justice-key-takeaways/ .

[19] Mikael Thalen, Privacy in 2026: Will AI Further Supercharge Surveillance?, STRAIGHT ARROW NEWS, Dec. 30, 2025, https://san.com/cc/privacy-in-2026-will-ai-further-supercharge-surveillance/.

[20] Mary T. Costigan, Jason C. Gavejian, Joseph J. Lazzarotti & Damon W. Silver, Top 10 Privacy, AI & Cybersecurity Issues for 2026, JD SUPRA, Jan. 28, 2026, https://www.jdsupra.com/legalnews/top-10-privacy-ai-cybersecurity-issues-7515759/.

[21] Id.

[22] SecurePrivacy.ai, Privacy Laws 2026: Global Updates & Compliance Guide, SECUREPRIVACY.AI, Dec. 11, 2025, https://secureprivacy.ai/blog/privacy-laws-2026 .

[23] Supra Note 17.

[24] Supra Note 18.

[25] Kelly D. Martin & Johanna Zimmermann, *Artificial Intelligence and Its Implications for Data Privacy*, 59 Current Op. Psych. 101829 (2024), https://doi.org/10.1016/j.copsyc.2024.101829.

[26]Pablo Lázaro, *Artificial Intelligence in Criminal Investigation*, A-ID (Aug. 11, 2020).

Table 3: AI breaches on Privacy Rights

AI negative Effect	Affected Privacy Right Area	Explanation
Mass Surveillance Without Oversight	Prevents Government Overreach and Defends Against Surveillance	Permits the use of face recognition technology for warrantless, real time tracking (e.g., U.S. ICE tools), circumventing scrutiny and transforming public areas into panopticons, eliminating restrictions on governmental intrusion.[27]
Bias Amplification in Profiling	Shields Reputations, Supports Democratic Foundations and Protects Individual Autonomy	False "high risk" profiles for minorities are produced by flawed AI, such as COMPAS, which results in intrusive investigations that stigmatize groups, undermine equitable democratic participation and compel individual decisions.[28]
Data Hoarding and Unauthorized Access	Blocks Data Misuse by Groups, Gives Control Over Personal Data and Ensures Accountability for Breaches	Without permission, programs like Clearview AI scrape billions of faces, enabling for unrestricted government and corporate retention and resale, depriving users of their data sovereignty and avoiding breach accountability.[29]
Lack of Transparency (Black Box Decisions)	Ensures Accountability for Breaches, Safeguards Freedom of Expression and Builds Trust in Society	Opaque algorithms (such as EU border AI) cause searches without any discernible reason, making it unable to correct mistakes, stifling free expression because of erratic surveillance and undermining public confidence in data sharing.[30]
Chilling Effect on Free Speech	Safeguards Freedom of Expression, Supports Democratic Foundations and Protects Individual Autonomy	Pegasus and other spyware monitor journalists' private communications, stifling dissent by exposing anxieties and undermining democratically crucial personal liberties and the right to protest.[31]
Biometric Overreach	Shields Reputations and Gives Control Over Personal Data	Unnoticed gait/voice AI collects distinctive characteristics (e.g., CIPA cases), allowing for permanent identification that commodifies private identity data and harms reputations through leaks.[32]
Responsibility for AI Driven Actions	Ensures Accountability for Breaches, Blocks Data Misuse by Groups,	Uncertain responsibility (e.g., who pays for biased AI breaches under GDPR?) allows businesses to avoid penalties, allowing governments and corporations to misuse data without restraint

[27] Supra Note 17, at 9.
[28] Supra Note 18, at 9.
[29] Supra Note 18, at 9.
[30] Supra Note 20, at 9.
[31] Supra Note 17, at 9.
[32] Supra Note 18, at 9.

