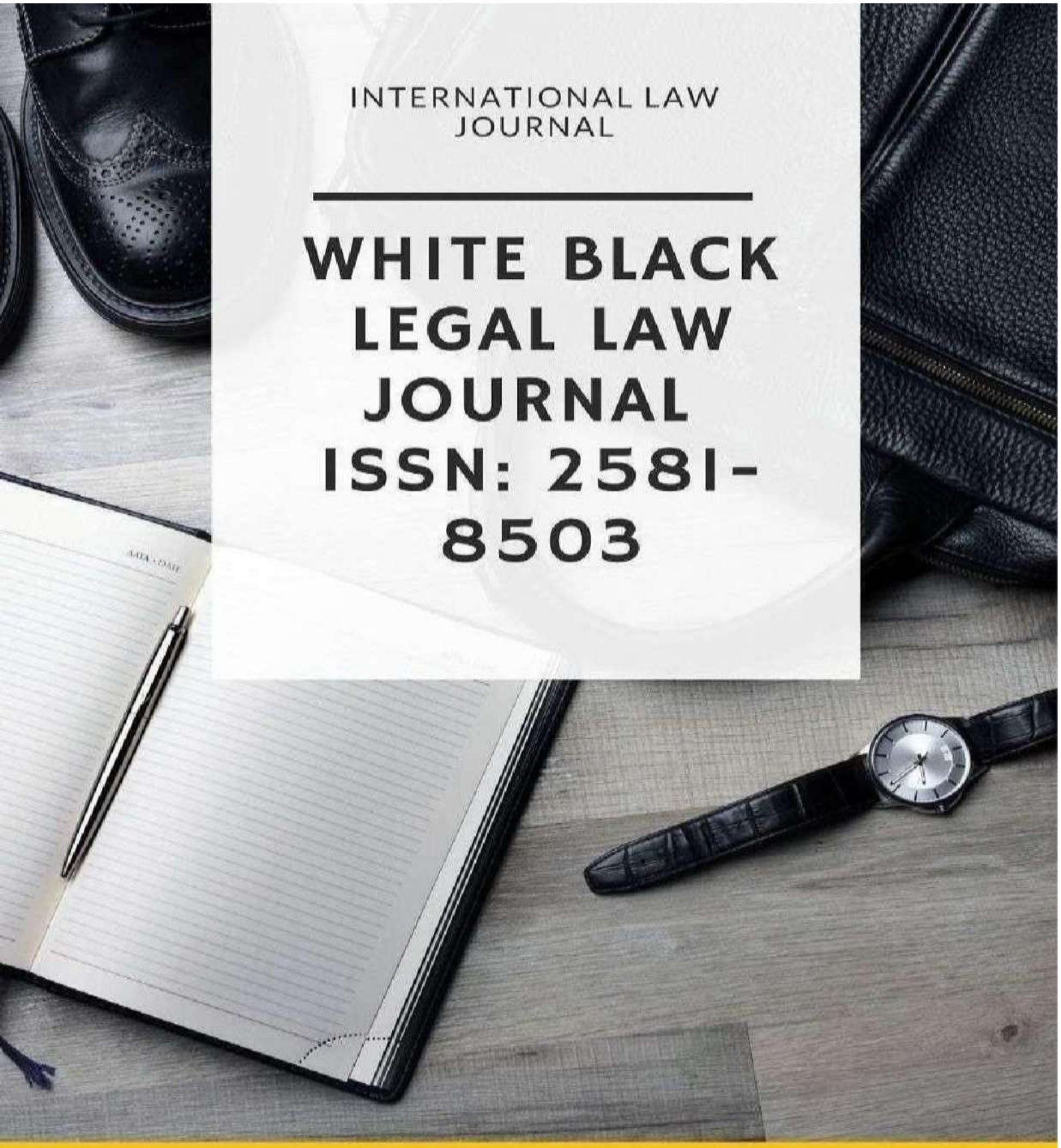

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 2 | Oct 2025 ISSN: 2581-8503

"WHEN SECURITY SEES YOUR FACE: THE PRIVACY DILEMMA OF AI SURVEILLANCE"

AUTHORED BY - MR. JAKEY KHAN,
Research Scholar, University School of Law and Research (USLR), University of Science and Technology Meghalaya (USTM).

Abstract:

In 2023, India recorded over 1,300 CCTV cameras per square mile in New Delhi, making it the most surveilled city in the world, overtaking Beijing and London. At the same time, the global facial recognition market is projected to grow to USD 16.74 billion by 2030, driven by governments and corporations seeking enhanced security, efficiency, and predictive policing tools. Against this backdrop, the rapid deployment of Facial Recognition Technologies (FRTs) in India presents a double-edged sword: promising stronger security while triggering deep concerns of privacy erosion, algorithmic bias, and unchecked state surveillance. While countries like those in the European Union have introduced rigorous safeguards through the General Data Protection Regulation (GDPR) and the proposed EU AI Act, India's Digital Personal Data Protection Act, 2023 remains inadequate. It neither defines biometric data nor imposes specific restrictions on FRT and critically allows state agencies sweeping exemptions, leaving citizens vulnerable to misuse of their most personal data: their faces. This paper critically interrogates the ethical and legal challenges of FRT in India through a doctrinal and case study method. It analyses the constitutional evolution of the right to privacy from M.P. Sharma (1954) to Puttaswamy (2018), the loopholes in India's new data protection regime, and recent deepfake controversies such as the Rashmika Mandanna incident that underscore the inadequacy of existing safeguards. By juxtaposing potential benefits like crime detection, border security, anti-terrorism, with risks such as false arrests, discrimination against minorities, and chilling effects on free expression, the study highlights the precarious balance between security and liberty. Ultimately, the research argues that while FRT may strengthen public safety, its unregulated use risks creating a digital panopticon where individuals are perpetually monitored, judged, and controlled. To prevent such a dystopia, India must urgently develop a rights-based regulatory framework rooted in privacy by design, transparency, accountability, and judicial oversight. This paper contributes to the global discourse by offering

