**Forging Trust: Navigating Artificial Intelligence and Technology Governance for Public Confidence\*[[1]](#footnote-1) \*\*[[2]](#footnote-2)**

**Abstract**

AI-driven tech design and development are becoming prevalent in a tech-centric culture. AI is literally and metaphorically reshaping our lives in agriculture and education. AI originated in the second part of the 20th century, but it has resurged in the past decade. Big Data analytics, data gathering, aggregation, and processing—has driven the emergence of advanced technologies like deep learning, machine learning, neural networks, and processing of natural languages, etc. The political and social and financial implications of AI are raising concerns during this technological revolution. In particular, these developing technologies may conflict with modern democracies' essential values. This is driving discussions about AI ethics and safe and responsible AI use. The present study critically reviewed and analyzed FRT and Digi Yatra as AI applications in the public sphere.

***Key words: Artificial Intelligence, FRT, DIGI Yatra, public trust, effective governance***

**1. Introduction**

India's national policy for leveraging AI's promise while avoiding its drawbacks was issued by NITI Aayog. [1] This was preceded by two more approach papers last year on Indian AI ethics. Constitutional ethical standards have been envisaged as the foundation for AI ethics in India, elevating our fundamental freedoms and culture to the forefront for responsible AI deployment. [2] After establishing the key ethical principles, it is important to evaluate how they are addressed in specific AI use cases within the Responsible Designs, Creation, and Deployment of AI (RAI Principles) framework.

**2. Responsible A.I**

Over time, technical advances have increased computer computational power. First-generation computers had human-implemented programmes. The advent of technology has led to the creation of algorithms, which are computers' instructions to calculate or solve problems and are crucial for all AI systems. [3] Today, an artificial intelligence (AI) system can read a set of commands and decipher the output function that that it requires to perform due to algorithmic advances. These algorithms undergo development on enormous datasets, or data sets for training, which provide them input and output information to recognise the tasks needed for creating an output that takes into account future real-world inputs. Nevertheless, its capacity to self-implement commands and perform these activities based on its training raises unique ethical issues for AI systems in diverse capacities. AI and algorithmic functionalities are being used in the public and private sectors, as discussed in this Paper, posing ethical challenges. Indian ethics investigations into AI systems are not new. NITI Aayog's 2021 AI ethics overview emphasises the need for an ethics-based examination of AI deployment, considering opacity, trustworthiness, understanding, equal treatment, algorithmic bias, exclusions, accountability, and privacy. [4]

**3. FRT (Facial Recognition Technology) as a Concept**

FRT is an artificial intelligence (AI) system that uses pictures or video data to identify or verify a person. [5] FRT is unique in personal identification and verification since faces, or facial picture information, may be recorded and analysed remotely, including covertly. [6] This section paper discusses governmental authorities' use of FRT for authentication and identification and its effects.

**3.1 How does FRT operate?**

FRT is a data-driven AI system that focuses on detection of facial features, extraction of features, and identification. [7] FRT applications identify or verify people using an assortment of facial photos, requiring big facial databases for wider use. This ecosystem requires facial data since FRT programmes undergo prolonged instruction and machine learning procedures using big training datasets before their implementation. [8] Large face data databases are essential for FRT applications.

Facial detection algorithms recognize human faces in images. This alone allows the use of technologies that just care about the presence of a face in an image. However, most FRT uses start with facial detection, and then proceed to extraction of features and recognition of facial features if needed. Feature extraction uses quantitative representations of the distinctive traits on faces found in the first phase to create unique identifiers. Facial recognition concludes with computerized cross-referencing of a person’s facial traits with a gallery dataset.

