Page 828 - 846

DOI: *https://doij.org/10.10000/IJLSI.111987*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 3

2024

© 2024 International Journal of Legal Science and Innovation

Follow this and additional works at: https://www.ijlsi.com/

Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com)

This Article is brought to you for free and open access by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in International Journal of Legal Science and Innovation after due review.

In case of **any suggestion or complaint**, please contact **Gyan@vidhiaagaz.com.**

To submit your Manuscript for Publication at **International Journal of Legal Science and Innovation**, kindly email your Manuscript at **editor.ijlsi@gmail.com.**

Biometric Facial Recognition Technology through the Lens of Right to Privacy

VENKITESH M.J.[1]

ABSTRACT

This study explores the implications of biometric facial recognition technology (FRT) on the right to privacy, particularly in the context of India and the UK. FRT, a sophisticated biometric technology used for identifying and verifying individuals based on their facial features, has seen a rapid increase in deployment across various sectors including law enforcement, security, and public services. While FRT offers numerous benefits such as enhanced security and streamlined services, it raises significant privacy concerns due to its potential for mass surveillance and data misuse.

The research delves into the historical evolution of FRT, from its early manual classification systems in the 1960s to the advanced automated systems in use today. It highlights the extensive adoption of FRT in Western countries for security purposes and contrasts this with the situation in India, where the lack of comprehensive data protection laws exacerbates privacy risks. The study also examines the legal frameworks governing FRT in India and the UK, with a focus on the implications of landmark judicial decisions such as the Puttaswamy case in India and the Bridges case in the UK.

In India, the widespread use of FRT without adequate legal safeguards poses serious threats to individual privacy and civil liberties. The Information Technology (Amendment) Act 2008 and the Personal Data Protection Bill 2019 are analyzed to understand their adequacy in addressing these concerns. The research emphasizes the need for robust regulatory frameworks to ensure that the deployment of FRT does not infringe on fundamental rights.

In the UK, the use of FRT by law enforcement agencies is scrutinized through the lens of the Bridges case, which underscores the necessity for clear legislative mandates and transparency in the use of such intrusive technologies. The study advocates for balanced policies that protect individual rights while leveraging the benefits of FRT for public safety. Ultimately, this research highlights the complex interplay between technological advancement and privacy rights, urging for comprehensive and adaptable legal frameworks to govern the use of FRT in both India and the UK. It calls for greater public awareness, informed consent, and stringent data protection measures to mitigate the risks associated with this powerful technology.

[1] Author is a LL.M. student in India.

I. Introduction

Facial Recognition Technology (FRT) is a method of verifying or establishing a person's identity by analysing their facial features. These systems utilize images or videos to identify individuals, often in real time. It falls under the category of biometric data, specifically considered as 'special category personal data' in data protection regulations, requiring cautious handling. While predominantly employed in security and law enforcement, there is an increasing curiosity about its applications in different sectors like education, transportation, and public spaces by governmental bodies.[2] The FRT is significantly advanced when compared to other biometric-based technologies. The application of this technology to boost public and private safety will only develop and grow.

(A) Background and Content

FRT was first used in the middle of the 1960s when scientist Woodrow Wilson Bledsoe created a system that could manually classify pictures of faces. Although the system was straightforward, it provided the foundation for the creation of systems that were more complex. More automated systems started to emerge in the 1970s, including one created by Goldstein, Harmon, and Lesk that could recognise 21 distinct subjective facial characteristics, including hair colour and lip thickness.[3] With Kirby and Sirovich's breakthrough in 1988 that effectively recognised faces using principal component analysis, FRT continued to advance throughout the 1980s and 1990s.[4] The technology had advanced to the point that it could be employed in more useful applications by the 1990s' conclusion, most notably in surveillance and security systems.

Today FRT is already pervasive and has application in a wide range of fields. It is utilised in social networking, police enforcement, immigration, and even disease control, as demonstrated by the use of it during the COVID-19 epidemic to identify people even when they were wearing masks.[5] As a biometric technology, it offers the potential for tailored user experiences across a variety of industries, making it extremely adaptable and significant. The face recognition method is one of the few biometric methods that offers both high accuracy and low

[2] Faizah Patel and Zena Stephenson, 'Through the "Eyes" of the ICO: Facial Recognition Technology (FRT) in the Public Sector' (*Sharpe Pritchard*23 February 2023)

[3] Goldstein, A., Harmon, L., & Lesk, A. (1971). Identification of human faces. Proceedings of the IEEE, 59(5), 748-760.

[4] Kirby, M., & Sirovich, L. (1990). Application of the Karhunen-Loeve procedure for the characterization of human faces. IEEE Transactions on Pattern Analysis and Machine Intelligence.

[5] Walid Hariri, 'Efficient Masked Face Recognition Method during the COVID-19 Pandemic' [2021] National Library of Medicine.

intrusiveness.[6]. The approach is as accurate as an approach based on physiological principles without being intrusive.

Police and corporations use facial recognition technology in Western countries. It identifies, verifies, and searches individuals through a facial database. The technique measures facial features and creates a mathematical faceprint. The system compares the image with the database and displays the corresponding image.