legal and ethical recommendations to reconcile technological advancement with the enduring principles of human dignity and constitutional freedom.

Keywords: Facial Recognition Technology, Surveillance, Privacy, Security, AI Ethics, Data Protection, Human Rights.

Introduction:

The Prime Minister of India Narendra Modi tweeted on 24th of June 2023 stating, "AI is the future, be it Artificial Intelligence or America-India! Our nations are stronger together, our planet is better when we work in collaboration."[1] The goal of the current administration is to keep India competitive in the current AI race, as seen by this tweet and other government measures recently involving the adoption and application of Artificial Intelligence (AI) in many industries. In this digital age, the rapid advancement of artificial intelligence (AI) has ushered in a new era of surveillance systems where facial recognition technology plays a pivotal role. The deployment of AI-powered surveillance systems, equipped with facial recognition capabilities, has significantly transformed the landscape of security and public safety. However, this emergence has also given rise to critical ethical implications that demand careful examination and consideration.

Facial recognition technology enables automated identification and verification of individuals based on their unique facial features, allowing for real-time tracking, monitoring, and profiling. While proponents argue that these systems enhance security measures and aid in crime prevention, ethical concerns have been raised regarding the potential invasion of privacy, misuse of personal data, discrimination, bias, mass surveillance and potential breach of fundamental rights, embedded within the algorithms. In light of ethical dilemmas, it is crucial to critically examine the legal and regulatory frameworks governing the use of facial recognition technology in surveillance systems. The effectiveness and adequacy of current laws in India safeguarding individual rights and mitigating potential abuses need to be evaluated. Additionally, the impact of government surveillance on citizen rights and the need for international perspectives in addressing these ethical implications deserve careful consideration. Beyond legal considerations, the societal implications of AI-powered

[1] Narendra Modi [@narendramodi], "AI is the future, be it Artificial Intelligence or America-India! Our nations are stronger together, our planet is better when we work in collaboration. https://t.co/wTEPJ5mcbo" *Twitter, 2023 available at:* https://twitter.com/narendramodi/status/1672333386319290368 (last visited July 15, 2023).

surveillance systems with facial recognition technology must be examined. The constant monitoring and surveillance can affect social behaviour, erode trust between individuals and institutions, and potentially alter the fabric of society. Furthermore, the psychological effects of living under constant surveillance and the potential ramifications for marginalized communities and vulnerable populations require thoughtful analysis. Evaluating the advantages and risks of facial recognition technology is essential while navigating the ethical minefield of AI in surveillance systems. Despite the potential for improved security measures offered by these systems, it is crucial to critically assess their shortcomings, the trade-offs between security and privacy, and the possibility of unexpected effects.

This research paper contributes to the ongoing discourse surrounding the ethical implications of AI in surveillance systems by focusing on the specific context of facial recognition technology. By critically analyzing the multifaceted ethical challenges, legal considerations, societal implications, and the balance between security and privacy, this study aims to provide insights and recommendations for policymakers, legislators, and stakeholders. Ultimately, the goal is to foster responsible and ethical use of facial recognition technology in surveillance systems, ensuring the preservation of individual rights and societal values in our increasingly interconnected world.

Research Objectives and Methodology:

The primary objective of this research paper is to critically analyze the ethical implications of artificial intelligence (AI) in surveillance systems, specifically focusing on the use of facial recognition technologies (FRTs). By exploring the delicate balance between security and privacy in the digital age, this study aims to shed light on the multifaceted ethical challenges that arise when utilizing facial recognition technology in surveillance systems. The research methodology adopted by the researcher is doctrinal and the researcher has adopted a case study research method to substantiate his research.

Artificial Intelligence (AI):

John McCarthy also known as the "father of artificial intelligence" offers the following definition of artificial intelligence in his research paper titled “What is Artificial Intelligence”. He stated that "It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically

observable."[2] In simple words, artificial intelligence may be understood as a branch of computer science that can simulate or replicate human intelligence. It is an algorithm that has the capability of learning, planning, reasoning etc. i.e., it can simulate tasks or jobs that require human intelligence. Research and Development in developing AI have been going on since the 1950's and social media was the first contact of humanity with artificial intelligence (AI). But people started noticing or had a first-hand experience of artificial intelligence (AI) when OpenAI released ChatGPT 3.5 which is a form of AI known as a Large Language Model or LLM.