Facial recognition is widely tilized in 1:1 and 1:n FRT devices. [9] FRT is mostly used in 1:1 systems to authenticate or validate a person’s live face data with a gallery dataset’s facial image data. This occurs in authentication circumstances like unlocking phones or authenticating faces for public services. As shown, 1:1 systems identify two faces through authentication, and greater control throughout the standard of images of faces collected simultaneously at the time of building the gallery data set as well as the time of authorization improve accuracy and reduces verification factors. [10] However, 1:many FRT systems are used for identification, processing multiple images or videos of faces to identify a given person. Law enforcement as well as mass surveillance agencies use 1:many systems for live face recognition technology (LFRT). Using 1:n LFRT systems. This absence of consent and supervised facial data collecting can lower facial data quality and make it erroneous.

**3.2 Rise in use of FRT**

In recent years, FRT development and use have increased significantly due to the massive volumes of facial photographs and video data and advances in image recognition technologies. Government programmes worldwide, including India, collect biometric facial data during public service registration. [11] Gathering biometrics allows manual identity authentication while providing identification documents or using certain services. An increase in FRT computational power permits automatic authentication. Biometric and facial recognition projects have been established in airlines and other areas worldwide.

Social networking platforms and other websites allow millions of photographs to be submitted by individuals worldwide and viewed openly. While the apparently unbridled sharing and utilization of these images without the uploader's consent raises ethical and privacy concerns, social media sites have acknowledged to using this large dataset to train their FRT systems, including image-recognition and image-categorization methods using hashtags. [12]

The pervasive deployment of CCTV cameras has also helped public service facial recognition. The deployment of CCTV cameras in Delhi, Chennai, Hyderabad, Indore, and Bangalore is among the greatest in the world, and India's surveillance unit markets are growing 20-25% annually. CCTV cameras are used worldwide, with China and Russia heading the way, followed by large towns in the UK, South Korea, and the US. Government agencies offering public services are adopting FRT to maximise efficiency and accuracy. Newer FRT systems can identify faces via masks, raising problems about opt-outs and a person's control over their faces. [13]

**3.3 FRT applications deployed in foreign jurisdictions**

Foreign jurisdictions use FRTs in several settings. FRT systems are used for airport access controls, security, surveillance, and law enforcement. Only six of the world's 100 most populous countries did not adopt FRT, likely due to budget/technology constraints rather than ideological resistance. It also found that seven of the 100 most populous nations had deployed FRT extensively.

**3.4 Risks of FRT**

The growing usage of FRT for security and non-security purposes necessitates a deeper look at its hazards. FRT systems provide unique hazards based on their use-case operations and repercussions, in addition to the moral challenges raised by AI systems. This chapter discusses design-based hazards and rights-based difficulties from widespread FRT system adoption.

**3.5 Design-based risks of FRT systems**

The FRT paradigm poses distinct ethical problems when public authorities use FRT technology. While automation bias, discrimination, exclusion, and lack of accountability apply to all AI systems, FRT systems' operations and effects demand a special consideration of their design-based dangers. Greater complexity in computational methods leads to more accurate but less explainable AI system results, affecting accuracy and interpretability. Reviewing inaccuracy-related misidentification, its causes, and its effects is important at this stage.

**3.5.1 Design-based risks**

*1. Technical errors:*

* Intrinsic variables: facial expression, ageing, plastic surgery, disfigurement; or b. Extrinsic factors: lighting, position variation, occlusion, and image quality.

*2. Inaccuracy from underrepresentation bias:*

* Color-based: International studies show skin tone-based mistake rates.
* Gender-based: Indian FRT system studies show error rates differ by gender.
* FRT system import highlights: Categories are used by FRT systems to process facial images. A FRT system built outside India may use categories that don't make sense here.
* Racial bias is especially difficult in India, because there are many communities with different physical and facial traits. A pan-India facial and biometric database is needed to establish a viable FRT system.
* Indian context assessment: FRT systems must be appraised for the Indian setting. The validation mechanism must imitate a real-world facial recognition system encountering purposeful and unintentional unconstrained disguises.

*3. Lack of human operator training causes inaccuracies in FRT systems:*

* FRT systems require human operators to check or act on outputs. The FRT system requires a qualified human operator to avoid misidentification owing to inaccuracy.