The utilisation of FRT raises apprehensions regarding privacy, consent, and surveillance. Critics argue that its application by government or law enforcement bodies may infringe upon privacy and result in a surveillance state reminiscent of Orwell. The use of FRT also poses ethical concerns regarding consent. Do individuals consent to having their faces scanned and stored when entering public spaces? This technology may encroach upon privacy and cause stress, leading people to engage in self-censorship and undermining freedom of speech and expression, particularly if sensitive information such as biometrics is collected and exploited for unexpected purposes. Additionally, the accountability for individuals who use the data to make judgements may be lowered by the ongoing collecting of photographs and data using facial recognition technologies by governmental and commercial organisations.[7] Similar to fingerprint and DNA profiles, the FRT generates unalterable data and images; as a result, particular care and thought should be provided to safeguard the privacy of the data.[8]

Many common law nations lack specific laws regarding data protection and privacy, including those related to biometric technologies like FRT. This results in inadequate legal systems that do not adequately address privacy rights violations or provide compensation for victims in civil cases. The UK Data Protection Act, 2018 was used as a model for data protection legislation due to its comprehensiveness and currency among common law countries. Since the UK was a member of the EU, its data protection law was amended in accordance with the EU General Data Protection Regulation 2018.[9]

Facial Recognition Technology is utilised in various sectors in India such as law enforcement, surveillance, immigration, and consumer technology. The lack of knowledge among Indian

[6] Nurul Azma Abdullah and others, ‘Face Recognition for Criminal Identification: An Implementation of Principal Component Analysis for Face Recognition’ (2017) 1891 AIP conference proceedings.

[7] Snyder, E., 2018. Faceprints and the fourth amendment: how the fbi uses facial recognition technology to conduct unlawful searches, Syracuse Law Rev.

[8] Jawahitha Sarabdeen, ‘Protection of the Rights of the Individual When Using Facial Recognition Technology’ (2022) 8 Heliyon <https://www.sciencedirect.com/science/article/pii/S2405844022003747> accessed 18 August 2023.

[9] Jawahitha Sarabdeen, ‘Protection of the rights of the individual when using facial recognition technology’, (2022)

residents about how widely FRT is utilised and how it may affect their privacy is a serious concern.[10] Informed permission is disregarded when using FRT, resulting in uncertainty regarding its usage, storage, and sharing. The current legal framework for FRT application in India is inadequate, and a balance must be struck between technology growth and individual privacy rights.

(B) Policy Transferability:

A comparative study can help discern if certain policies or regulations from one country are transferable to another, or how they might be adapted to fit different contexts.

The intersection of facial recognition technology and the right to privacy is a complex and evolving issue that has garnered significant attention and debate.

Facial recognition can be used for mass surveillance, enabling governments and private entities to track and monitor individuals in public spaces without their knowledge or consent.The use of facial recognition often involves the collection and storage of biometric data, raising concerns about the potential misuse or unauthorised access to this sensitive information.Facial recognition technology is not perfect and can sometimes produce inaccurate results. This may lead to false identifications and consequences for innocent individuals.There have been concerns about the bias in facial recognition algorithms, especially when it comes to race and gender. If the training data used to develop these systems is not diverse, the technology may exhibit discriminatory behavior.Governments may use facial recognition for law enforcement purposes, such as identifying and tracking individuals in public spaces. Critics argue that this can infringe on citizens' civil liberties and rights to privacy.Some jurisdictions have implemented or are considering legislation to regulate the use of facial recognition technology. These regulations may set limits on its application, establish safeguards, and define how collected data should be handled.In certain places, there have been calls for outright bans on the use of facial recognition technology due to the perceived risks and concerns.Many argue that individuals should have the right to be informed when facial recognition technology is in use, and they should be able to give or withhold consent for their data to be processed.There is a push for greater transparency in the development and deployment of facial recognition systems, including disclosing how the technology works and its potential impacts.The debate often involves finding a balance between national security concerns and protecting individual rights to privacy.

[10] Kay L Ritchie and others, 'Public Attitudes towards the Use of Automatic Facial Recognition Technology in Criminal Justice Systems around the World' (2021) 16 PLOS ONE.

Striking the right balance is challenging but crucial.As technology continues to advance, the ethical and legal considerations surrounding facial recognition and privacy are likely to evolve. It is important for societies to engage in open discussions, involve stakeholders, and establish frameworks that protect individual rights while addressing security needs.The Indian government has implemented facial recognition technology in various areas, including law enforcement and security. For example, it has been used in airports for identity verification and security purposes.The Aadhaar system, India's biometric identification program, primarily relies on fingerprints and iris scans. However, there have been discussions about incorporating facial recognition as an additional authentication method. The use of facial recognition with Aadhaar has raised concerns about privacy and security.Some Indian law enforcement agencies have adopted facial recognition technology for surveillance and criminal identification. This includes the deployment of facial recognition systems in public spaces and at major events.Facial recognition is being explored and implemented in smart city projects across India. It is used for purposes such as traffic management, public safety, and improving the efficiency of public services.The use of facial recognition technology in India has faced criticism from privacy advocates and civil liberties groups. Concerns have been raised about the potential for mass surveillance, data security, and the lack of a comprehensive legal framework to govern its use.As of my last update, there were discussions about the need for regulatory frameworks to govern the use of facial recognition technology. It's essential to monitor any developments in this regard, as regulations can play a crucial role in safeguarding individual privacy.Beyond government use, facial recognition technology has found applications in various industries, including banking, retail, and healthcare, for tasks such as customer authentication and personalised services.

II. Right to privacy

In 2017, the Supreme Court of India, in the landmark case of Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, recognized the right to privacy as a fundamental right under the Indian Constitution. This decision may have implications for cases related to the use of facial recognition technology.