Considering how overused the word AI is today, businesses frequently use it to promote their products, whether or not the products actually exhibit AI-like traits. However, intelligence should not be misunderstood as automata or automatic. The former has the capability of being autonomous while the latter cannot be autonomous without human intervention. This is the reason that people should be concerned. Today a human being taking a decision for another human being can be held accountable for their decision or they can explain as to how they have arrived at the decision. Whereas with the advent of artificial intelligence (AI) corporations and even the government have started employing AI which is going to make decisions for human beings and such decisions will directly affect their lives with no accountability, transparency or liability attached. Moreover, eighty-five million jobs would be lost due to automation and a new division of labour between humans and machines by 2025 in medium-sized and big firms spanning fifteen industries and twenty-six economies. As automation and digitization in the workplace rise, positions in areas like data entry, accounting, and administrative assistance are becoming less in demand. Ninety-seven million new employment will be created by the robot revolution, but the places most at risk of disruption will require assistance from businesses and governments.[3]

Facial Recognition Technology (FRT):

The Facial Recognition Technology (FRT) or facial recognition system is a computer programme that uses a digital image or a video frame from a video source to automatically recognise or confirm a person. Comparing specific face traits from the image and a facial

[2] John McCarthy, 'What is Artificial Intelligence?' (2007)
[3] "Recession and Automation Changes Our Future of Work, But There are Jobs Coming, Report Says," *World Economic Forum available at:* https://www.weforum.org/press/2020/10/recession-and-automation-changes-our-future-of-work-but-there-are-jobs-coming-report-says-52c5162fce/ (last visited July 16, 2023).

database is one approach to achieve this. It can be comparable to other biometrics like fingerprint or eye iris recognition systems and is frequently utilised in security systems. One of the numerous companies creating facial recognition technology is Identix®, which has its headquarters in Minnesota. Its software, FaceIt®, has the ability to recognise a face in a crowd, separate the person from the background, and compare it to a database of previously captured photographs. This software must be able to distinguish between a simple face and the surrounding background in order to function. The foundation of facial recognition software is the capability to identify a face and then quantify its numerous aspects.[4]

Position of the Right to Privacy in India:

We are all monitored from the moment of our birth till the moment of our death and even after. Even a seemingly innocuous Tweet or Facebook "Like" can reveal sensitive information, such as where someone's location and occupation. The most important issue of our day is now privacy, but it is still routinely infringed. The right to privacy is the highest human right and is naturally endowed by nature, but its standing as a fundamental right under the Constitution is still under question.

It is noteworthy to point out that the right to privacy was not specifically intended by the framers of the Constitution because it is not mentioned even once throughout the entire constituent assembly deliberations. As a result, it is the judiciary in our country that has thought about the issue and has defined privacy from the start. In just four years after the Constitution came into being, the Supreme Court had to deal with the question of privacy which signifies the vitality and relevancy of the right to privacy.[5]

In the case of M.P. Sharma and Ors. vs. Satish Chandra and Ors. (1954)[6], the Supreme Court by a majority decision of an eight-judge Constitution bench held that the right to privacy was not a fundamental right under the Indian Constitution and also held that search and seizure is a must for the protection of social security and also stated that search and seizure process is temporary interference for which statutory recognition was unnecessary. In Kharak Singh vs.

[4] S. B. Thorat, S. K. Nayak and Jyoti P. Dandale, "Facial Recognition Technology: An analysis with scope in India" (arXiv, 2010).
[5] "A short history of right to privacy," *Governance Now, 2016 available at:* https://www.governancenow.com/gov-next/egov/a-short-history-right-privacy (last visited July 18, 2023).
[6] M.P. Sharma and Ors. vs. Satish Chandra and Ors., AIR 1954 SC 300

The State of U.P. and Ors. (1962)[7] a minority opinion recognized the right to privacy as a fundamental right. The minority judges said that the right to privacy was both the right to personal liberty and freedom of movement as well. Thereafter, there are a plethora of cases before the Supreme Court of India in which our dynamic judiciary had time and again confirmed the right to privacy of Indian Citizens. However, the government's submission to the Supreme Court in July 2015 that there is no fundamental right to privacy gave the issue of privacy as a right new weight. The Supreme Court of India, on its part, assembled a bench of five judges to hear the arguments made on this basis. Ultimately on 26/09/2018 in the case of Justice K. S. Puttaswamy and Ors. Vs. Union of India and Ors. (2019)[8] right to privacy has been declared as a fundamental right. Although the right to privacy has been declared as a fundamental right the laws protecting the same are not up to the mark and in the name of security surveillance continues to be the most significant invasion of privacy.

Until August 2023 India did not have any specific legislation governing data protection and data privacy, but rather, broadly follows the consent-based regime concerning the collection and processing of information which includes personal information as well, subsumed into the applicable rules of the Information Technology Act, 2000. Section 72 of the Act provides for a penalty for breach of confidentiality and privacy with imprisonment for a term which may extend to two years, or with a fine which may extend to Rs.1,00,000/- (Rupees One Hundred Thousand) only. The relevant laws governing data protection and the principle of privacy in India broadly are the Information Technology Act, 2000 and its corresponding rules under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

However, India has enacted a comprehensive data protection law based on the draft Personal Data Protection Bill, 2019 which was inspired by the General Data Protection Regulation (GDPR) which is a legal framework that sets guidelines for the collection and processing of personal information from individuals framed by the European Union (EU). The law was enacted on August 11, 2023. The Act recognizes the right of individuals to protect their personal data and the need to process it for lawful purposes. It establishes procedures for processing personal data in a lawful manner. The Act allows personal data to be processed for

[7] Kharak Singh vs. The State of U.P. and Ors. AIR 1963 SC 1295
[8] Justice K. S. Puttaswamy and Ors. Vs. Union of India and Ors. (2019)1 SCC 1

any lawful purpose. The entity processing data can do so either by taking the concerned individual's consent or for “legitimate uses”. The Act applies to all digital personal data in India, regardless of whether the data was originally collected in digital or non-digital format and subsequently digitized. However, the government can exempt state agencies from the provisions of the Act at its discretion.

