International Research Journal of Multidisciplinary Scope (IRJMS), 2025; 6(1):407-423 IRJMS

Review Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2025.v06i01.02025

GDPR Safeguards for Facial Recognition Technology: A Critical Analysis

Peter I Gasiokwu, Ufuoma Garvin Oyibodoro*, Michael O Ifeanyi Nwabuoku

Faculty of Law, Delta State University, Oleh Campus, Nigeria. *Corresponding Author's Email: garvinesuire@gmail.com

Abstract

The application of Face Recognition Technology (FRT) in various sectors has raised significant concerns regarding privacy and data protection, especially in the context of the General Data Protection Regulation (GDPR) 2018 (EU) 2016/679. This article critically evaluates the procedural safeguards mandated by the GDPR for the deployment of FRT. Adopting a doctrinal approach, it examines the adequacy of existing regulations in addressing the unique challenges posed by FRT, such as the risks of mass surveillance, data breaches, and biased algorithms. Through a comprehensive analysis of the GDPR's provisions, including legal justification for processing, data minimization, and the rights of data subjects, this study identifies gaps and proposes enhancements to guarantee robust protection of individual rights. The findings underscore the need for stricter enforcement mechanisms and the development of specific guidelines tailored to the nuances of FRT.

Keywords: Data Protection, Facial Recognition Technology, GDPR, Privacy, Procedural Safeguards.

Introduction

FRT has rapidly evolved into a critical tool in various domains, including security, law enforcement, marketing, and even social networking. This technology is often heralded as a breakthrough in enhancing security and efficiency because it uses sophisticated algorithms to detect and authenticate people based just on their face features. However, as FRT becomes more pervasive, it brings with it profound implications for data protection and privacy, especially within the European Union (EU), where the GDPR (EU) 2016/679 sets stringent standards for processing personal data. To generate a unique face signature that can be distinguished to a database of previously saved images, FRT analyses face traits such as the space between the eyes, the contour of the lips, and the curve of the cheekbones. The technology's accuracy and reliability have improved significantly with advances in machine learning and artificial intelligence, leading to its widespread adoption across various sectors. For example, FRT is used in airports for security screening, by law enforcement agencies to identify suspects, in retail for customer tracking, and even in social media platforms for automatic tagging of photos (1). Despite these advancements, the deployment of FRT has sparked a global debate about its implications for privacy and civil liberties. Specifically, the GDPR's fundamental rights are seriously threatened by FRT's ability to obtain and use biometric data without individuals' express consent. Biometric data, within the GDPR by virtue of Article 9, is classified as a "special category" of personal data, requiring heightened safeguards due to its sensitive nature. The regulation states that it is generally forbidden to process this kind of data unless certain requirements are satisfied, like obtaining the data subject's express consent or confirming that the processing is necessary for significant importance to the public. The GDPR was implemented in May 2018 with the aim of standardizing data protection regulations throughout the EU and granting individuals more autonomy over their personal information. It is among the most complete frameworks for data protection globally, with provisions that are particularly relevant to the deployment of FRT. The GDPR's Article 5(1) requires that data processing operations, including those requiring FRT, be conducted in a manner that data subjects can easily understand and backed by a valid legal basis. This is consistent with the principles of lawfulness, fairness, and transparency.

(Received 15th August 2024; Accepted 13th January 2025; Published 31st January 2025)