(A) Aadhaar Case:

While not specifically about facial recognition, the Aadhaar case (decided by the Supreme Court in 2018) had significant implications for biometric data. The court imposed restrictions on the use of Aadhaar for authentication purposes and emphasized the need for data protection.

(B) Data Protection Bill:

The Personal Data Protection Bill, 2019, which was introduced in the Indian Parliament, addresses issues related to the processing of personal data, including biometric data. The Bill proposes a comprehensive framework for the protection of personal data and includes provisions related to consent, data localization, and the handling of sensitive personal data.

Privacy advocates and civil liberties groups have raised concerns about the use of facial recognition technology for surveillance purposes without proper safeguards. Legal challenges could emerge if such uses are perceived as infringing on the right to privacy.

(C) Increasing uses of Facial Recognition System in both private and government sectors

The usage of facial recognition systems has recorded a tremendous rise over the past few years globally. Nowadays, most mobile applications are secured with the aid of a facial recognition system. Users are required to authenticate such mobile applications through a facial recognition system before operating them. The major usage of a facial recognition system is either to identify or verify the user. Additionally, facial recognition systems are adopted in major private businesses such as the hospitality industry is employing facial recognition systems to enhance customer service, while luxury apartment buildings are using them to do away with the need for occupants to carry keys11. Airlines are also utilising it to speed up boarding. Facial recognition is used by many internet businesses as a component of their services or features. Google, Apple, and Facebook use face recognition technology to help identify people in photos. The largest image database on the globe is probably found on Facebook.

III. LEGAL LANDSCAPE OF FACIAL RECOGNITION TECHNOLOGY IN INDIA AND THE UK

(A) Introduction

the impact of Puttaswamy case on the Personal Data Protection Bill (PDPB) in India. It also analyzes the influence of the GDPR and the Data Protection Act 2018 in the UK on the creation of Indian PDPB 2019.

Lack of Opt-out: Citizens had limited choices. If one wanted to receive certain government benefits or services, enrolling in Aadhaar became almost compulsory[12]

[11] 'Human Rights and Law in the Age of Artificial Intelligence', (Abacademies.org, September 2022) <*https://www.abacademies.org/articles/human-rights-and-law-in-the-age-of-artificial-intelligence-12420.html*> accessed 22nd September 2022

[12] Vanya Rakesh, 'Aadhaar Act and Its Non-Compliance with Data Protection Law in India — the Centre for

The above concerns culminated in the Justice K.S. Puttaswamy (Retd.) vs. Union of India case[13]. The constitutionality of Aadhaar was challenged by petitioners due to its infringement upon privacy rights. The Supreme Court upheld the validity of Aadhaar while recognizing privacy as a fundamental right, but certain provisions were struck down. This decision limited the expansion of Aadhaar and made its linkage voluntary for many services, establishing privacy as an undeniable right for Indian citizens. The Privacy Data Protection Bill 2019 of India is based on these developments.

(B) The Personal Data Protection Bill 2019 and adopting the GDPR

a. Privacy protections

Drawing inspiration from the GDPR, India's Personal Data Protection Bill introduces rigorous data management guidelines. By proposing the establishment of a Data Protection Authority, it seeks to ensure corporate accountability. Mandates, such as having dedicated data protection officers and compelling foreign firms to maintain local contacts, signal a proactive stance. Yet, while its "privacy by design" principle is commendable, the Bill's effectiveness hinges on the balance between safeguarding user data and potentially burdening businesses with frequent compliance checks[14]

b. The Legal Landscape of Facial Recognition Technology in India

Facial Recognition Technology (FRT) has emerged as a revolutionary tool in India with implications spanning from security enhancement to convenience in daily life. However, its widespread adoption has ignited a profound discussion around the legal framework governing its use, particularly in terms of individual privacy and civil liberties. This essay delves into the legal landscape of FRT in India, scrutinizing the existing laws, regulations, and judicial precedents that shape its deployment and impact. As FRT becomes an integral part of various sectors, it is crucial to understand how Indian law addresses the complex interplay between technological advancement and individual rights, ensuring a balance between security imperatives and personal freedoms.

c. The Information Technology (Amendment) Act 2008

The Information Technology (Amendment) Act 2008 provides a somewhat nebulous foundation for the use of facial recognition technology (FRT) in India. One must question

Internet and Society' (cis-india.org14 April 2016) <https://cis-india.org/internet-governance/blog/aadhaar-act-and-its-non-compliance-with-data-protection-law-in-india#:~:text=Purpose%20Limitation&text=Section%2029%20of%20the%20Act> accessed 18 August 2023.

[13] Justice KS Puttaswamy(Retd) v Union of India The Supreme Court of India (2017) 10 SCC 1 547

[14] ibid

whether a generic piece of legislation like the IT Act can cater to the nuanced requirements of FRT.

The Act defines data as a "structured representation of facts, knowledge, or instructions meant for processing in computer systems or networks."[15] This data can exist in variousformats[16] like computer printouts, magnetic storage, optical media, or even within a computer's memory. Information, on the other hand, encompasses elements like data, text, images, voice, software, and even databases[17] The inclusivity of these definitions suggests that the state is equipped to monitor contemporary computer systems and compile a database from the gathered data[18] However, any such surveillance and data compilation must adhere to the constraints mentioned in Section 69B (8), particularly concerning how long records can be retained.Drawing from the Act, data and information definitions are vast, including everything from messages to sound to computer programs. .The state, in its ambition to use the latest technology, could argue that FRT is just another form of surveillance under this Act, but is this a reasonable stretch? When the Act mentions activities like interception and decryption, facial recognition doesn't naturally fit into those categories.