The Digital Personal Data Protection Act (DPDP) of 2023 has some limitations and loopholes that do not adequately address the challenges posed by AI and facial recognition technologies in protecting data and privacy. The law exempts publicly available data from its scope, which means that AI and facial recognition companies can scrape and use such data without any consent or accountability. This could lead to privacy violations, discrimination, or manipulation of people based on their online activities, preferences, or identities. The law does not define or regulate biometric data, which is a type of sensitive personal data that includes facial images, fingerprints, iris scans, etc. Biometric data is often used by AI and facial recognition systems to identify, verify, or authenticate individuals. However, biometric data is also prone to errors, breaches, or misuse, and can have serious implications for people’s rights and freedoms. The law does not provide any specific safeguards or restrictions for the use of AI and facial recognition technologies by law enforcement authorities. The law allows such authorities to process personal data for the purposes of prevention, detection, investigation, or prosecution of any offence, without any judicial oversight or transparency. This could result in arbitrary or excessive surveillance, profiling, or targeting of individuals or groups, especially those who are marginalized or vulnerable. The law does not address the cross-border transfer or sharing of personal data with foreign entities or governments, which could involve AI and facial recognition technologies. The law leaves the details of such transfers to the discretion of the central government, which could compromise the data sovereignty and security of India and its citizens.

Another criticism of the Digital Personal Data Protection Act (DPDP) of 2023 is that it gives the government the power to exempt any state agency from the provisions of the Act at its discretion. This means that the government can decide which agency can process personal data without following the rules and safeguards of the Act, such as obtaining consent, ensuring data quality, or providing data protection impact assessments. Such broad exemptions can be misused for surveillance and put the interests of the State ahead of the right to privacy of individuals. This could create a lack of accountability and transparency in the use of personal

data by state agencies, and potentially violate the privacy rights of individuals. According to Section 17 (2) of the Act, the central government can issue a notification exempting any instrumentality of the state from the provisions of the Act if the processing of personal data is in the interests of the sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order, or preventing incitement to any cognizable offence relating to any of the above. However, the Act does not define what constitutes an instrumentality of the state, or what criteria the government will use to grant such exemptions. This leaves a lot of room for interpretation and discretion by the government, which could lead to arbitrary or discriminatory decisions. Moreover, the Act does not provide any mechanism for judicial review or oversight of the government's decisions to exempt state agencies from the provisions of the Act. This means that there is no way for individuals or civil society to challenge or question the validity or necessity of such exemptions, or to seek redress or remedy for any harm caused by the processing of personal data by exempted state agencies. This could undermine the rule of law and the constitutional right to privacy of individuals in India. Therefore, the Digital Personal Data Protection Act (DPDP) of 2023 should be amended to limit the scope and frequency of exemptions granted to state agencies, and to provide clear and objective criteria and procedures for granting such exemptions. The Act should also ensure that the government's decisions to exempt state agencies from the provisions of the Act are subject to judicial review and public scrutiny, and that individuals have the right to access, correct, or delete their personal data processed by exempted state agencies, or to seek compensation for any damage caused by such processing.

Case Study:

The recent incident involving a deepfake video featuring Indian actress Rashmika Mandanna[9] has highlighted the urgent need for effective regulation of Artificial Intelligence (AI) and Facial Recognition Technologies (FRTs) in India. This case study delves into the incident, its legal implications, and the subsequent legal developments.

A deepfake video emerged on various social media platforms, portraying Rashmika Mandanna's face morphed onto another person's body in a manner both distasteful and misleading. The video not only raised concerns about the privacy and data rights of the actress

[9] "Rashmika Mandanna deepfake video: Delhi Police registers case," India Today *available at:* https://www.indiatoday.in/india/story/rashmika-mandanna-deepfake-video-delhi-police-case-registered-2461547-2023-11-10 (last visited January 2, 2024).

but also underscored the potential for deepfake technology to be misused for defamation, intellectual property infringement, and manipulation of public opinion. The Delhi Police initiated legal proceedings by filing a First Information Report (FIR) under Sections 465 (forgery) and 469 (harming reputation) of the Indian Penal Code, 1860, and Sections 66C (identity theft) and 66E (privacy violation) of the Information Technology Act, 2000. This legal action acknowledged the multifaceted nature of the offense, covering forgery, harm to reputation, identity theft, and privacy violation.

India's Data Protection and Privacy Act (DPDP Act), enforced in August 2023, marked a significant step in regulating the processing of digital personal data. However, it did not explicitly address the challenges posed by deepfake videos. The newly enacted Bharatiya Nyaya Sanhita, 2023, replaced the archaic Indian Penal Code and introduced offenses like cyber fraud but failed to explicitly define or criminalize the creation or dissemination of deepfake videos.

