INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ARTIFICIAL INTELLIGENCE-BASED FACIAL RECOGNITION TECHNOLOGY IN INDIA: A CRITICAL ANALYSIS OF THE RIGHT TO PRIVACY AND THE NEED FOR A REGULATORY FRAMEWORK

AUTHORED BY - J.M. ANISHA

ABSTRACT

The development of Artificial Intelligence, such as Facial Recognition Technology allows public authorities to collect process and utilise information in new ways. Facial Recognition Technology is used to identify or confirm an individual using facial features by using digital images and videos. In India, there has been an increasing amount of attention paid to the use of facial recognition technology by law enforcement agencies such as police. This can be used to identify suspects, find missing persons and improve public safety. However, there are significant concerns around this technology concerning privacy, personal liberty, data protection and potential misuse.

It is recognised as a fundamental right in relation to privacy in India under Article 21 of the Constitution due to the ruling in Justice K.S. Puttaswamy v. Union of India. This judgement means any interference with your privacy by the State must meet the principle of legality, legitimate aim and proportionality. There have been laws introduced in relation to personal data protection and biometric data collection however these do not provide a full and specific framework for the use of facial recognition technology by the police.

This paper will look at how the use of facial recognition technology by police can impact on your constitutional right to privacy in India. It will look at the current legal framework, problems with incorrect identification and bias created by the algorithms. It will also look at some examples of how countries worldwide regulate facial recognition technology. This paper will argue that for technology to develop there must be clear guidelines, independent monitoring and accountability to ensure that public safety is not impacted upon by fundamental rights.

ISSN: 2582-6433

1. INTRODUCTION

Artificial Intelligence has become a huge part of current society, with multiple areas of society being influenced, from communications, to healthcare, education, transport and law enforcement. One major area of AI is Facial Recognition Technology. This uses computer based systems to analyse a person's facial features and match them to photographs or facial data in a database. This means individuals can be identified by authorities.

Within law enforcement, facial recognition technology has been seen as a way to help make citizens safer and aid criminal investigations. Police can use facial recognition technology to identify suspects, locate missing people, monitor public areas and match images obtained from CCTV cameras. Within a country such as India, where public areas are often overcrowded, this may provide some benefits to authorities.

However, there are concerns about using this technology. Unlike regular CCTV cameras, individuals can be identified and linked to personal information. This can make individuals continuously monitored and personal data being collected on a large scale without them knowing. This could lead to issues with personal privacy, personal freedom of expression and freedom to participate in peaceful activities.

Personal privacy is a fundamental part of an individual's right to life and personal freedom, protected under article 21 of the Indian Constitution. In Justice K.S. Puttaswamy v. Union of India the Supreme Court recognised privacy as a fundamental right. Any actions taken by the state to affect an individuals privacy must meet constitutional standards[1]. The judgement stated that any interference with privacy must be lawful, further the interference must be for a proper purpose by the state and must meet proportionality[2].

India have implemented multiple laws regarding personal information, biometric data and electronic data. The Digital Personal Data Protection Act, 2023 sets out rules for how digital personal data should be processed. The Criminal Procedure (Identification) Act, 2022 covers how measurements of certain people involved in criminal proceedings should be collected and preserved[3]. However, these do not cover how facial recognition technology should be used by police in a detailed manner.

The key issue here is not that facial recognition technology should be entirely banned, but whether it can be controlled so constitutional rights are protected whilst still allowing police to

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[2] Id.
[3] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023); Criminal Procedure (Identification) Act, No. 11 of 2022, INDIA CODE (2022).

ISSN: 2582-6433

conduct legitimate activities. Police surveillance should have boundaries set by law.

This paper will look at the legal and constitutional issues around facial recognition technology being used by police in India. It will also look at the need for specific controls to be put into place regarding transparency, accuracy, data storage and accountability.

2. REVIEW OF LITERATURE

The relationship between facial recognition technology and individual privacy has been widely discussed within legal, policy and technological research. Literature reveals many advantages and concerns around facial recognition technology.

The ruling provided by the Supreme Court in Justice K.S. Puttaswamy v. Union of India can be used as the basis for understanding how facial recognition technology is used within India. The ruling identifies information privacy as a key component of individual autonomy and outlines that any interference from the state must be lawful, have a legitimate aim and be proportionate[4]. Although the case did not focus specifically on facial recognition technology, the principles can be applied to understand how public authorities may use facial recognition technology in a digital way.