The Puttaswamy case, an essential legal touchstone, states that any infringement on privacy needs a clear legislative mandate. The IT Act might be seen as this mandate, but it's a stretch. If FRT isn't merely 'interception, decryption, or monitoring', then relying on the IT Act as a justification becomes shaky ground.[19]

The embryonic stage of India in creating an FRT regulatory matrix prompts apprehensions regarding accountability, governance, and remedial avenues. This void is exacerbated by an unclear policy direction. The UK, with established supervisory bodies such as the Information Commissioner's Office (ICO) and the Biometric and Surveillance Camera Commissioner, ostensibly offers a more organized oversight mechanism. However, genuine concerns loom about their actual potency, breadth, and the intricacies of regulating private FRT deployments.

i. Use of FRT in law enforcement in India.

In September 2020, the Election Commission of Telangana, a State in India, initiated a trial run

[15] Information Technology (Amendment) Act, 2008

[16] Elonnai Hickok and others, 'Facial Recognition Technology in India — the Centre for Internet and Society' (cis- india.org31 August 2021) <https://cis-india.org/internet-governance/blog/hrbdt-and-cis-august-31-2021-facial- recognition-technology-in-india> accessed 20 July 2023.

[17] Information Technology (Amendment) Act, 2008

[18] ibid, 2008

[19] Elonnai Hickok and others, 'Facial Recognition Technology in India — the Centre for Internet and Society' (cis- india.org31 August 2021)

of facial recognition software during the Greater Hyderabad Municipal Corporation elections,[20] deploying it in a single polling location within each of the 150 sectors[21] Since 2019, Hyderabad's airport has been leveraging facial recognition technology (FRT)[22] Furthermore, the Telangana law enforcement uses FRT to match a suspect with the Crime and Criminal Tracking Network and System (CCTNS) records[23] Also during the COVID-19 pandemic, the Telangana Police have employed AI-driven systems, including CCTV and FRT, to identify individuals not wearing masks[24] Telangana is not the only state that uses FRT in law enforcement in India,various governmental agencies and police departments around the country started to use FRT because it elevates "efficiency, transparency and accountability in the entire process"[25] For example, in Chennai, the technology is employed to pinpoint individuals appearing suspicious; in Delhi, it's utilized to recognize frequent protesters; while in Punjab, it aids in real-time intelligence collection[26]

These actions may infringe on individuals' rights to free speech, expression, and assembly, serving as a means of social control.

ii. Use of FRT in law enforcement in The UK

The trajectory of FRT in the UK, from its inception in CCTV systems in the 1950s to its current sophisticated integration, offers a panorama of technological advancement interfacing with civil liberties[27]. The expansion of this technology raises pivotal questions about the delicate

[20] Moulika K V and Sagar Kumar Mutha, 'TSEC Set to Use Face Recognition App in Civic Polls despite Concerns over Privacy' The Times of India (21 September 2020) <https://timesofindia.indiatimes.com/city/hyderabad/tsec-set-to-use-face-recognition-app-in-civic-polls-despite-concerns-over-privacy/articleshow/78224182.cms> accessed 6 September 2023.

[21] The Hindu, 'Telangana Tests Facial Recognition in Local Polls as Privacy Fears Mount' The Hindu (22 January 2020) <https://www.thehindu.com/sci-tech/technology/telangana-tests-facial-recognition-in-local-polls-as-privacy-fears-mount/article30623453.ece> accessed 6 September 2023.

[22] Sudipta Sengupta, 'Hyderabad Airport Pilots Face Recognition for Entry' The Times of India (2 July 2019) <https://timesofindia.indiatimes.com/city/hyderabad/face-it-entry-into-airport-just-got-hi-tech-for-fliers-from-city/articleshow/70032153.cms> accessed 6 September 2023.

[23] Venkat Ananth, 'In Tech-Driven Telangana, the Eyes Have It' The Economic Times (16 March 2020) <https://economictimes.indiatimes.com/technology/in-tech-driven-telangana-the-eyes-have-it/articleshow/74644565.cms> accessed 17 August 2023.

[24] Aneesha Bedi, 'Geo-Mapping, CCTV Cameras, AI — How Telangana Police Is Using Tech to Enforce Covid Safety' (ThePrint2 June 2020) <https://theprint.in/india/geo-mapping-cctv-cameras-ai-how-telangana-police-is-using-tech-to- enforce-covid-safety/433856/> accessed 17 August 2023; Vrinda Bhandari, 'Facial Recognition: Why We Should Worry about the Use of Big Tech for Law Enforcement' [2020] SSRN Electronic Journal.

[25] 'Centre for Communication Governance, with Support from the Friedrich Naumann Foundation for Freedom (FNF)' (2021) <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/the-future-of-democracy-in-the-shadow-of-big-and-emerging-tech-249.pdf> accessed 18 August 2023.

[26] Jay Mazoomdaar, 'Delhi Police Film Protests, Run Its Images through Face Recognition Software to Screen Crowd' (The Indian Express28 December 2019) <https://indianexpress.com/article/india/police-film-protests-run-its-images- through-face-recognition-software-to-screen-crowd-6188246/> accessed 16 August 2023.

[27] Giulia Gentile, 'Does Big Brother Exist? Face Recognition Technology in the United Kingdom' [2023] SSRN Electronic Journal

balance between the state's interest in public safety and individuals' right to privacy.