The legal landscape witnessed a landmark development when the Delhi High Court ruled on a similar matter involving celebrities Anil Kapoor and Amitabh Bachchan.[10] In the case of Anil Kapoor v. Simply Life India and Ors., the court held that the face and voice data of celebrities cannot be used without their consent in creating AI-generated videos. Anil Kapoor's successful lawsuit, which aimed to protect his personality rights, demonstrated the court's recognition of the need for legal and ethical safeguards in the realm of deepfake technology. On the same line, the legendary actor Mr. Amitabh Bachchan in the case Amitabh Bachchan v. Rajat Negi and Ors. was granted ad interim in rem injunction against the unauthorized use of his personality rights and personal attributes such as voice, name, image, likeness for commercial use.

While the Delhi High Court's ruling sets a precedent for protecting individuals' rights in the age of deepfakes, it also emphasizes the gaps in current legislation. There is a pressing need for a comprehensive legal framework specifically addressing AI and FRTs, with a focus on deepfake technology. This framework should define and regulate the use of deepfake technology, outline rights and obligations, and establish technical and ethical standards for

[10] Vikrant Rana Thakur Anuradha Gandhi And Rachita, "Deepfakes And Breach Of Personal Data – A Bigger Picture," 2023available at: https://www.livelaw.in/law-firms/law-firm-articles-/deepfakes-personal-data-artificial-intelligence-machine-learning-ministry-of-electronics-and-information-technology-information-technology-act-242916 (last visited January 2, 2024).

development and deployment.

The Rashmika Mandanna deepfake incident underscores the urgency of regulatory measures to address the ethical challenges posed by AI and FRTs. The legal response, legislative gaps, and the Delhi High Court's ruling collectively highlight the intricate balance required between technological innovation and the protection of individual rights in the evolving landscape of deepfake technology. This case study contributes to the broader discourse on the need for a robust legal framework that navigates the complexities of AI, FRTs, and deepfake technologies in India.

Potential benefits of facial recognition technology in enhancing security:

Facial recognition technology offers several potential benefits in enhancing security across various sectors and applications. Some of the key advantages include:

1. **Enhanced Identification and Authentication:** Facial recognition can accurately and quickly identify individuals based on their unique facial features, providing a reliable method of authentication.[11] This technology can be integrated into access control systems, replacing traditional methods like ID cards or passwords, thereby reducing the risk of unauthorized access.
2. **Improved Surveillance and Public Safety:** Facial recognition systems enable real-time monitoring of public spaces, critical infrastructure, and crowded events.[12] This capability allows law enforcement and security personnel to detect and respond promptly to potential threats, including criminals, suspects, or missing persons.
3. **Crime Prevention and Investigation:** By cross-referencing facial data with criminal databases, law enforcement agencies can efficiently identify and apprehend individuals involved in criminal activities.[13] This can lead to a deterrence effect, reducing the likelihood of crimes being committed.
4. **Border Security and Immigration Control:** At border crossings and immigration checkpoints, facial recognition technology can streamline and expedite the process of

[11] Shaxun Chen, Amit Pande and Prasant Mohapatra, "Sensor-assisted facial recognition: an enhanced biometric authentication system for smartphones" *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services* 109–22 (Association for Computing Machinery, New York, NY, USA, 2014).
[12] Sikender Mohsienuddin Mohammad, "Facial Recognition Technology" (Rochester, NY, 2020).
[13] Isadora Neroni Rezende, "Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective," 11 *New Journal of European Criminal Law* 375–89 (2020).

verifying travellers' identities.[14] This helps improve border security by identifying persons of interest and potential threats.

5. **Anti-Terrorism Efforts:** Facial recognition can aid in identifying and tracking suspected terrorists or individuals affiliated with extremist organizations.[15] It enables law enforcement agencies to pre-emptively detect potential threats and prevent terrorist acts.
6. **Enhanced Retail and Customer Service:** In the retail industry, facial recognition can be used to enhance customer experiences by recognizing loyal customers and personalizing services accordingly.[16] It can also help identify shoplifters or potential security threats, thereby improving store security.
7. **Remote Biometric Authentication:** Facial recognition can facilitate secure remote authentication for various online services and financial transactions.[17] This reduces the risk of identity theft and fraudulent activities.
8. **Missing Persons and Amber Alerts:** Facial recognition technology can be instrumental in locating missing persons, especially children, by analyzing surveillance footage and comparing it with databases of known individuals.[18]
9. **Health and Safety Applications:** In the wake of the COVID-19 pandemic, facial recognition has been used to monitor mask compliance and social distancing in public spaces, contributing to public health efforts.[19]
10. **Customization and Personalization:** In various industries like entertainment and marketing, facial recognition can be utilized to personalize experiences for users, such as recommending content based on facial expressions or emotional reactions.[20]