*4. Inaccuracy from glitches or perturbations:*

* Small changes can render FRT systems unusable, making them subject to sabotage.

*5. Breaches of data and unauthorised access security risks:*

* Hackers can profit from the massive amounts of facial data collected by FRT system developers and operators.
* The privacy of concerned persons may also be compromised by bad institutional data security practises that leak enormous amounts of personal data.

*6. Legal liability, accountability, and grievances:*

* FRT systems have the ‘many hands problem’ while building, testing, training, and deploying them.
* This raises questions about responsibility and legal consequences for FRT system errors.
* Trade secrets and rights to intellectual property may make it harder for impacted parties to prove prejudice or bias.

**3.6 Rights-based challenges to use of FRT systems**

When considering the privacy and liberty costs of FRT systems, they create significant rights-based challenges. Any FRT system processes biometric face data, a unique identifier for any individual, and therefore any legal analysis falls under personal information security and confidentiality law. However, its potential for state agencies to restrict or harm free expression by rapidly lowering privacy in both the public and private realms prompts liberty discussions.

**3.6.1 Rights-based challenges**

*1. Privacy and informational independence: Puttaswamy*

* In Justice K Puttaswamy v. UoI (2017), the Supreme Court established informational autonomy as a right to privacy under Article 21.
* FRT systems must consume and compute massive volumes of biometrics facial data for training and operation in real life.
* CCTVs, government programmes, and 1:n systems may not inform individuals of the scope for their biometrics facial data being analysed for training or managing a FRT system.
* Security and informational autonomy issues have been raised, and will continue to be raised, in India and around the world, about FRT.
* FRT systems must work within Puttaswamy's bounds and future judicial rulings on this Paper's evolving concepts.

*2. Informational autonomy issues:*

* Using biometric facial photographs for multiple purposes violates the notion of information independence.
* A person who agrees to the first reason may not know, oversight, or agree to the second reason.

**3.7 Legal thresholds applicable to FRT systems**

In 2017, the Supreme Court established a three-pronged test for restricting privacy by the state, including legal validity, legitimate interests, and proportionality, in along with informational autonomy. This test considers national security including legitimate state objectives. In 2018, the Supreme Court broadened the test for proportionality to a four-part test, assessing whether a measure restricting privacy has a legitimate goal, is suitable, least restrictive, equally effective, and does not disproportionately affect the right holder. The wide range of capabilities available through FRT makes it vital for effective protections and regulatory structures that moderate and regulate biometric personal data transport, use, and preservation.

**3.8 Regulatory aspects of FRT**

FRT regulation continues to develop in most jurisdictions. This is due to two simultaneous developments: FRT's varied applications and the relevant national authority's regulatory tools. FRT concerns are usually governed by privacy legislation in each jurisdiction. Most jurisdictions lack a distinct FRT/AI law, except for the EU, which recently enacted a standalone AI regulatory proposal. Thus, studying AI/FRT regulation involves studying the laws and regulatory structures. FRT laws usually have three parts. First, they limit FRT's use. Second, they require written authorizations and court mind application before deployment. Third, they outline technology deployment safeguards. These include recordkeeping, human assessment, periodic assessment, and FRT openness.

The following cross-jurisdiction studies of FRT legislation can help you comprehend them. It will enable politicians using this handbook to apply relevant ideas to India.

**1. European Union**

The EU treats FRT legislation as an element of AI regulation. For the second case, the EU updates its rules to address AI issues rather than starting from scratch. [14] The General Data Protection Regulations (GDPR) and its Data Protection Directive control biometric data collection and processing. Additionally, the EU has suggested an AI Act with a risk-based compliance system. This proposed AI Act classifies FRT systems as “high risk” with the most stringent regulatory requirements.

**2. United Kingdom**

FRT deployment is regulated by UK data protection law. This incorporates the 2000 EU Charter of Fundamental Rights, 2018 Data Protection Act, and UK-GDPR. [15] The Court of Appeal banned live automated FRT in 2020. The Information Commissioner (ICO) then published an opinion on live FRT deployment in public spaces.