Historically, London pioneered the use of surveillance cameras, positioning itself as a global leader in adopting CCTV technology for public safety. The first use of the CCTV system adopted in the UK was during the Queen’s Coronation in 1953[28] With evolving technology, these cameras were eventually fortified with FRT, enabling real- time identification against vast law enforcement databases. Critics argue that FRT enhances security, streamlines investigations, and fosters a sense of public safety. The Metropolitan Police[29] and the College of Policing's[30] endorsement reflects this stance, pointing to its potential in bolstering the war against crime. The UK government identifies four core objectives behind the deployment of CCTV: crime detection and emergency response, investigation and evidential purposes, active monitoring of suspects, and deterring criminal activities. Historically, there have been doubts about the tangible impact of CCTV on crime reduction. Notably, a 2009 study by London’s Metropolitan Police highlighted that merely one in 1,000 cameras played a direct role in solving a crime[31] Recent findings by the MET police emphasize the significant role of FRT in enhancing the efficiency of manhunts. It's been noted that high-profile manhunts, especially for grave crimes like murder, demand extensive resources, both in terms of personnel and time. Cumulatively, such operations consume thousands of hours in London alone[32] Yet, a comparison with recent trials of Live Facial Recognition (LFR) reveals its potential: four LFR trials led to eight arrests[33]

Furthermore, LFR enables police officers to swiftly interact with individuals who might be on their wanted list. Comparing the effectiveness of LFR with traditional 'stop and search' techniques, a 2020 MET report indicated that while 13.3% of traditional stops culminated in an arrest, an impressive 30% of LFR-triggered engagements did so after a validated system alert[34]

[28] Philip Chertoff, ‘Facial Recognition Has Its Eye on the U.K.’ (Default7 February 2020)

[29] MET Police, ‘Facial Recognition Technology guidance’, <https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition-technology/> assessed on 18 August 2023

[30] college of policing, ‘Live Facial Recognition Technology Guidance Published’ (College of Policing22 March 2022) <https://www.college.police.uk/article/live-facial-recognition-technology-guidance-published> accessed 18 August 2023.

[31] Parliamentary office of Science and Technology, ‘Postnote CCTV’ (April 2002), <https://www.parliament.uk/globalassets/documents/post/pn175.pdf> , assessed on 17 August 2023

[32] National Physical Laboratory, Metropolitan Police Service, ‘Metropolitan Police Service Live Facial Recognition Trials’, (February 2020) <https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing- information/facial-recognition/met-evaluation-report.pdf>, assessed on 17 August 2023;

[33] Giulia Gentile, ‘Does Big Brother Exist? Face Recognition Technology in the United Kingdom’ [2023]

[34] Giulia Gentile, ‘Does Big Brother Exist? Face Recognition Technology in the United Kingdom’ [2023]

IV. THE BRIDGES CASE

The Bridges case, centered around the deployment of Automated Facial Recognition (AFR) Locate by South Wales Police, serves as a litmus test for the alignment of advanced surveillance technologies with established human rights norms. Edward Bridges, supported by NGO Liberty, challenged this technology, arguing that it infringes upon the European Convention on Human Rights' Article 8 – the right to privacy[35]

Despite the Divisional court's initial endorsement, viewing the Police and Criminal Evidence Act 1984 as a sufficient regulatory shield, the Court of Appeal provided a counternarrative. They deemed such a framework unsatisfactory for a technology as intrusive as AFR. The court's apprehension emanated from two pivotal concerns: the ambiguous criteria underpinning watchlist selections ("who") and the obscurity surrounding the technology's operational domains ("where"). Moreover, the court flagged the problematic persistence of data, particularly for individuals who weren't identified as matches.

A more granular analysis of the ruling indicates the court's scrupulous assessment of the proportionality principle in the context of AFR. While acknowledging SWP's grounding in legal norms, the court argued that their interpretation of Article 8(2) ECHR wasn't sufficiently robust to address AFR's inherent intrusiveness. Additionally, the court underscored the imperativeness of an unbiased FRT mechanism, hinting at larger questions of racial and gender justice[36]

Crucially, while the judgment illuminated regulatory blind spots, it concurrently underscores the pressing need for comprehensive FRT legislation in the UK, advocating for a framework that dovetails technological prowess with human rights safeguards.

Facial Recognition Technology (FRT) has established a distinct position in the law enforcement structures of India and the UK, citing improved crime-solving abilities. However, its integration has raised significant ethical, legal, and societal predicaments.

India's approach to FRT, characterized by its extensive use and limited oversight, is a cause for concern. Such comprehensive surveillance confers significant authority to the state, potentially suppressing dissenting opinions and undermining core democratic principles. While the technology's benefits, such as aiding in investigations and enhancing public safety, are evident, they are counterbalanced by significant threats to personal freedom. The absence of an all-inclusive regulatory framework in India intensifies the vulnerabilities associated with

[35] ibid

[36] ibid

misidentification and privacy breaches, in addition to posing threats to democracy.

Conversely, the UK's long-standing surveillance culture presents a nuanced perspective. The Bridges case brought attention to the need for rigorous FRT guidelines. The judiciary's position emphasized the importance of explicit legislative support and delineated operational standards, with a broad emphasis on protecting citizens' privacy and ensuring equal treatment.