[14] Jose Sanchez del Rio et al., "Automated border control e-gates and facial recognition systems," 62 *Computers & Security* 49–72 (2016).
[15] James Jay Carafano, The Future of Anti-Terrorism Technologies (Heritage Foundation, 2005).
[16] Elias Wright, "The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector," 29 Fordham Intellectual Property, Media & Entertainment Law Journal 611 (2018).
[17] J. Aravinth and S. Valarmathy, "Multi classifier-based score level fusion of multi-modal biometric recognition and its application to remote biometrics authentication," 64 *The Imaging Science Journal* 1–14 (2016).
[18] "Facial Fiction Becoming Fact: Facial Recognition Technologies Continue to Improve in Performance | Office of Justice Programs," *available at:* https://www.ojp.gov/ncjrs/virtual-library/abstracts/facial-fiction-becoming-fact-facial-recognition-technologies (last visited July 19, 2023).
[19] S. Sulochanan Karthick Ramanathan, Rani Fathima Kamal Basha and Asan Banu, "A novel face recognition technology to enhance health and safety measures in hospitals using SBC in pandemic prone areas," 45 *Materials Today: Proceedings* 2584–8 (2021).
[20] James M. Tien, "Toward the Fourth Industrial Revolution on Real-Time Customization," 29 *Journal of Systems Science and Systems Engineering* 127–42 (2020).

Critical examination of the risks and limitations of facial recognition systems:

Facial recognition systems, while offering various benefits, also come with significant risks and limitations that warrant careful consideration. Some of the key risks and limitations include:

1. **Privacy Concerns:** Facial recognition technology raises significant privacy issues, as it involves the collection and storage of biometric data without individuals' explicit consent.[21] Continuous surveillance through facial recognition systems can lead to an invasion of privacy and erode individuals' right to anonymity and freedom of movement.
2. **Inaccuracy and Bias:** Facial recognition systems may suffer from inaccuracies, leading to false positives and false negatives.[22] These inaccuracies can result from variations in lighting conditions, facial expressions, ageing, or changes in appearance due to accessories or facial hair. Moreover, these systems can exhibit bias, misidentifying certain demographic groups, leading to potential discrimination and civil rights violations.
3. **Security Vulnerabilities:** Facial recognition databases are attractive targets for hackers and cybercriminals.[23] Unauthorized access to biometric data can have severe consequences, including identity theft and misuse of personal information.
4. **Lack of Regulation and Standards:** The rapid adoption of facial recognition technology has outpaced the development of comprehensive regulations and standards.[24] As a result, there is a lack of uniform guidelines governing the ethical use, storage, and sharing of facial recognition data.
5. **Function Creep:** Facial recognition systems intended for specific security purposes can be repurposed for other applications without individuals' knowledge or consent.[25] This "function creep" raises concerns about the expansion of surveillance and the potential misuse of biometric data.
6. **Social Implications:** Constant monitoring through facial recognition can lead to a chilling effect on individual behaviour, affecting personal freedoms and self-

[21] K.W. Bowyer, "Face recognition technology: security versus privacy," 23 *IEEE Technology and Society Magazine* 9–19 (2004).
[22] Yi Zeng et al., "Responsible Facial Recognition and Beyond" (arXiv, 2019).
[23] A. Peña et al., "Facial Expressions as a Vulnerability in Face Recognition" 2021 *IEEE International Conference on Image Processing (ICIP)*, 2021.
[24] Monique Mann and Marcus Smith, "Automated facial recognition technology: Recent developments and approaches to oversight," 40 *UNIVERSITY OF NEW SOUTH WALES LAW JOURNAL* 121–45 (2020).
[25] James Riley, "Face recognition, function creep and democracy" InnovationAus.com, 2020 *available at:* https://www.innovationaus.com/face-recognition-function-creep-and-democracy/ (last visited July 19, 2023).

expression.[26] The feeling of being under surveillance may also impact social interactions and impede community trust.

7. **False Arrests and Misidentification:** In law enforcement contexts, relying solely on facial recognition for identifying suspects can lead to false arrests and wrongful convictions.[27] Human verification is essential to prevent such miscarriages of justice.
8. **Ethical and Legal Challenges in Consent:** Obtaining informed consent for the use of facial recognition data can be challenging, especially in public spaces where individuals might not be aware of being monitored.[28]
9. **Lack of Transparency:** Some facial recognition systems use proprietary algorithms, making it challenging to assess their accuracy and potential biases.[29] A lack of transparency can hinder the ability to scrutinize and improve these systems.
10. **Data Retention and Deletion:** The retention and deletion of facial recognition data raise concerns about the permanence of personal information and the potential for unauthorized access even after the intended use.[30]
11. **Cross-Border Data Sharing:** International sharing of facial recognition data raises jurisdictional and privacy concerns, as data protection laws may vary significantly between countries.[31]
12. **Social Justice and Equity:** Facial recognition systems can exacerbate existing societal inequalities by disproportionately affecting marginalized communities and minority groups.[32]

Balancing the trade-off between security and privacy:

It is a difficult and delicate undertaking to strike a balance between security and privacy, especially in the context of facial recognition technology and monitoring systems. To guarantee

[26] Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (NYU Press, 2011).
[27] Laura Moy, *"Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions"* (Rochester, NY, 2021).
[28] Inioluwa Deborah Raji and Genevieve Fried, "About Face: A Survey of Facial Recognition Evaluation" (arXiv, 2021).
[29] Denise Almeida, Konstantin Shmarko and Elizabeth Lomas, "The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks," 2 *AI and Ethics* 377–87 (2022).
[30] Jawahitha Sarabdeen, "Protection of the rights of the individual when using facial recognition technology," 8 *Heliyon* e09086 (2022).
[31] Monika Zalnieriute, "Protests and Public Space Surveillance: From Metadata Tracking to Facial Recognition Technologies" (Rochester, NY, 2021).
[32] Sidney Perkowitz, "The Bias in the Machine: Facial Recognition Technology and Racial Disparities*" MIT Case Studies in Social and Ethical Responsibilities of Computing* (2021).