**3. United States**

FRT is regulated at the federal, state, and city levels in the US. Since FRT regulation rarely stands alone and pulls from existing laws, states have more thorough regulatory frameworks with privacy laws. Different FRT laws use prohibitions, time-bound or directive moratoriums, and regulation.

**4. Australia**

Australian privacy law, the Privacy Act, 1988, regulates FRT. FRT and AI are not regulated by law.42 The Office of the Australian Information Commissioner (OAIC) inquiry into law enforcement and private enterprises' FRT use regulated FRT in Australia. The Australian HRC is also formulating a FRT deployment regulation position.

**5. Canada**

Canada oversees FRT under data protection and privacy legislation. It currently has no FRT or AI law. The Privacy Act and PIPEDA are federal privacy laws.

**4. DIGI Yatra**

Digi Yatra (‘Digi Yatra’) (‘DY’) is a planned biometric boarding system (‘BBS or DY-BBS’) for Indian airports that will streamline, paperless, and contactless check-in and boarding. An authentication and authorization ecosystem for Indian airports can improve civil aviation infrastructure, digitise manual processes, boost security, and cut airport operating costs.

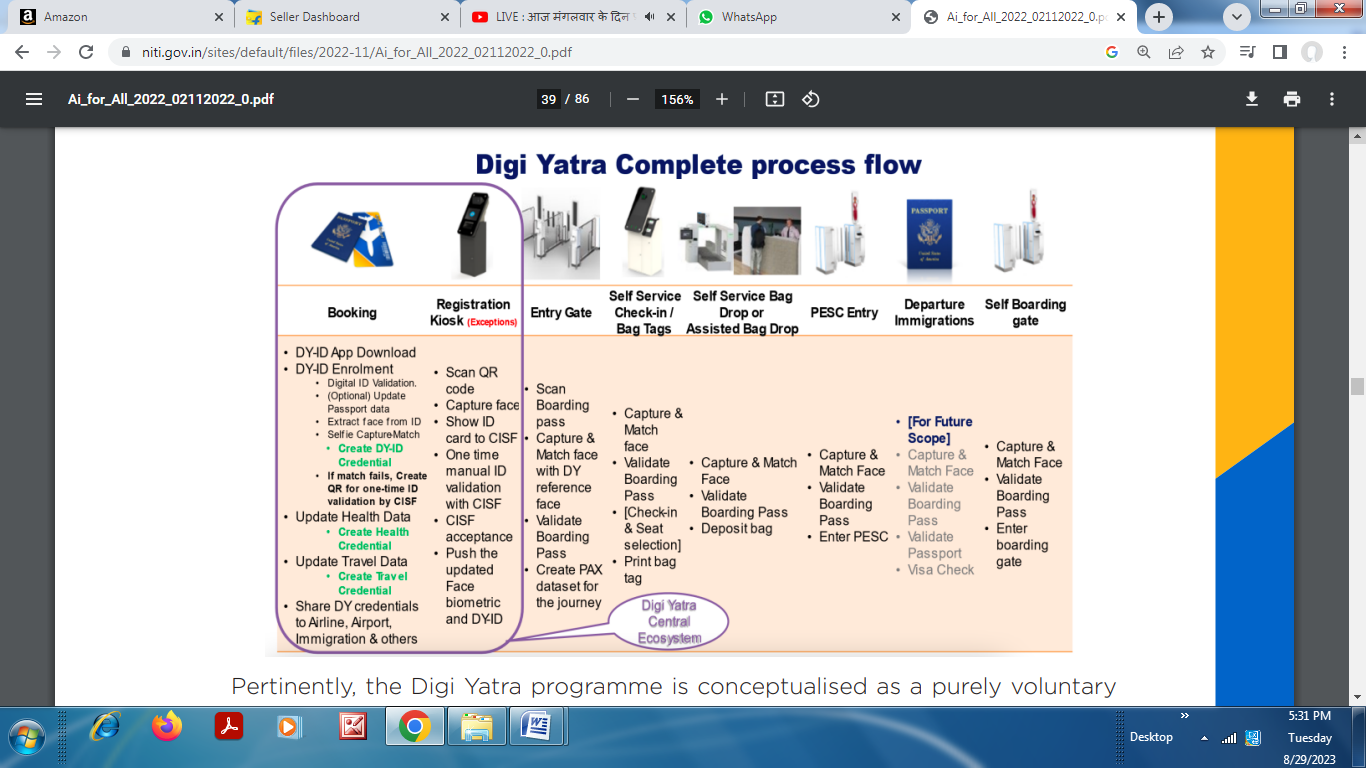
Digi Yatra suggests using FRT to confirm passengers' travel credentials, allowing additional airport checks to be automated with minimum human intervention. FRT could reduce bottlenecks at Indian airports thus help the civil aviation environment. FRT deployment must also be privacy-protecting, equitable, legally permissible, and consistent with RAI principles.