Both India and the UK, although operating under different socio-political contexts, share a common predicament: navigating the delicate balance between utilizing FRT for public safety and preserving individual rights. In the absence of strict regulations, public accountability, and transparency, FRT's potential as a tool of dominance overshadows its benefits. As these nations progress further into the digital sphere, it is crucial to ensure that technology does not undermine democratic principles. A well-regulated, purposeful approach to FRT is essential to maximize its capabilities while safeguarding individual rights.

(A) The digital data protection Act 2023, whether FRT should be used even agaisnt the privacy of persons in the interest of public.

The Digital data protection act 2023 is a very recent legislation and the ramifications it might have on the privacy of persons in the interest of public has to be analysed. As I have mentioned in the earlier chapters India had several laws and Acts that indirectly connected to “Digital data or Automated data” that involves Facial Recognition Technology(FRT), but all these Acts never directly implied any laws or regulations that manages the definitions, grounds for processing digital personal data, rights and duties of data principal, establishment of a board for data protection, or penalties and redressal methods. But India on 11 August 2023 notified in the Official Gazette the Digital Personal Data Protection Act (DPDA) 2023[37]. The DPDA Act lays the foundation for India's updated data protection system, but it will only be active once the Central Government releases the corresponding rules. Additionally, a Data Protection Board of India will be set up as a judicial entity, empowered to identify violations of the DPDP Act or its rules and enforce penalties[38]. The DPDP (Data Protection and Digital Privacy) law imposes comprehensive responsibilities.

It establishes specific and limited legal grounds for processing any personal data in digital form. It also introduces obligations related to limiting the purposes of data usage, including a

[37] The Digital Personal Data Protection Act 2023 <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf> accessed 16 August 2023

[38] Deepa Christopher, Anindita Dutta and Aanchal Kabra, ‘India – the Digital Personal Data Protection Act, 2023 Finally Arrives’ (www.linklaters.com23 August 2023) <https://www.linklaters.com/en/insights/blogs/digilinks/2023/august/india- the-digital-personal-data-protection-act> accessed 27 August 2023.

requirement to delete the data once its intended purpose is fulfilled. Interestingly, the law offers limited flexibility for utilizing personal data for ancillary objectives. It grants a series of rights to individuals regarding their personal data that's being gathered and processed. These rights include being notified, accessing their data, and the ability to request data deletion. Additionally, the legislation establishes a supervisory entity, the Data Protection Board of India, with the jurisdiction to delve into grievances and levy penalties. However, this agency does not possess the authority to offer advice or set rules[39]

The activation of the DPDP Act is dependent on the government's notification of an effective date. In contrast to the GDPR, there is no set transitional period in the DPDP Act and the government has the power to determine when the Act's sections take effect.This includes the sections related to the establishment of the new governing body responsible for ensuring adherence to the law[40]

(B) DPDP Act and General Data Protection Regulation (GDPR)

The DPDP Act is established on fundamental principles, which are comparable to those found in the GDPR[41] This categorizes its primary participants as data fiduciaries, processors, and data principals. Unlike the GDPR's extensive protective coverage, the DPDP Act confines its extent to personal data that identifies a data principal, regardless of whether it is sourced digitally or transformed from physical records. It is noteworthy that the DPDP excludes personal data utilized for personal or household matters and aggregated data for research, which potentially creates loopholes in protection. The Act does not safeguard data willingly disclosed by individuals, in contrast to the GDPR. The territorial boundaries of the Act mirror the GDPR[42], and it encompasses data activities within India and those abroad linked to services or goods offered in India. Nevertheless, it arguably falls short of global reach by not encompassing overseas entities monitoring Indian data principals' behaviors, thus potentially limiting its efficacy against international data breaches.

The DPDP Act differs from the GDPR by avoiding the latter's nuanced approach of identifying a "special data category of personal data" for increased scrutiny. Rather, the DPDP implements a universal approach, treating all digital personal data equally without additional safeguards, even for sensitive or critical data. Arguably, this lack of specificity in the DPDP might streamline operations but could potentially compromise the heightened protections certain

[39] ibid

[40] ibid

[41] Deepa Christopher, Anindita Dutta and Aanchal Kabra, 'India – the Digital Personal Data Protection Act, 2023 Finally Arrives' (www.linklaters.com23 August 2023)

[42] ibid

sensitive data categories warrant, a crucial aspect embraced by the GDPR.

The DPDP Act seeks to usher in a holistic paradigm for personal data management[43] superseding the rather piecemeal provisions of the IT Act. While the latter narrowly catered to select data types like health, the DPDP broadens the scope, encompassing all data discernible to an individual. Though it resonates with GDPR's broad- based "identifiability" standard, it interestingly bypasses the categorization of sensitive data, banking solely on the digitization criterion.

The Act introduces "data principal,"[44] analogous to GDPR's "data subject,"[45] symbolizing individuals whose data is being processed. Its counterpart, "data fiduciary,"[46] equivalent to GDPR's "data controller," governs the processing methodology. Notably, the Act cryptically alludes to joint fiduciary arrangements, leaving room for ambiguity.

A critical oversight in the Act is its blanket approach to defining fiduciaries. The statement lacks subtlety as it fails to differentiate between public and private entities and individuals and corporations. This overarching classification could pose challenges, as it lumps diverse entities under a single umbrella, potentially overlooking the unique risks and responsibilities each poses. Such a generalized perspective might necessitate future clarifications or revisions to ensure precision and efficacy.