public safety and uphold people's fundamental rights to privacy and autonomy, it is crucial to strike this balance. From the above discussion, we have seen the benefits and potential of facial recognition technology. Today in order to develop no nation will be reluctant in using such promising technologies which have the potential to identify and recognise a potential threat from CCTV footage and neutralize the same for the safety and prosperity of the citizens. However, the researcher has already highlighted certain difficulties as such technologies are not one hundred per cent accurate (although claimed by the companies) and cannot be relied upon totally to form the basis of conviction. On the 16th of February 2023, the German Federal Constitutional Court declared the use of Palantir surveillance software by police in Hesse and Hamburg unconstitutional in a landmark judgment because it raised the risk of mistakes and discrimination by law enforcement agencies.[33] The idea that the accused should always be given the benefit of the doubt is one of the fundamental tenets of the criminal justice system. One innocent person shouldn't be punished even if a thousand criminals get away with it. Therefore, two things can be asserted. First, that the technology is still in its infancy and that, perhaps, one day, it will be faultless; and second, that its usage should be strictly controlled so that it cannot be abused.

Findings and Analysis:

1. **Pervasive Deployment Without Oversight:** In India, FRT has been rolled out in over 75 airports and railway stations under the DigiYatra and safe-city projects. Law enforcement agencies in Delhi, Telangana, and Uttar Pradesh use facial recognition to identify suspects during protests or public gatherings. However, there is no national law regulating FRT deployment, unlike the EU where GDPR provisions and the upcoming EU AI Act demand explicit safeguards. The absence of a clear framework in India risks unchecked expansion of surveillance networks.
2. **Privacy at Risk Despite Constitutional Recognition:** The Supreme Court's decision in *K.S. Puttaswamy v. Union of India* (2018) firmly established the right to privacy as a fundamental right under Article 21. Yet, mass surveillance through FRT continues without explicit consent or adequate legal justification. For instance, police in Delhi used FRT to scan protest crowds during the anti-CAA demonstrations, raising questions of whether surveillance undermines the principles laid down in *Puttaswamy*.

[33] "German Constitutional Court strikes down predictive algorithms for policing," www.euractiv.com, 2023 *available at:* https://www.euractiv.com/section/artificial-intelligence/news/german-constitutional-court-strikes-down-predictive-algorithms-for-policing/ (last visited July 19, 2023).

3. **Loopholes in the Digital Personal Data Protection Act, 2023:** The DPDP Act, 2023 exempts state agencies from its provisions under vague grounds of "national security" and does not classify biometric data separately for higher protection. Section 17(2) allows wide exemptions for government bodies without judicial oversight. By contrast, under GDPR Article 9, biometric data is classified as "special category data," requiring higher safeguards. This legal lacuna in India creates an environment ripe for misuse.
4. **High Risk of Bias and Discrimination:** Global studies, including MIT's 2018 Gender Shades project, revealed error rates of up to 34% for darker-skinned women compared to less than 1% for lighter-skinned men. In India, where marginalized groups already face systemic disadvantages, biased algorithms could reinforce inequality. There are reports of FRT being disproportionately deployed in regions with minority populations, echoing global concerns of racial and communal profiling.
5. **Deepfake and Identity Theft as Emerging Threats:** The Rashmika Mandanna deepfake incident in 2023 triggered nationwide debate on AI misuse. Though the Delhi Police registered an FIR under IPC and IT Act provisions, no specific law addresses deepfakes. The Delhi High Court in *Anil Kapoor v. Simply Life India* (2023) and *Amitabh Bachchan v. Rajat Negi* (2022) granted injunctions to protect celebrity rights, setting precedents for personality rights in India. However, ordinary citizens lack similar legal protection, leaving them exposed to reputational harm and identity theft.
6. **Security Gains Remain Contested:** Proponents argue FRT aids law enforcement. For instance, Delhi Police claimed their FRT system helped identify 1,100 missing children in four days in 2018. However, critics highlight that the same technology has been used to monitor political dissent. In Germany, the Federal Constitutional Court (2023) struck down police use of Palantir software for predictive surveillance, citing disproportionate intrusion into citizens' rights. This highlights the tension between claimed security benefits and actual civil liberty risks.
7. **Absence of Accountability Mechanisms:** Currently, there is no legal requirement in India for transparency reports or independent audits of FRT use. By comparison, UK's Surveillance Camera Code of Practice (2013) mandates public accountability for CCTV and biometric systems. The absence of similar provisions in India leaves citizens without remedies in cases of wrongful arrests or misuse of data.
8. **Chilling Effect on Civil Liberties:** Continuous monitoring discourages participation in protests and civic movements. The Internet Freedom Foundation (IFF) reported that facial recognition was deployed during farmers' protests in Delhi, raising concerns

about surveillance being weaponized to deter dissent. This aligns with the chilling effect doctrine articulated by the U.S. Supreme Court in *Lamont v. Postmaster General* (1965), where surveillance of speech was found to discourage free expression.