A discussion paper published by NITI Aayog titled Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology (2022) looks into the practical application of facial recognition technology and how it can cause risk. The document identifies concerns around privacy, bias, accuracy, transparency and accountability. Recommendations are made that facial recognition technology should be developed and used responsibly with human oversight and proper safeguards[5]. As the document is relevant to the Indian context, it also acknowledges that social and demographic factors need to be considered during design.

Research undertaken by Joy Buolamwini and Timnit Gebru in their paper titled Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification (2018) show that there are disparities in the accuracy of facial analysis systems based on an individual's demographic. It demonstrates how technology can cause inequality if it is trained on data that does not represent the population well[6]. Although this focuses on commercial gender classification systems, it still provides useful evidence on the potential risks of bias.

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

[5] NITI AAYOG, RESPONSIBLE AI FOR ALL: ADOPTING THE FRAMEWORK—A USE CASE APPROACH ON FACIAL RECOGNITION TECHNOLOGY (Nov. 2022).

[6] Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 PROC. MACH. LEARNING RSCH. 1 (2018).

ISSN: 2582-6433

The National Institute of Standards and Technology (NIST) has looked into the differences in accuracy within facial recognition algorithms via their research. They found that accuracy can vary depending on the algorithm used, quality of the image and the demographics of the individual[7]. This is relevant when determining if any results gathered from facial recognition technology should be trusted.

International legislation has also provided some useful insight. The European Union has created legislation titled Artificial Intelligence Act, 2024 that limits the use of real time remote biometric identification in publicly accessible areas by law enforcement with only very specific exceptions and safeguards[8]. There was also a ruling by the Court of Appeal in R (Bridges) v. Chief Constable of South Wales Police looking into how police authorities are using automated facial recognition within the UK. This identified that there should be clear legal guidelines, proportionality and proper safeguards[9].

Whilst all of these documents give a good basis into the risks and regulation of facial recognition technology, it is important to look at the legal position in India. The relationship between police surveillance, a constitutional right to privacy and no specific regulation needs to be investigated further. This essay will attempt to do so by looking at how well current laws are within India and what safeguards are needed.

3. FACIAL RECOGNITION TECHNOLOGY AND ITS USE IN POLICE INVESTIGATIONS

3.1 Nature, Applications and Growing Use of Facial Recognition Technology

Facial Recognition Technology uses AI to identify individuals and works through three different stages. The system detects the face, extracts facial features and matches the face to compare against.

The system identifies a face within an image or video. Then, it will detect the facial features and convert them into digital data. Finally, the facial recognition software compares the data to images already held within a database to determine if there a potential match.

There are generally two different types of facial recognition. Verification will confirm that the individual is who they say they are. Identification determines whether there is a potential match between the individual's face and a database with multiple records. This type of facial

[7] NAT'L INST. OF STANDARDS & TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS, NISTIR 8280 (2019).
[8] Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L) 1689, art. 5.
[9] R (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058 (Eng.).

ISSN: 2582-6433

recognition can be useful for police as it can help to identify individuals using CCTV footage or images.

Facial recognition technology has been looked at and used in India for various law enforcement reasons. This includes identifying individuals wanted for criminal cases, finding missing people, helping with investigations and monitoring public areas. NITI Aayog identified that facial recognition technology was being used by police in states such as Punjab, Gujarat and Tamil Nadu[10].

For police, this could help speed up the process of identifying individuals. It could help police with handling large amounts of visual data and help find missing children. It could also help to identify individuals that are linked to serious criminal investigations.

Whilst there are many benefits to using facial recognition technology, there are also some limitations. Facial recognition doesn't always confirm that the individual is who they are. It will provide a result based on mathematical calculations. There are many factors that can affect how accurate the result is, such as the quality of the image, lighting, camera angle, facial expression and quality of the database.

Therefore, this should only be seen as a lead for investigation. If police authorities use inaccurate results without verifying independently this could cause an innocent individual to be suspected of something they didn't do.