1. Consent

The DPDP Act, while echoing the GDPR's principle that data processing requires a lawful basis, appears notably restrictive in its approach. By confining data fiduciaries to only two legal grounds - the unequivocal "consent" and the ambiguously termed "legitimate use,"[47] the Act risks oversimplifying a complex issue. GDPR's broader framework, offering six lawful grounds, provides entities with flexibility, recognizing the multifaceted nature of data processing in today's digital age. The DPDP Act's emphasis on "consent" may inadvertently lead to reduced transparency. For instance, data fiduciaries might forgo providing notices or entertaining correction and erasure requests when they pivot to the "legitimate use" ground, leaving data principals potentially uninformed and vulnerable. The Act's lack of detailed definitions further exacerbates these concerns[48]

[43] Digital Personal Data Protection Act 2023, s(t)

[44] Digital Personal Data Protection Act 2023, s2(j)

[45] Raktima Roy and Gabriela Zanfir Fortuna, 'The Digital Personal Data Protection Act of India, Explained - Future of Privacy Forum'

[46] Digital Personal Data protection Act 2023, s2(i)

[47] ibid, s4

[48] Raktima Roy and Gabriela Zanfir Fortuna, 'The Digital Personal Data Protection Act of India, Explained -

International data transfers.

The DPDP Act's focus on "digital personal data" within Indian territory sets a clear jurisdiction, yet the inclusivity of the term "data principal" sans residency or citizenship requirements broadens its reach[49] This implies that India-centric entities, while catering to foreign nationals, could inadvertently fall within the Act's purview, potentially complicating international transactions and collaborations.

2. Rights and Duties of data principal

The DPDP Act's provision for data subjects[50] while comprehensive, still falls short when compared to the GDPR in terms of data portability – a significant gap given its potential for enhancing consumer control. Although its limited use in the EU might justify this absence, it doesn't eliminate the benefits it could bring in promoting data subject autonomy[51]

However, the DPDP's introduction of a clear "grievance redressal"[52] right, backed by an established contact point, offers a proactive approach, empowering individuals to voice concerns. Additionally, the unique " appoint a nominee"[53] right showcases a forward-thinking perspective, acknowledging the eventualities of life. While both

GDPR and DPDP strive for data protection, the balance between rights, responsibilities, and feasibility remains a nuanced debate.

(C) Indian constitutional aspects

The Indian Constitution guarantees fundamental rights to its citizens, encompassing civil, political, economic, and social rights. The judiciary in India has played a crucial role in expanding the scope of human rights through judicial interpretations, recognizing un-enumerated rights like the "right to live with human dignity" and facilitating public interest litigation to protect the rights of vulnerable sections of society[54]

1. Data protection Board

The DPDP Act heralds the inception of an independent "Board" designed to be the primary

Future of Privacy Forum' (https://fpf.org/15 2023)

[49] Digital personal data protection Act 2023, s2(j)

[50] ibid, s11

[51] Deepa Christopher, Anindita Dutta and Aanchal Kabra, 'India – the Digital Personal Data Protection Act, 2023 Finally Arrives' (www.linklaters.com23 August 2023)

[52] Digital personal data protection Act 2023, s13

[53] ibid, s14

[54] IJLMH, 'Development of Human Rights Jurisprudence in India: An International Perspective' (International Journal of Law Management & Humanities9 September 2020) <https://ijlmh.com/development-of-human-rights-jurisprudence-in-india-an-international-perspective/> accessed 17 May 2024.

enforcement mechanism[55] It's structured with a Chairperson at its helm and members appointed by the Government, all serving a renewable two-year term. While this promises a streamlined complaint redressal system, post the exhaustion of internal grievance channels, the short tenure raises questions about continuity and consistent policy enforcement.

The Board's expansive powers mirror civil court authority but curiously limit access to these very courts for data protection remedies. This decision parallels Article 82 of the GDPR, funnelling appeals to the Telecom Disputes Settlement and Appellate Tribunal instead. The financial penalties, varying significantly from a mere USD $120 to a staggering $30.2 million, depend wholly on the Board's discretion, potentially causing inconsistencies[56]

Perhaps the most controversial aspect is the Central Government's extended oversight[57] Its ability to demand information and even enforce public information blocks, with the Board's sanction, treads into the domain of online platform regulation, rather than classic data privacy, which may raise concerns about overreach and the genuine independence of the Board.

Several legal frameworks are discussed that are used in different countries to make facial recognition with the help of AI technologies. Most of the laws are against managing basic human rights. Therefore, ***ethical and legal security frameworks*** need to be included in most of the existing legal Frameworks[58]. Hence, ***the International Centre for Not-for-Profit Law*** (ICNL) is discussed in the research. Such a law needs to enforce the law against ***data breaches*** and ***lack of informed consent***. Hence, in some cases, ***inefficient legal support*** for digital data privacy and face recognition are noticed which needs to be developed among the existing legal frameworks. Thereafter, the "***Universal Declaration on Human Rights***" is also discussed which has focused on the inviolable rights of the human being and the obligations of the international community. Such rights need to ***include the ethical rights of human being***s and the importance of their consent before getting access to personal data. Some changes are required in the "***American Human Rights Law***" as they do not focus on the facial recognition law so deeply. The law needs to focus on the facts of the "***Biometric Technology Moratorium Act of 2021***" as it speaks about protecting children, and students, by avoiding bias during face detection. Hence, all the legal bodies need to focus on the "local law enforcement entities" to develop the existing human rights laws. Nonetheless, human rights acts or laws need to ***focus on the illegal issues*** that the human being of that country may face while doing facial

[55] ibid, s18
[56] ibid, s33
[57]ibid, s36
[58] Geeksforgeeks.org, (2020). *Face recognition using Artificial Intelligence*. https://www.geeksforgeeks.org/face-recognition-using-artificial-intelligence/

recognition.