The Department of Civil Aviation created a Technical Working Group to plan Digi Yatra. In 2018, Digi Yatra released a policy outlining its passenger processes and technical features. The policy was later updated from Digi Yatra Central Identity Management Platform (DYCIMP) to Digi Yatra Central Ecosystem, a Distributed Ecosystem based on W3C standards, Self-Sovereign Identity (SSI), Verifiable Credentials (VCs), and Decentralised Identifiers with a Distributed Ledger trust layer. The Digi Yatra Foundation (‘DYF’), a Section 8 not-for-profit business under the Companies Act, 2013, was founded in 2019 to implement the Central Ecosystem.

**4.1 The Digi Yatra programme**

The Digi Yatra project proposes biometric boarding. In an airport, this involves two steps: passenger authentication and development of a digital identity, and subsequent verification at airport checkpoints. The standard airport passenger process incorporates both manual components. CISF employees at Indian airports verify identities, travel documents, etc. at entry gates. At following airport checkpoints, CISF and airline officials manually verify identity. An identity administration system can help reduce airport congestion and expenditures by supplementing human involvement. Automating identity verification at checkpoints might also give travellers a paperless, frictionless experience.

The Digi Yatra Core Ecosystem would enable biometric boarding system operation with modules. The Digi Yatra policies and procedures both national and global travel SOPs for the Digi Yatra Core Ecosystem. Passengers can understand Digi Yatra's operation from the subsequent schematic:



Source: Niti Aayog, 2019

The Digi Yatra initiatives are voluntary, so the Digi Yatra Policies specifies that CISF personnel at airports will continue to physically verify travel ID documents for passengers who do not opt-in. The existing Digi Yatra procedure will supplement human engagement at airports and may be expanded to all airports with legal frameworks.

**4.2 Potential benefits**

This section discusses the benefits of using FRT for identity verification. While there may be major benefits, two ideas must be carefully taken into account: first, the financial implications of this strategy must also be addressed, particularly in terms of its possible hazards and influence on citizen interests. [16] The following chapters analyze this from the perspective of Responsible AI; secondly, to obtain these benefits, the right operational and organisational procedures must be developed. [17] This is examined through systems failure analysis in the following chapters. Digi Yatra ecosystem benefits include:

**1. Lower congestion at airports**

* FRT authentication and verification at airports can reduce human-caused wait times and errors. The computerization of identity verification can reduce airport passenger process bottlenecks.
* Digi Yatra is a voluntary policy, so alternative check-in and boarding methods will continue, and human assistance may be needed if authentication or other FRT issues occur.

**2. Seamless, paperless and contactless passenger experience**

Digi Yatra eliminates the need to manually verify passengers' credentials at each level, simplifying the airport experience. This may give travelers a paperless, contactless experience. In Covid-19 or other future scenarios, contactless technologies in general aviation could render passenger travel safer by adopting health-risk-free operations. [18]

**3. Lower operational costs and enhanced civil aviation capabilities**

* Automating human efforts will cut operational expenses for airport operators, airlines, and state identification verification agencies. These lower airport operations expenses may benefit the Indian aviation industry.
* Increased automation will lower human errors and inefficiencies, improving airport passenger experiences. Lower congestion at airports will allow them to serve more passengers, improving civil aviation.