	Builds Trust in Society, Prevents Government Overreach and Supports Democratic Foundations	and undermining trust because victims have no recourse.[33] Governments circumvent accountability and weaken democratic balances on state authority by implementing unaccountable AI surveillance without taking responsibility for damages (such as predictive policing blunders).[34]
Responsibility for Robotics	Shields Reputations, Protects Individual Autonomy, Gives Control Over Personal Data, Safeguards Freedom of Expression, Defends Against Surveillance and Ensures Accountability for Breaches	Autonomous robots (such as drones used in investigations) gather and process biometrics without obvious owner liability, leaving personal information vulnerable to theft or misuse and damaging reputations on their own.[35] Robotic AI in border/military operations (such as deadly drones) violates privacy without attribution, suppresses expression by fear of unassailable surveillance and avoids accountability.[36]

4. AI Based Real World Investigation Examples

In this section of research there is a mention of examples of AI based Investigations done in Indian Territory and in European Union's territory such as Pegasus spyware, The spam of Vyapam, 26/11 Terror in Mumbai,[37] Operation Cumberland, Operation Encrochat and Operation Trojan Shield.

4.1. Pegasus spyware: Amnesty International and The Washington Post have discovered fresh proof that Pegasus spyware is being used to target Indian journalists. Notable journalists were recently targeted, such as Anand Mangnale (OCCRP) and Siddharth Varadarajan (The Wire). During his inquiry into suspected corporate theft in August 2023, Mangnale's iPhone was targeted via iMessage using a zero click vulnerability, according to confirmation from Amnesty's Security Lab. In October 2023, Varadarajan was again targeted. The same email account under the spyware operator's control was used in both attempts. The Israeli business NSO Group created Pegasus, an extremely intrusive program that can covertly access a device without the user's knowledge. There hasn't been much accountability in India in spite of earlier disclosures. Although the Supreme Court acknowledged the use of spyware in previous cases, it deferred its conclusions, citing the government's lack of cooperation.[38]

---

[33] Ashish Chaturvedi, *Defining Legal Responsibility in the Age of AI: Addressing Gaps in Data Privacy Regulation*, 3 Indian J. Integrated Rsch. L. Iss. II (2023), https://ijirl.com/wp-content/uploads/2023/05/DEFINING-LEGAL-RESPONSIBILITY-IN-THE-AGE-OF-AI-ADDRESSING-GAPS-IN-DATA-PRIVACY-REGULATION.pdf.

[34] Rowena Rodrigues, *Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities*, 4 J. Responsible Tech. 100005 (2020), https://doi.org/10.1016/j.jrt.2020.100005.

[35] Shreyansh Upadhyay, *Navigating Liability in Autonomous Robots: Legal and Ethical Challenges in Manufacturing and Military Applications*, Yale Rev. Int'l Stud. (Mar. 6, 2025), https://yris.yira.org/column/navigating-liability-in-autonomous-robots-legal-and-ethical-challenges-in-manufacturing-and-military-applications/.

[36] Erica Stanford, *Autonomous AI: Who Is Responsible When AI Acts Autonomously and Things Go Wrong?*, Global Legal Insights: AI, Mach. Learning & Big Data Laws & Reguls. 2025 (May 15, 2025), https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/autonomous-ai-who-is-responsible-when-ai-acts-autonomously-and-things-go-wrong/.

[37] *What Was Vyapam Scam? 10 Must Know Facts*, Zee News (June 11, 2023, 6:47 PM IST), https://zeenews.india.com/india/what-was-vyapam-scam-10-must-know-facts-2620421.html .

[38] Amnesty International, India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists, AMNESTY INTERNATIONAL (2023),

This occurs in the midst of larger crackdowns on privacy and freedom of expression in India, which include harassment, arrests and surveillance of activists and journalists. Amnesty advocates for a ban on spyware but NSO Group insists that its software is only sold to approved counterterrorism organizations. They call on the Indian government to carry out an impartial, open inquiry into these instances and make the Supreme Court's conclusions public.[39]

4.2. The spam of Vyapam: The Madhya Pradesh Professional Examination Board (MPPEB) scam, also known as the Vyapam scam, was a widespread corruption scandal that negatively impacted the standing of the BJP led administration led by Chief Minister Shivraj Singh Chouhan. Vyapam, abbreviation for Vyavsayik Pariksha Mandal, is the MPPEB, which administers recruitment tests for government positions and entrance exams for professional degrees. Investigations showed that the scam had been going on for years and had impacted other tests and recruitments but it only came to light in 2013 when anomalies were discovered in the Pre Medical Test (PMT). Exam results were manipulated, impersonation was used and admissions and employment were obtained by fraud by a network of intermediaries, candidates and authorities. Politicians, government employees and school administrators were arrested as a result. Exams for government, engineering and medical jobs were affected by the scam, which involved thousands of applicants. Due to the strange deaths of multiple defendants, witnesses and whistleblowers, the case gained notoriety and sparked debates. The scam, which was looked into by organizations like the CBI and STF, resulted in acquittals, convictions and important changes to the examination procedure. The scandal caused long lasting harm to Madhya Pradesh's recruitment and education institutions, notwithstanding attempts to rebuild trust.[40]