It can be analysed that some other changes are required in the present legal frameworks such as a ***committee that needs to be developed*** to monitor the legal activities of the digital media and enforce effective laws[59]. All the laws need to ***mention rules against different types of violations*** so that people feel protected through facial detection[60]. Moreover, most of the legal framework includes punishment against data breaches and unethical behaviour but there are a few regulations that focus on inaccurate systems. Hence, the legal frameworks need to create a ***law against using inaccurate systems by the organisation*** to make facial detection. In some cases, it has been noticed that people are killed due to ***the misidentification of victims***. Hence, the legal bodies need to be concerned about such matters so that organisations can make a proper identification of victims and any mishaps do not occur. Thereafter, laws against financial fraud through facial detection age are quite noticeable in most of the regulations but the legal framework needs to focus on ***differential error rates*** during facial detection. A change to the "***Canadian Human Rights Act "*** needs to be brought based on the ***freedom of digital data protection***. It can help the Canadian people to feel protected while they are using digital platforms, web cameras, and other software on a daily basis. Moreover, above mentioned minor changes need to be done to the existing legal frameworks to maintain proper face identification with the incorporation of AI technology.

2. Penalties

The Data Privacy and Protection Act (DPDP) presents a stark contrast to the GDPR in terms of penalty assessment. Instead of gauging the turnover of the offending entity, as GDPR does, the DPDP Act levies flat-rate penalties ranging from INR 50 crores to 250 crores[61] One could argue that such a model potentially overlooks the scale and financial magnitude of the erring organizations. Whereas the GDPR's turnover-based approach could be viewed as ensuring equitable punishment proportionate to an organization's size, the DPDP's structure might unfairly burden smaller entities while providing a mere slap on the wrist for larger corporations.

Moreover, while the DPDP considers each offence for penalties, it caps it at the maximum penalty for the most severe offence, possibly downplaying cumulative breaches. However, the Act does offer a structured approach in evaluating penalties, focusing on the breach's nature,

[59] Kaspersky, (2018). *How does facial recognition work?* https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition

[60] Markey.senate.gov, (2022). IN THE SENATE OF THE UNITED STATES. https://www.markey.senate.gov/download/facial-recognition-and-biometric-technology-moratorium-act

[61] Digital Personal Data Protection Act 2023, s33

affected data type, financial ramifications, and mitigation efforts[62] This ensures a degree of tailored punitive actions but might fall short of achieving the deterrence desired in larger organizations.

The DPDP Act, 2023 can be considered a major legal milestone in the protection of digital data in India. Public and private parties should start to consider how to follow the obligations of the DPDP Act. As the GDPR is a major inspiration they can start from that; still India’s DPDP Act and some of its requirements are different compared with GDPR. The DPDP Act 2023 is a direct statute that can deal with privacy and legal issues related to FRT. Even though the act does not fully acknowledge the legal issues of digital data, it can still be considered as a short term relief until other amendments and major developments are introduced.

The facts that to be taken note of is the DPDP Act will only be in effect when the government of India provides an effective date. If things do not work in the progress direction, India would still be stuck with the Privacy Data Protection BIll 2019.

The DPDP Act carries significant ramifications for the public interest. Nonetheless, certain aspects of the Act's structure and execution have faced criticism due to specific provisions that could potentially diminish its advantages if not executed meticulously. One area of concern is the composition and operation of the Data Protection Board, which has sparked apprehensions regarding its autonomy and neutrality.In conclusion, the DPDP Act of 2023 plays a vital role as a legislative measure aimed at safeguarding personal privacy and advancing public welfare in the era of digitalization. The Act contains various clauses that bolster data security; however, its execution and efficacy hinge upon the interpretation and enforcement of these clauses. Ensuring a harmonious implementation of the Act that reconciles individual privacy rights with public welfare imperatives is imperative for cultivating a more secure and reliable digital sphere.

V. Conclusion

The evolution of data privacy regulations in India, exemplified by the landmark Justice K.S. Puttaswamy (Retd.) vs. Union of India case. The subsequent Personal Data Protection Bill (PDPB) 2019 embodies the nation's commitment to data rights, while unique adaptations reflect the Indian context. While the PDPB aligns with international norms, it navigates the challenge of ensuring digital privacy amid a rapidly transforming digital landscape. The efficacy of the PDPB hinges on its implementation and businesses' adaptability.

[62] ibid, s33(2)

the DPDP Act, 2023, as a notable stride in India's data protection journey. While drawing inspiration from GDPR, it adapts to India's unique circumstances. The act provides a vital framework for FRT-related legal issues, acting as a solution while awaiting further amendments. However, the act's effectiveness hinges on its implementation and the government's provision of an effective date. If not executed well, India may remain tethered to the Privacy Data Protection Bill 2019, underscoring the urgency of regulatory advancements.

the collective findings emphasize the paramount importance of a harmonious synergy between technological innovation, legal frameworks, and individual rights. While FRT holds immense potential for societal benefits, its unregulated proliferation can infringe on privacy and democratic values. Both India and the UK stand at a juncture where striking this equilibrium is vital. Robust regulatory mechanisms that align with.

*****