Facial recognition systems can cause issues with over-surveillance. If the facial recognition systems are placed in public areas then individuals can be identified even if they are not suspected of doing anything wrong. This causes concerns over how much information the state should be collecting and analysing for normal citizens.

Although facial recognition technology could help with legitimate policing, it should be restricted and kept transparent.

3.2 Constitutional Right to Privacy and the Adequacy of the Indian Legal Framework

A key issue relating to the usage of facial recognition technologies by Government authorities is the right to privacy. This is derived primarily from Article 21 of the Indian Constitution, which protects the right to life and personal liberty.

The landmark 'Justice K.S. Puttaswamy v. Union of India' case (2017), confirmed that the right to privacy was a constitutional right. The Supreme Court recognised privacy as a fundamental right and includes personal autonomy, bodily privacy, and informational privacy.

[10] NITI AAYOG, supra note 5.

ISSN: 2582-6433

It also acknowledged that the right to privacy is not absolute and can be limited if the state meets certain conditions.

There were three conditions provided to ensure privacy is properly interfered with:

Legal- There must be a proper law in place allowing interference.

Legitimate aim- The interference must be for a legitimate reason. This could include ensuring public safety or avoiding crime.

Proportionality- The measure must be proportionate and reasonably related to the aim.

The principle of proportionality has also been discussed in cases such as 'Modern Dental College and Research Centre v. State of Madhya Pradesh'[11].

This is highly relevant when looking at how Police forces may use facial recognition technologies. Although there are legitimate aims to avoid crime and ensure public safety, the authorities will need to prove that the use is legal, necessary, and proportionate.

The Digital Personal Data Protection Act, 2023 is another key provision in relation to data protection. It provides a legal framework regarding the processing of digital personal data. This includes ensuring there is consent, the data is processed lawfully, and there is security in place. If the facial image or template is identifiable then this may be considered personal data[12].

However, there is no specific framework for Police facial recognition technologies. Section 17 (1)(c) means that some processing will be exempt if it is necessary to prevent, detect, investigate or prosecute an offence or contravention of law[13]. This needs to be considered carefully.

An important factor to consider with this Act is that it will come into effect in stages. The main provisions relating to data processing will come into effect eighteen months after 13th November 2025, meaning that they will only come into effect on 13th May 2027[14]. Therefore, at the time of writing (November 2026), these shouldn't be considered active.

The Criminal Procedure (Identification) Act, 2022 provides a legal framework allowing the measurement of certain information such as photographs to be collected and stored[15]. However, this shouldn't be seen as allowing unlimited use of facial recognition technologies.

The Information Technology Act, 2000 also provides a legal framework around electronic information. However, it doesn't provide a full framework for the use of AI based facial

[11] Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353 (India).
[12] Digital Personal Data Protection Act, No. 22 of 2023, § 3, INDIA CODE (2023).
[13] Id. § 17(1)(c).
[14] Ministry of Electronics & Information Technology, Notification No. G.S.R. 843(E), Gazette of India, Extraordinary, Nov. 13, 2025 (India).
[15] Criminal Procedure (Identification) Act, No. 11 of 2022, §§ 2, 3, INDIA CODE (2022).

ISSN: 2582-6433

recognition by Police authorities.

Overall, there are provisions in place to protect privacy and biometric data. However, there aren't provisions in place to fully address all issues regarding Police facial recognition. There should be more specific legal provisions surrounding the creation of watchlists, reasons for use, accuracy of matches, storage timeframes, independent authorisation, and actions in cases of incorrect identification.

Therefore, the constitutional principles set out in Puttaswamy must be followed and facial recognition technologies used accordingly until a full framework is in place.

3.3 Algorithmic Bias, Misidentification and the Need for Regulatory Safeguards

One of the most obvious issues faced by using facial recognition technology is that there could be cases of incorrect identification. Although AI systems will be efficient at analysing information, the quality of the information inputted will affect the outcome of the data.

This could result in algorithmic bias whereby some groups of people within certain demographics receive inaccurate results due to the lack of representation of different skin tones, genders, ages and other facial attributes within the training data. This can cause serious issues when using this technology within criminal investigations.

Research undertaken by Joy Buolamwini and Timnit Gebru has shown that some commercial facial analysis systems do show discrepancies between different demographics. The NIST has also identified discrepancies between different demographics in facial recognition algorithms. This shows how important it is to independently test systems before being implemented within law enforcement[16].