4.3. 26/11 Terror in Mumbai: Concern over cyberterrorism is on the rise in India, where events are frequently connected to organizations like the Indian Mujahideen. These attacks use cyber communication to target authorities, disseminate terror messages and claim responsibility for attacks. Modern terrorists do not rely primarily on conventional weaponry but also use advanced technology like computers, laptops and tablets. Cyberterrorism presents two major problems. First, the general populace is ignorant of basic computer skills and cyberthreats. Second, cyber attacks are harder to trace, making them more hazardous and effective. The 26/11 Mumbai attacks revealed how cyber technologies were used to coordinate and execute the operation. The attackers relied on social media and cellular networks to track and thwart Indian government attempts and they used Google Earth to plan their attacks. Advanced methods were used to convey commands, making it challenging for Indian soldiers to intercept them. There are three categories of cyberterrorism that occurred during the 26/11 attacks. Physical attacks damaged infrastructure through bombings and gunfire, knocking off internet and communication networks. In order to compromise intelligence, synthetic attacks included hacking, infecting computers with viruses and breaking into security systems. Semantic attacks monitored live web feeds to impede security responses and took advantage of systems to cause problems. These instances pushed the Indian government to tighten digital security measures.[41]

4.4. Operation Cumberland: 25 individuals involved in child sexual exploitation were apprehended in February 2025 as a result of a multinational operation known as "Operation Cumberland."[42] With assistance from Europol, 19 nations carried out the operation. This case is significant because it dealt with AI generated child sexual abuse material (CSAM), which uses artificially manufactured images rather than actual child photos. Such content encourages the sexualization and objectification of minors and causes significant social harm, even if it does not

---

https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/.

[39] Id.

[40] Supra 35, at11.

[41] Abhijit Chanda & Muskaan Verma, *Critical Evedenciarcy Analysis of 26/11 Attacks with Reference to Cyber-Terrorism*, 6(S2) International Journal of Health Sciences 10011 (2022), https://doi.org/10.53730/ijhs.v6nS2.7663.

[42] Europol, '25 Arrested in Global Hit against AI-Generated Child Sexual Abuse Material' (28 February 2025) https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

depict actual victims. Additionally, it makes it challenging for law enforcement to properly identify victims and conduct criminal investigations. Currently, many nations lack the necessary legislation to handle AI generated CSAM. In order to better safeguard children from exploitation and abuse, the European Commission has suggested new legislation that EU member states are debating.[43]

4.5. Operation Encrochat of 2020: A significant multinational law enforcement investigation known as "Operation EncroChat" (2020) targeted organized crime gangs that made use of the encrypted communication software EncroChat. With assistance from Europol and Eurojust, French and Dutch officials oversaw the inquiry. Investigators were able to intercept and analyze millions of messages sent by criminals in real time by successfully breaking into EncroChat's encrypted network. Plans for drug trafficking, money laundering, violent attacks, corruption and attempted murders were disclosed in these emails. Numerous European nations saw hundreds of arrests as a result of the operation and substantial amounts of cash, luxury goods, guns and drugs were seized. Additionally, it revealed how heavily encrypted technologies were used by organized crime networks to evade discovery. The operation turned into a historic illustration of global collaboration and the application of cutting edge investigative methods against transnational organized crime.[44]

4.6. Operation Trojan Shield: In order to combat international organized crime, the Federal Bureau of Investigation initiated "Operation Trojan Shield," an inventive covert operation, with assistance from the Australian Federal Police.[45] The agencies sent more than 12,000 modified smartphones to criminal organizations worldwide and covertly developed and ran their own encrypted communication infrastructure. Criminals used these devices to share private information concerning illicit operations, such as drug trafficking and violent crimes, since they thought the platform was safe. Law enforcement organizations from several nations, including as Europol and the Drug Enforcement Administration, obtained important information through this operation, which resulted in hundreds of arrests throughout Europe and Australia. Using encrypted communication technology, the operation also assisted authorities in breaking up criminal networks and preventing grave risks to human life.[46]