**4.3 Legal aspects of Digi Yatra**

Given the above, it may be prudent to consider Digi Yatra's legal issues, including data privacy, Aadhaar biometric verification, and information security.

**1. Data privacy**

* The Digi Yatra Policy calls for voluntary participation. A voluntary plan where passengers sign up and agree to utilise Digi Yatra for check-in and boarding is an optional agreement for temporary data collection, storage, and use, this agreement must adhere to current data privacy laws and regulations. IT Act, 2000, [19] and IT (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules, 2011 (‘SPDI Rules’) govern these rules. The Digi Yatra Foundation, which operated the Digi Yatra Central Ecosystem, is a ‘body corporate’ under the SPDI Rules because it was constituted under the Companies Act, 2013. Digi Yatra must follow SPDI guidelines.
* SPDI Rules define ‘biometric information’ as ‘sensitive personal data or information’. [20] Thus, such data must be protected more. Thus, Digi Yatra data acquisition must comply with SPDI Rule 5. [21]
* Looking ahead, the planned Personal Data Protection Bill (‘PDP Bill’) will provide data protection principles, norms, and standards. [22]

Data privacy issues may also arise:

* While the Digi Yatra Policy specifies that use is voluntary, any compelled use must conform with K.S. Puttaswamy v. Union of India's legality, necessity, and proportionality criteria. [23] The Digi Yatra Policy deletes facial biometrics from the local airport's database 24 hours following the passenger's flight. The Policy must clearly state how to delete other passenger data and face biometrics kept in other registries.
* The Digi Yatra Policy states that users may consent to value-added services at the airport, which may involve cab operators and other commercial companies sharing their data. Care must be taken to offer meaningful consent that is not bundled by default. This may demand ‘opt-in’ consent instead of ‘opt-out’. This would default to not sharing passenger data with third parties unless they opt-in. Opt-in mechanisms limit consent given without understanding the ramifications.

2. Aadhar-based verification

* The Digi Yatra Policy requires the Foundation to get an AUA licence under Section 4 of the Aadhaar Act, 2016 and regulations there under. [24]
* As an AUA, the Digi Yatra Foundation must comply with the Aadhaar Act, 2016 and its rules, including the Aadhaar (Authentication) rules, 2016, including user consent, data storage, log maintenance, and data security.

**5. Conclusion**

In 2019, India introduced the PDP Bill, which was removed this year. The government says this withdrawal is transitory and a new data security measure will be proposed in Parliament. FRT, like other clever algorithms, is data-intensive. To assure propriety and legality in data processing to train and build FRT systems, the country needs a codified safeguarding of data regime. The PDP Bill, 2019, must be retained in the new data protection bill, including obligations, enforcement procedures, a regulating agency, penalties, and remedies. Such a framework must also codify fundamental privacy safeguards against state agencies, including law enforcement, in addition to regulating private data processing. New data protection rules should protect sensitive personal data, including biometric data like facial photos and scans. To address privacy risks connected with FRT systems, any recommended data protection policy should address rigorous data processing, storage, and retention standards for sensitive biometric data.

**References**

[1] Niti Aayog, ‘National Strategy for Artificial Intelligence’ Discussion Paper (June 2018) accessed 10 August 2023

[2] Niti Aayog, ‘Approach Document for India Part 1 – Principles for Responsible AI’ (February 2021) accessed 10 August 2023

[3] World Economic Forum, ‘A Policy Framework for Responsible Limits on Facial Recognition: Use Case: Law Enforcement Investigations’ (October 2021) White Paper, pp. 26

[4] Niti Aayog, ‘Approach Document for India Part 1 – Principles for Responsible AI’ (February 2021) <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 10 August 2023