Within India, this is a concern to consider due to the diversity of the population. If facial recognition systems are being developed with training data that does not represent the demographics of India well then results may not be reliable for some groups of people.

If the individual is incorrectly matched then they could be questioned, investigated or even arrested without sufficient independent evidence. This can cause issues with their personal freedoms and reputation. Therefore, results provided should never be considered as evidence that the individual has committed a crime.

Another key issue to consider is the impact on freedom of speech and peaceful protest. Individuals may feel less likely to join protests, public meetings or other lawful activities if they believe their identity and location are constantly being monitored. This can cause a chilling

[16] Buolamwini & Gebru, supra note 6; NAT'L INST. OF STANDARDS & TECH., supra note 7.

ISSN: 2582-6433

effect on individuals exercising their rights within the constitution under article 19.

In People's Union for Civil Liberties v. Union of India, the Supreme Court acknowledged the importance of protecting individuals from arbitrary monitoring by the state. Although this was for monitoring of telephone calls, the reasoning behind this is applicable[17].

India therefore should implement a specific set of regulations that governs how facial recognition technology is used by the police. This should include:

A. Specific and legitimate purposes

Facial recognition technology should only be used for specific and legitimate reasons. General monitoring of the public should not be allowed. The law should outline when the police can use facial recognition technology and what type of investigations it can be used for.

B. Independent approval and monitoring

Before facial recognition systems can be used to monitor individuals intrusively, they should require independent approval from a judicial or administrative body. This should only be allowed in very specific emergencies. Approval should outline why, how long and what the surveillance is for. Independent monitoring would ensure the police cannot use this technology arbitrarily.

C. Accuracy testing and human verification

Regular independent testing should be done to ensure the accuracy of the facial recognition systems. Police should always verify any potential matches with further evidence before taking coercive measures against the individual. It is important that there is a human element to this as the results should not replace professional judgement.

D. Data storage

Facial images and digital representations should not be stored for long periods of time. Any information gathered for a specific investigation should be removed once it is no longer needed. Only authorised individuals should have access to facial recognition databases.

E. Transparency

The public should have access to basic information about the use of facial recognition technology, why it is being used and what safeguards are in place. The police should keep a record of searches, matches and actions taken. Independent auditing should be carried out to identify any misuse, inaccuracies or discriminatory results.

F. Effective complaints process

Individuals who have been incorrectly identified or unlawfully monitored should have an

[17] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).

ISSN: 2582-6433

effective complaints process. If the individual has suffered due to misuse or negligence then those responsible and any other legally responsible parties should face appropriate consequences.

Internationally there are some useful examples. The European Union have created the Artificial Intelligence Act, 2024 which puts severe restrictions in place for real-time remote biometric identification in publicly accessible areas for law enforcement. There are limited exceptions but they must be necessary and proportionate and require independent approval[18].

Within the United Kingdom, the Court of Appeal looked at whether the police use of automated facial recognition was legal. They found there were issues with the law around choosing where and who to target[19]. This shows the importance of having clear rules and appropriate safeguards.

In Glukhin v. Russia, the European Court of Human Rights looked at the use of facial recognition technology by the authorities to identify an individual who had taken part in a peaceful one person protest. They found there had been a breach of the individuals rights under articles 8 and 10 of the European Convention on Human Rights[20]. This shows how facial recognition technology can impact an individuals privacy and freedom of speech.

Although these do not need to be fully incorporated into Indian law, they are a good example of how to regulate new technologies whilst still protecting individuals rights.

India should consider implementing specific legislation or detailed statutory guidance that outlines the use of facial recognition technology by law enforcement. This should provide clear guidelines on how much surveillance can be done, independent monitoring and ensure the technology is held accountable to constitutional values.

4. CONCLUSION

Facial recognition technology powered by artificial intelligence can be used to increase efficiency within police investigations and support public safety. Facial recognition can help law enforcement locate lost people, identify suspects and understand criminal activity. However, there are serious issues surrounding privacy and personal freedom, as well as equality issues.