5. Laws Governing Technological And AI Driven Investigations To Protect Privacy Rights:

Privacy rights are important, as they stop unwarranted government monitoring, shield private information from being misused by businesses and hold wrongdoers accountable. They guarantee people have ownership over their data, foster trust by protecting sensitive information and support the maintenance of boundaries in relationships and the workplace. Freedom of expression and political engagement also depend on privacy since it enables people to think, speak and vote without fear. It protects financial information from abuse, including identity theft and preserves reputations by empowering users to delete damaging content. Upholding privacy rights is essential to preserving individual liberty, security and trust in the digital age as technology develops.[47]

---

[43] Cornelia Riehle LL.M., *Hit against AI-generated child sexual abuse material.* eucrim. (2025, March 24). https://eucrim.eu/news/hit-against-ai-generated-child-sexual-abuse-material/

[44] Europol and Eurojust, 'Dismantling of an Encrypted Network Sends Shockwaves through Organised Crime Groups across Europe' (2 July 2020) https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

[45] Nicholas Davis, 'The FBI's Operation Trojan Shield: Infiltrating Criminal Groups through their Phones' (American University, 27 August 2021) https://www.american.edu/sis/centers/security-technology/operation-trojan-shield.cfm

[46] Federal Bureau of Investigation, 'FBI and Global Partners Announce Results of Operation Trojan Shield' (8 June 2021) https://www.fbi.gov/news/stories/fbi-global-partners-announce-results-of-operation-trojan-shield-060821 accessed 16 May 2026.

[47] Supra Note 8, at 7.

5.1. Indian Constitution:

Article 21 of the Constitution guarantees the right to privacy and the legislation guarantees that people have control over their personal data. But for reasons like national security, this freedom may be curtailed, necessitating a careful balancing act between state interests and privacy rights.

Moreover as per Article 21 of the Constitution, the right to privacy is an essential component of the right to life and personal liberty in India, as stated in the Supreme Court's historic Puttaswamy v. Union of India (2017) ruling.[48]

People can live without worrying about discrimination or arbitrary surveillance thanks to the right to privacy, which guarantees them control over their personal information. It is necessary to uphold human dignity, permit freedom of speech and facilitate social engagement. Without privacy, people would find it difficult to express themselves freely, make independent decisions, or preserve safe interpersonal interactions. The right to privacy is even more important as technology develops and data becomes more susceptible to abuse. Protecting this right is essential to preserving individual freedom, autonomy and dignity in the face of digital data gathering and monitoring technology. This ensures a democratic society in which individual liberties are upheld.[49]

5.2. DPDP:

The Digital Personal Data Protection Act i.e. DPDP act, 2023 (Ministry of Law and Justice, 2023), governs how personal data is processed in India, including information gathered offline and online that is subsequently converted to digital form and information processed outside of India in order to provide services in India.[50] Information that can be used to identify a person is referred to as personal data and processing include tasks including gathering, storing and disseminating it. According to the Act, personal data can only be processed with a person's consent after they have been given explicit notice. In certain situations, such as government services, medical emergency, or employment, consent is not necessary.[51] Parents or guardians must give their consent for minors. The rights of individuals (data principals) include the ability to view, amend, or remove data as well as designate a representative to oversee these rights. Data fiduciaries, or organizations that handle data, are responsible for making sure that data is accurate, secure and erased on time. The law exempts some operations, such as state security and permits data transfers overseas, with the exception of banned nations. With fines of up to ₹250 crore for violations, the Data Protection Board manages complaints, enforces penalties and monitors compliance.[52]

5.3. GDPR:

The General Data Protection Regulation (GDPR) is the European statutory act which focuses on the right to privacy of an individual.[53] Due to AI systems' ability to re identify, link and act upon sensitive data, personal information is susceptible to abuse. Large language models and generative AI systems that need enormous datasets should be especially concerned about this. The conflict between privacy protection and technological advancement emphasizes the significance of strong data protection regulations, as the planned Artificial Intelligence Act. The EU acknowledged the need for improved security as technology developed and the internet

---

[48] Supra Note 11, at 7.