[5] Smriti Parsheera, ‘Adoption and regulation of facial recognition technologies in India: Why and why not?’ (August 2019) Data Governance Network, Working Paper 05

[6] Andrew W. Senior, Sharath Pankanti, ‘Privacy protection and face recognition’ in Stan Li, Anil Jain (eds), Handbook of Facial Recognition Technology (Ch. 3.1.1, Springer 2011)

[7] Shahina Anwarul, Susheela Dahiya, ‘A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy’ P. K. Singh et al. (eds) (2020) Proceedings of ICRIC 2019 <https://www.researchgate.net/publication/337446642\_A\_Comprehensive\_Review\_on\_Face\_ Recognition\_Methods\_and\_Factors\_Affecting\_Facial\_Recognition\_Accuracy> accessed 18 December 2021

[8] Priya Vedavalli et al, ‘Facial Recognition Technology in Law Enforcement in India: Concerns and Solutions’ (2021) Data Governance Network, Working Paper 16

[9] Major Cities Chiefs Association, ‘Facial Recognition Technology in Modern Policing: Recommendations and Considerations’ (2021) Facial Recognition Working Group, <https://majorcitieschiefs.com/wp-content/uploads/2021/10/MCCA-FRT-in-Modern-Policing-Final.pdf> accessed 18 December 2021

[10] Blerim Rexha et al, ‘Increasing Trustworthiness of Face Authentication in Mobile Devices by Modeling Gesture Behavior and Location Using Neural Networks’ (2018) 10(2) Future Internet <https://www.mdpi.com/1999-5903/10/2/17/htm> accessed 15 December 2021

[11] PTI, ‘Biometric data of 99 cr Indians collected: Govt’ (New Delhi, 6 September 2016) The Hindu <https://www.thehindu.com/news/national/aadhar-bill-biometric-data-of-99-cr-indians-collected-govt/article8341976.ece> accessed 18 August 2023

[12] Tom Simonite, ‘Your Instagram #Dogs and #Cats Are Training Facebook’s AI’ (2 May 2018) WIRED <https://www.wired.com/story/your-instagram-dogs-and-cats-are-training- facebooks-ai/> accessed 10 August 2023

[13] Varsha Bansal, ‘The Hyderabad Model of CCTV Surveillance’ (10 August 2020) Livemint <https://www.livemint.com/news/india/the-hyderabad-model-of-cctv-surveillance-11604926158442.html> accessed 20 August 2023

[14] European Commission, On Artificial Intelligence - A European approach to excellence and trust (COM(2020) 65) <https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020\_en.pdf> accessed 16 August 2023

[15] The UK-GDPR is the domestic retention of the GDPR, 2016 which ceased to apply post Brexit.

[16] NITI Aayog, ‘Approach Document for India Part 1 – Principles for Responsible AI ’ (February 2021) Responsible AI <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 20 August 2023

[17] NITI Aayog, ‘Approach Document for India: Part 2 - Operationalizing Principles for Responsible AI ’ (August 2021) Responsible AI <https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf> accessed 20 August 2023

[18] PTI, ‘Mumbai airport rolls out contactless check-in system for passengers’ (8 September 2020) Business Standard <https://www.business-standard.com/article/current-affairs/mumbai-airport-rolls-out-contactless-check-in-system-for-passengers-120090801106\_1.html> accessed 2 August 2023

[19] S. 43, Information Technology Act, 2000

[20] Rule 3, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (‘SPDI Rules’)

[21] Rule 5, SPDI Rules

[22] ‘A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians’ (2018) Committee of Experts under the Chairmanship of Justice Srikrishna

[23] Justice KS Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, Part S, para 180

[24] Sec 4, Aadhaar Act, 2016

1. Author: Dr. Mohd. Asad Malik, Professor, Jamia Millia Islamia, New Delhi

   [↑](#footnote-ref-1)
2. Co-Author: Ms. Hina ILiyas, Research Scholar, Jamia Millia Islamia, New Delhi [↑](#footnote-ref-2)