9. **Weak International Harmonisation:** India's DPDP Act does not adequately regulate cross-border data transfers. In contrast, GDPR Chapter V imposes strict conditions on transfers to non-EU countries. This gap means that Indian biometric data can potentially be shared with global corporations or foreign governments without sufficient safeguards, undermining data sovereignty.
10. **Potential for Function Creep:** Globally, FRT systems introduced for terrorism prevention have expanded to commercial uses like retail tracking and workplace surveillance. In India, police departments initially claimed FRT use for child protection but later deployed it during public demonstrations. This gradual shift, known as "function creep", mirrors the warning of Justice Subba Rao's dissent in *Kharak Singh v. State of U.P.* (1962), where he cautioned that surveillance mechanisms, if unchecked, could erode liberty incrementally.

Recommendations:

1. **Establish a Comprehensive Legal Framework:** Enact a dedicated Facial Recognition and Biometric Surveillance Regulation Act in India, drawing on global models like the EU AI Act and GDPR, to set out clear rules for permissible uses, prohibited practices, and enforcement mechanisms.
2. **Mandate Judicial Authorization for Surveillance:** Require prior judicial approval or independent oversight before law enforcement can deploy FRT in public spaces, ensuring alignment with the constitutional principles of proportionality and necessity laid down in *Puttaswamy (2018)*.
3. **Amend the Digital Personal Data Protection Act, 2023:** Introduce explicit provisions for biometric data as a sensitive category of personal data, restrict exemptions for state agencies, and impose strict penalties for unlawful use of FRT.
4. **Address Algorithmic Bias Through Regulation and Audits:** Mandate independent algorithmic audits to detect and mitigate bias, require publication of error rates, and enforce accountability on companies deploying FRT systems to ensure non-discrimination against vulnerable communities.
5. **Criminalize Deepfakes and Identity Theft:** Introduce new offences under the Bharatiya Nyaya Sanhita (2023) to explicitly criminalize the creation and dissemination

of deepfakes. Extend personality rights protections (currently benefiting celebrities) to all citizens, with remedies including injunctions and compensation.

6. **Balance Security Gains with Rights Protection:** Adopt a "strict necessity and proportionality" test before deploying FRT in law enforcement. Security agencies should be required to demonstrate that no less-intrusive alternatives exist, similar to the standard upheld by the German Constitutional Court.
7. **Ensure Accountability Through Transparency Mechanisms:** Mandate annual transparency reports by all state agencies and corporations using FRT, covering purpose, scope, accuracy, and number of false matches. Establish an independent Data Protection Authority with oversight powers, public complaint mechanisms, and audit mandates.
8. **Safeguard Civil Liberties and Democratic Freedoms:** Prohibit FRT deployment at protests, political rallies, and other civic gatherings to protect the rights to free speech, assembly, and association. Implement "privacy by design" safeguards to minimize risks of mass surveillance.
9. **Strengthen International Data Protection Standards**: Introduce strict rules on cross-border transfers of biometric data, ensuring parity with GDPR standards. India should pursue bilateral and multilateral agreements to prevent misuse of citizens' biometric data by foreign corporations or governments.
10. **Prevent Function Creep Through Purpose Limitation:** Codify the principle of purpose limitation in law, restricting FRT to its declared purpose (e.g., child safety, border security). Any expansion of scope must undergo parliamentary scrutiny and public consultation before approval.

Conclusion:

The unfolding debate on facial recognition technology in India represents far more than a technical or legal question, it is a test of how a constitutional democracy balances innovation with its most cherished freedoms. This study has shown that while FRT holds undeniable promise in advancing security, streamlining identification, and even aiding humanitarian objectives like locating missing persons, its unregulated spread creates disproportionate risks to privacy, equality, and liberty. The constitutional recognition of privacy in *Puttaswamy* stands in stark contrast to the unbridled surveillance practices that continue to flourish in India under weak legislative safeguards and broad state exemptions. The Digital Personal Data Protection Act, 2023, though a landmark step, reveals troubling gaps in addressing biometric data,

algorithmic accountability, and state overreach. Cases such as the *Rashmika Mandanna deepfake incident* and the Delhi High Court rulings on celebrity personality rights further illustrate the pressing need for legal adaptation in the face of AI-generated harms. Comparative insights from jurisdictions such as the EU, UK, and Germany demonstrate that democratic societies can, and must, impose strict proportionality standards, transparency requirements, and human rights safeguards while still enabling security objectives. Without similar frameworks, India risks drifting into a digital panopticon, where citizens are perpetually watched, profiled, and judged without recourse. The challenge, therefore, is not to reject FRT outright, but to build a governance architecture rooted in accountability, purpose limitation, and the ethical use of technology. By institutionalizing privacy by design, mandating independent audits, restricting surveillance at civic spaces, and embedding judicial oversight, India can shape a rights-respecting model that reconciles technological advancement with constitutional morality. Ultimately, the discourse on FRT is a mirror of our broader struggle to uphold human dignity in an era where lines between liberty and security are increasingly blurred. The way forward lies in embracing technology responsibly, legislating with foresight, and ensuring that the promise of artificial intelligence strengthens rather than undermines the democratic values of justice, freedom, and equality.