[49] Id.

[50] Arokia Sushma, Ranjit Oommen Abraham & R. Haritha Devi, Artificial Intelligence and Data Privacy Challenges: A Legal Perspective, 5(5) INDIAN J. INTEGRATED RES. L. 221, 221–235 (2025), https://ijirl.com/wp-content/uploads/2025/09/ARTIFICIAL-INTELLIGENCE-AND-DATA-PRIVACY-CHALLENGES-A-LEGAL-PERSPECTIVE.pdf.

[51] Id.

[52] *The Digital Personal Data Protection Bill, 2023*, PRS Legislative Research, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (last visited May 9, 2026).

[53] General Data Protection Regulation (GDPR) – Legal Text, GDPR Info, https://gdpr-info.eu/ (last visited May 9, 2026).

became an essential component of daily life. In order to set fundamental guidelines for data security and privacy, the European Data Protection Directive was adopted in 1995. On the basis of this directive, member states subsequently enacted legislation. But as technology advanced quickly and more people turned to the internet for purposes like social networking, online banking and advertising, it became evident that more stringent regulations were required.[54]

The European Parliament responded by passing the General Data Protection Regulation (GDPR) in 2016, which went into effect on May 25, 2018. By introducing thorough data protection measures, this regulation made sure businesses all over the world handle the data of EU citizens in accordance with stringent privacy requirements. The EU's commitment to modifying privacy regulations to address contemporary technology concerns while upholding individuals' rights is reflected in the GDPR.[55]

Table 4: Difference between GDPR and DPDP

Aspect	**GDPR**	**DPDP**
Full form	General Data Protection Regulation	Digital Personal Data Protection
Enacted	May 24, 2016	August 11, 2023
Enforcement	May 25, 2018	Probably from May 2027
Nature of Regulation	Data protection and Privacy Law	Data Protection and Digital Privacy Law
Primary Focus	Protection of Personal Data and Privacy of Individuals.	Protection of Digital Personal Data of Individuals in India.
Region or Jurisdiction	As per Article 3 of Chapter 1, to the European Union (EU) and to the organisation which are accessing data of Residents of EU.	As per Section 3 of Chapter 1, to the Indian Territory and to the organisations (offering goods and services) which are accessing data of Residents of India.
Objectives	Ensure Lawful, Fair and Transparent processing of personal data and Give control to Individuals which is precisely described in Chapter 3.	Protect Personal Data, ensure accountability and Lawful Processing
Legal Basis for processing	As per Chapter 2 and precisely according to Article 6 Legal basis for processing can be Consent, Legal Obligation, Vital Interests, Public Interest tasks or	As per Section 6 and Section 7 Consent and Legitimate Uses respectively are the main Legal basis for processing

[54] Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?*, GDPR.eu, https://gdpr.eu/what-is-gdpr/ (last visited May 9, 2026).
[55] Id.

	Legitimate Interest	
Rights of Individual	As per Chapter 3, Right to be Informed (Article 13 & 14), Access (Article 15), Rectification (Article 16), Erasure/Forgotten (Article 17), Restriction of processing (Article 18), Object (Article 21), Automated Decision Making (Article 22)	As per Chapter 3 From section 11 to 14: Right to access, Correction, Completion, Updating, Erasure, Grievance redressal, Nominate and as per Chapter 2's section 6 Consent Withdrawal are the Rights of Individual
Duty of Entities	As per Chapter 3 Rectification (Article 16), Request Deletion of data in case of erasure/Forgotten (Article 17), Limit how their data is used (Article 18), Data Portability (Article 20), Legitimate Interest (Article 21) and As per Chapter 8, File a complaint in case wrong happens (Article 77).	As per Chapter 3 Section 15; Comply with all applicable laws, Refrain From Impersonation, Avoid the suppression of material information (particularly with state), Not to File False or Frivolous complaints and Provide authentic information for Data Correction or Erasure request
Supervisor Authority	Data Protection Authorities in each EU member state; Coordinated by European Data Protection Board which is explained under Article 68	As per Chapter 5, Data Protection Board of India is the Supervisor Authority
Penalties for non compliance	As per Article 83 and 84 Administrative Fines (Lower Tier fines include €10 million or 2% of total worldwide annual turnover & Upper Tier Fines include €20 million or 40% of total worldwide annual turnover) and Criminal Sanctions	As per the Schedule penalties ranges from Rs. 10,000 for individual Violations to Rs. 250 Crore for massive Data Breach Negligence
Cross Border Data Transfers	As per Article 46, Allowed only to Countries with Adequate Protection or with Safeguards	Permitted with certain government approved conditions (section 16)
Exemptions to Objectives	National Security, Defense, Journalism, etc.	National Security, Research or Approved Government Functions.