India recognises the right to privacy through article 21 of the constitution. This means that any action by the state which will affect someone's privacy must be lawful, pursing a legitimate

[18] Regulation (EU) 2024/1689, supra note 8, art. 5.
[19] R (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058 (Eng.).
[20] Glukhin v. Russia, App. No. 11519/20, Eur. Ct. H.R. (July 4, 2023).

ISSN: 2582-6433

aim and be proportionate (Justice K.S. Puttaswamy v. Union of India). These factors are important to consider when using facial recognition technology.

Whilst there is current legislation in place relating to the protection of personal data and biometric data, there is currently no comprehensive legislation in place to deal with facial recognition by law enforcement. There is no clear guidelines regarding how surveillance will be carried out, how data will be managed, how accuracy will be tested, how long data will be stored for, meaning there is a risk of misuse. Algorithmic bias can lead to incorrect identification meaning innocent people could be investigated unnecessarily.

Other countries have shown that specific legal restrictions must be put in place to ensure there is independent oversight.

Therefore, India should consider creating specific legislation or a statute to regulate the use of facial recognition technology by law enforcement. This should outline what can be done with the data, what accuracy standards there are, reduce unnecessary data collection and ensure there is accountability for any unlawful surveillance. Any automatic identification must be checked by a person and there should be judicial oversight.

Technological advancement should not be seen as conflicting with fundamental rights. Facial recognition can be used for a legitimate reason in modern policing however there must be regulations in place to ensure it is used within the confines of the constitution. A balance must be struck between ensuring public safety without losing individual privacy.

5. FOOTNOTES

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
2. Id.
3. Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023); Criminal Procedure (Identification) Act, No. 11 of 2022, INDIA CODE (2022).
4. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
5. NITI AAYOG, RESPONSIBLE AI FOR ALL: ADOPTING THE FRAMEWORK—A USE CASE APPROACH ON FACIAL RECOGNITION TECHNOLOGY (Nov. 2022).
6. Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 PROC. MACH. LEARNING RSCH. 1 (2018).
7. NAT'L INST. OF STANDARDS & TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS, NISTIR 8280 (2019).

ISSN: 2582-6433

8. Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L) 1689, art. 5.
9. R (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058 (Eng.).
10. NITI AAYOG, supra note 5.
11. Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353 (India).
12. Digital Personal Data Protection Act, No. 22 of 2023, § 3, INDIA CODE (2023).
13. Id. § 17(1)(c).
14. Ministry of Electronics & Information Technology, Notification No. G.S.R. 843(E), Gazette of India, Extraordinary, Nov. 13, 2025 (India).
15. Criminal Procedure (Identification) Act, No. 11 of 2022, §§ 2, 3, INDIA CODE (2022).
16. Buolamwini & Gebru, supra note 6; NAT'L INST. OF STANDARDS & TECH., supra note 7.
17. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).
18. Regulation (EU) 2024/1689, supra note 8, art. 5.
19. R (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058 (Eng.).
20. Glukhin v. Russia, App. No. 11519/20, Eur. Ct. H.R. (July 4, 2023).

6. REFERENCES / BIBLIOGRAPHY

A. Constitutional and Statutory Materials

- Constitution of India, 1950.
- Digital Personal Data Protection Act, 2023.
- Digital Personal Data Protection Rules, 2025.
- Criminal Procedure (Identification) Act, 2022.
- Criminal Procedure (Identification) Rules, 2022.
- Information Technology Act, 2000.
- Regulation (EU) 2024/1689 – Artificial Intelligence Act.

B. Judicial Decisions

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.

ISSN: 2582-6433

- People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
- R (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058.
- Glukhin v. Russia, Application No. 11519/20 (European Court of Human Rights, 2023).

C. Books, Research Papers and Reports

- Buolamwini, Joy & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research, Vol. 81, 2018.
- NITI Aayog, Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology, November 2022.
- National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, 2019.

D. Official Online Sources

- NITI Aayog – https://www.niti.gov.in/
- India Code – https://www.indiacode.nic.in/
- Ministry of Electronics and Information Technology – https://www.meity.gov.in/
- European Union Law – https://eur-lex.europa.eu/
- National Institute of Standards and Technology – https://www.nist.gov/
- UK Judiciary – https://www.judiciary.uk/
- European Court of Human Rights – https://www.echr.coe.int/