6. Relevant Case Laws:

6.1. India:

The Supreme Court of India investigated whether surveillance practices that involved nighttime domiciliary visits were in violation of Article 21 of the Indian Constitution which protects the right to life and personal liberty in the case of Kharak Singh v. State of Uttar Pradesh and Ors (*Kharak Singh v. State of Uttar Pradesh & Others*,

1962).[56] The Court decided that this kind of surveillance did, in fact, violate Article 21. It is challenging to acknowledge privacy as a fundamental right under the Constitution, nevertheless, as the majority of judges ruled that Article 21 does not specifically mention the right to privacy. They claimed that simply keeping an eye on someone's whereabouts does not violate any of the fundamental rights protected by Part III of the Constitution. On the other hand, Justice Subba Rao's minority opinion highlighted that, in accordance with Article 21, privacy is an essential component of individual liberty. He maintained that liberty encompasses freedom from environmental and psychological interference in addition to freedom from physical limitation. Justice Subba Rao emphasized the importance of privacy for one's security, tranquility and sense of self, especially in the house, which acts as a haven from outside interference. He claimed that although privacy is not specifically listed as a fundamental right in the Constitution, it is an essential part of individual liberty. He claims that surveillance practices such as the ones used in this instance violate people's right to privacy and personal freedom.[57]

And In the another recent case of Vineet Kumar,[58] In accordance with Section 5(2) of the Indian Telegraph Act, 1885, the Indian Ministry of Home Affairs issued three orders between October 2009 and February 2010 to intercept businessman Vinit Kumar's phone conversations. This clause permits communication interception for public safety or in times of emergency as long as it protects public order, security, sovereignty, or deters criminal activity. The CBI utilized intercepted calls as evidence in its investigation into Kumar's alleged bribery of a public officer. In the Bombay High Court, Kumar contested the orders, claiming they were issued improperly and infringed upon his right to privacy guaranteed by Article 21 of the Constitution. The Court reaffirmed that privacy is a basic right under Article 21 and that interception must pass the proportionality and legitimacy test, citing court decisions such as PUCL v. Union of India and Puttaswamy v. Union of India. The Court determined that the orders were illegal and did not comply with the proper procedures since it could not find any evidence of a public safety danger to support the interceptions. It emphasized that unlawfully obtained evidence cannot be utilized in criminal proceedings and ordered the disposal of the intercepted data. The Court upheld the value of constitutional rights over procedural infractions, rejecting the claim that ends justify methods.[59]

The FMP requested explicit standards for law enforcement's search and seizure of digital devices in the Supreme Court case Foundation for Media Professionals (FMP) v. Union of India & Ors., which was filed as Writ Petition in October 2022.[60] The FMP maintained that the lack of such rules violates people's right to privacy and protection from self incrimination by enabling authorities to intervene without reasonable suspicion. They underlined that digital devices are an extension of a person's identity and include sensitive personal data. The Supreme Court voiced worries about the arbitrary seizure of media professionals' gadgets in November 2023 and instructed the Union government to think about creating restrictions for these searches. The Court emphasized the necessity of finding a compromise between upholding the rights of media professionals and attending to the demands of law enforcement.[61]

6.2. European Union

The Court of Justice of the European Union defined the extent of compensation for privacy infringement under the GDPR in the In Österreichische Post Case.[62] In the case, the Austrian postal service inferred citizens' political affiliations without their knowledge by employing computational technologies and sociodemographic profiling.

---

[56] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India), https://indiankanoon.org/doc/682321/.

[57] Rahul Kumar, *Jurisprudence of Right to Privacy in India* (July 30, 2020), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3664257.

[58] AIRONLINE 2019 BOM 1117, 2020 (1) ABR(CRI)

[59] *Kumar v. Central Bureau of Investigation*, Writ Petition (Criminal) No. 2367 of 2019 (Bom. H.C. Oct. 22, 2019), https://globalfreedomofexpression.columbia.edu/cases/kumar-v-central-bureau-of-investigation/.

[60] Writ Petition (Criminal) No. 395 of 2022.

[61] *Foundation for Media Professionals v. Union of India*, Writ Petition (Criminal) No. 395 of 2022 (India), Petition filed before the Supreme Court of India, https://www.scobserver.in/wp-content/uploads/2023/11/Petition-filed-by-Foundation-for-Media-Professionals.pdf.

[62] Supra Note 8, Page 3

The Court ruled that a person is not always entitled to compensation for a simple violation of the GDPR. A GDPR violation, actual material or non material harm, and a causal link between the breach and the damages incurred are instead necessary. Significantly, the Court upheld people's right to privacy in the digital sphere by rejecting any need that emotional or psychological harm meet a minimal seriousness threshold. The Court upheld the rights to informational privacy and transparency under Article 15 GDPR in the CRIF Case. In order to properly exercise their data protection rights, it was decided that people have the right to acquire copies of extracts, emails, or database records containing their personal data. The ruling emphasized the obligation of technology driven data controllers to balance trade secrets and third party rights while offering clear and accurate access to personal data.[63]

Moreover in another case, The Court of Appeal investigated the legitimacy of South Wales Police's use of Automated Facial Recognition (AFR) technology in public areas in Bridges v. South Wales Police.[64] The lawsuit started when Edward Bridges, a human rights activist, contested the police's use of live facial recognition technology in Cardiff. Without the public's agreement, the AFR system collected thousands of people's face biometric data and compared it with police watchlists. Because biometric face data is extremely sensitive personal information, the Court acknowledged that facial recognition technology violates the right to privacy under Article 8 of the ECHR. The Court discovered "fundamental deficiencies" in the legal framework governing the technology's usage, despite the fact that it served justifiable purposes like crime prevention. Specifically, there were inadequate controls over who might be added to watchlists and where the technology could be used. AI driven surveillance systems must adhere to the standards of legality, proportionality, justice, and data protection, according to the ruling. Concerns regarding algorithmic bias and possible prejudice were also brought to light, highlighting the necessity of more stringent regulation of new policing technology.[65]

7. Conclusion

The right to privacy is still fundamental to personal autonomy, independence and dignity, as well as defense against needless government intervention. Rapid advancements in technology, especially artificial intelligence, present both privacy opportunities and difficulties. Because AI can handle enormous volumes of personal data, there are serious worries about data security and monitoring, which calls for more laws to protect people's rights. With many unresolved issues about accountability and culpability, the legal responsibility of AI driven acts is still developing, particularly in the context of robotics and data exploitation. Biometric systems and other AI technologies provide advantages but they also carry risks that could violate people's privacy. Strong privacy rules and regulations are essential to addressing these problems and preventing the erosion of fundamental rights by technology advancements. Privacy protection must continue to be a top concern in legal and policy conversations as AI and other technologies continue to influence our society.

As AI technology advances, India must figure out how to regulate it while maintaining fundamental liberties. Despite being recognized as a fundamental right, privacy still faces challenges in areas such as monitoring, digital awareness and balancing it with other rights. The proliferation of digital platforms and government monitoring programs often pose a danger to privacy.[66] Unlike the EU, India does not have a comprehensive AI law; nonetheless, recommendations have been issued by the Ministry of Electronics and Information Technology.[67] Important legislation like the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023 regulate AI and data privacy. Concerns are raised by potential biases in AI since they could violate the

[63] CMS. (2023, June 1). *CJEU provides clarity on data protection: Judgments on right to compensation and right to obtain a copy of personal data*. CMS Law. https://cms.law/en/bel/legal-updates/cjeu-provides-clarity-on-data-protection-judgments-on-right-to-compensation-and-right-to-obtain-a-copy-of-personal-data

[64] Supra Note 9, Page 3

[65] JULIA Project. *Case law 270*. JULIA Project Database. Retrieved May 16, 2026, from https://www.julia-project.eu/database/case-law/270

[66] Supra Note 11, at 7.

[67] Ministry of Electronics & Information Technology, Government of India, *The Digital Personal Data Protection Act, 2023*, https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf .

right to equality. The evolving legal system needs to reconcile morality, innovation and respect for fundamental rights including privacy and equality.[68]

The Indian Constitution and other international legal frameworks both uphold the fundamental right to privacy, which is a component of personal liberty and autonomy. The General Data Protection Regulation (GDPR) and the Digital Personal Data Protection Act, 2023, both demonstrate the increasing acknowledgement of privacy as a fundamental human right, particularly in the digital era.[69] These regulations seek to safeguard people's private information and provide them authority over its usage. As seen by significant rulings like Vineet Kumar and Kharak Singh, where the courts affirmed privacy as a component of individual liberty, the Indian judiciary has been essential in defining the right to privacy. It is still difficult to strike a balance between state concerns like national security and privacy. Comprehensive legal frameworks and strict enforcement of privacy rights are becoming more important as technology advances in order to preserve individual dignity and guard against abuses of power.

It is still very difficult for nations all around the world to strike a balance between data privacy, national security and other rights. To ensure that privacy protections are thorough and efficient in the digital era, privacy laws must change to keep up with technological changes. A more secure and equitable digital environment can be achieved through international collaboration and learning from the experiences of other nations.[70]

8. Suggestions

I. Analyze how police use facial recognition technology, violates the privacy guarantees by many legislations collecting large amounts of biometric information without a warrant, as interpreted by Justice K.S. Puttaswamy (2017), incorporate adoption rate data from the NCRB to measure excessiveness and suggest proportionality standards for judicial review.

II. Examine algorithms that overtarget marginalized groups based on skewed crime statistics which used to undermine the rights. Cite empirical studies and Delhi Police pilots that demonstrate 20 to 30% error discrepancies to support the need for mandated bias audits under the CrPC evidentiary requirements.

III. Talk on how unintelligible algorithms violate disclosure standards by obfuscating the logic of the evidence, provide human readable explanations using XAI (Explainable Artificial Intelligence) approaches, backed by case studies of disputed AI outputs in courts.

IV. Examine how AI combines social media and telecom data into dossiers without permission, violating the minimization criteria of DPDP 2023; suggest fiduciary responsibilities for investigators, equating them with RBI data localization guidelines for better protections.

V. Investigate everlasting AI databases that suppress freedom of speech following an examination; cite UIDAI violations to recommend automated deletion procedures after six months, in line with international best practices such as the EU ePrivacy Directive.

VI. Examine false positives that result in unwarranted intrusions, use reports such as MeitY to demand accuracy thresholds above 99% prior to deployment, along with victim redress procedures under consumer protection legislation.

VII. Examine how private companies like Clearview are circumventing procurement openness by scraping photos for law enforcement; suggest public tender requirements that include privacy effect analyses and reference CAG audits to ensure accountability.

---

[68] Varun Pathak, Yash Karunakaran & Vishwajeet Deshmukh, *Balancing AI, Ethics and the Constitution*, Law.asia (Dec. 9, 2024), Law.asia .

[69] Supra Note 45, at 14.

[70] Supra Note 4, at 2.

VIII. Examine how mass AI data grabs undermine anonymity under UDHR Article 12 and ICCPR Article 17; use UN HRC reports as cross jurisdictional evidence to compare EU GDPR €20M fines and propose universal suspicion levels.

IX. Both privacy and AI or technological research are equally vital but it is also inappropriate to use them excessively to violate people's rights. Not even the majority of people know about it. Information should be provided to the person whose information will be reviewed and the investigation departments should have internal procedures.

X. Campaigns to raise awareness of people's right to privacy, how it can be infringed and the legal protections offered in the event that someone's right is abused in the process of investigation are necessary.

XI. If an individual's right to privacy is protected or the investigating officers are abiding by the regulations to preserve the harmony between the inquiry and the right to privacy, there should be appropriate judicial oversight.

XII. Advanced innovation is required, with an emphasis on individual privacy as well. There should be a rule that notifies the police before attempting to violate someone's right to privacy, just as there is a check that the person managing the website is not a robot.