Data controllers needs to put in place the necessary organizational and technological security measures to ensure the confidentiality of personal information, including biometric data, in accordance with GDPR Article 32. This provision elevates the standards for deploying FRT within the EU. The rapid proliferation of FRT begs important concerns associated with the suitability of existing legal frameworks in mitigating the privacy hazards linked to this technology. Although the GDPR offers a strong basis for data protection, its application to FRT is fraught with challenges. The possibility that FRT may make mass surveillance possible, violating people's right to privacy and data protection, is one of the main worries. For example, Law enforcement's application of FRT has been particularly controversial, with critics claiming that it could result in a society where people are continuously watched without their knowledge or consent (2). Furthermore, there have been doubts raised about the accuracy of FRT, especially in light of its potential for bias and discrimination. Research has demonstrated FRT systems can show significant differences in accuracy between different demographic categories, particularly when it comes to gender and race. Commercial FRT systems, for instance, were less accurate in detecting women and people with darker skin tones, according to research by Buolamwini and Gebru (3). This finding raises concerns about the possibility that these technologies would reinforce already-existing social disparities. The principles of non-discrimination and fairness are emphasized in Recital 71 of the GDPR and are critical in evaluating the implementation of FRT. According to these guidelines, data processing operations cannot produce results that are biased. Another challenge lies in the transparency of FRT systems. According to GDPR Article 13, individuals with regard to their personal data must be notified about its processing, including its aims and legal basis. However, the complex nature of FRT, combined with its often-covert deployment, makes individuals find it difficult to completely understand when and how their biometric data is being captured and processed. This lack of transparency undermines the GDPR’s goal of enabling people to take charge of their own data. The research challenge, therefore, centers on critically assessing whether the GDPR’s procedural safeguards are sufficient to address the unique risks posed by FRT. Key questions arise regarding the regulation’s capacity to mitigate threats such as mass surveillance, algorithmic bias, and data breaches, as well as its effectiveness in ensuring transparency, fairness, and accountability. This study aims to evaluate the adequacy of the GDPR’s legal framework in safeguarding individual rights amidst the rapid advancements in FRT. By identifying gaps in the current safeguards and proposing targeted enhancements, this research seeks to contribute to the broader discourse on balancing innovation with privacy rights in the digital age. This study aims to provide a critical evaluation of the procedural safeguards mandated by the GDPR for the implementation of FRT. The focus is on assessing the effectiveness of these safeguards in mitigating the privacy and data protection risks associated with FRT. By closely analysing the GDPR's requirements and provisions, the study seeks to determine whether the current legal framework adequately addresses the unique challenges posed by FRT and to identify potential gaps that may need to be addressed through regulatory or legislative reform.

Methodology

The methodological approach adopted for this study is doctrinal, focusing on a detailed examination of legal provisions and their application. This study employs a qualitative framework, structured around three core analytical stages: legal analysis, comparative evaluation, and critical appraisal.

Legal Analysis: The initial step entailed a thorough examination of the GDPR provisions pertinent to facial recognition technology (FRT). Key provisions analysed included those on lawful processing, data minimization, and data subject rights. This analysis was guided by established legal interpretation principles, emphasizing the text, context, and purpose of the GDPR to evaluate its alignment with the specific challenges posed by FRT.

Comparative Evaluation: The comparative study reveals disparities in FRT compliance, with commercial systems often breaching GDPR consent and transparency standards, open-source systems lacking accountability, and experimental systems failing to meet security measures.

Compared to GDPR, BIPA mandates explicit consent and provides a private right of action but is geographically limited, while PIPEDA aligns on transparency but lacks strong biometric safeguards. GDPR's comprehensive framework remains a leader, though enforcement gaps highlight the need for tailored improvements.

Critical Appraisal: The critical evaluation focused on identifying gaps or inadequacies in the existing regulatory framework, particularly concerning mass surveillance, biased algorithms, and data breaches. This stage employed a problem-based approach, critiquing the practical application of GDPR provisions and their sufficiency in addressing ethical and legal concerns associated with FRT. Recommendations for enhancements to GDPR provisions or additional guidelines tailored specifically to FRT were developed using criteria of legal coherence, practical feasibility, and adaptability.

Synthesis of Findings: The insights from the legal analysis, comparative study, and critical evaluation were synthesized to form a comprehensive view of GDPR's effectiveness in regulating FRT. This synthesis integrated legal theory with practical considerations, ensuring the findings and recommendations are grounded in both scholarly analysis and real-world applicability.

Materials: The primary materials used in this study include a range of legal and regulatory documents and scholarly literature. The GDPR 2018 (EU) 2016/679 was central to the analysis, providing the legal framework governing the use of FRT. This regulation includes key provisions related to lawful processing, data minimization, and the rights of individuals. Alongside the GDPR itself, guidance and best practice documents from the European Data Protection Board (EDPB) as well as numerous national data protection authorities were reviewed to gain insights into how the GDPR's obligations for biometric data are actually put to use.

Overview of FRT

Definition and Functionality

FRT is categorized as a biometric technology that uses patterns based on a person's facial features to analyse and verify identity (4). At its core, FRT functions by taking a picture of a person's face, either in real-time or from a photograph or video, and then converting this image into a digital model, commonly known as a facial template. This template is a mathematical model of the individual's unique distinct facial features, including the distance between the eyes, the nose's structure, and the jaw's contour (5). The process of facial recognition typically involves several key steps: detection, alignment, feature extraction, and matching. In the detection phase, the system identifies the presence of a face within an image or video frame. During alignment, the system normalizes the detected face by adjusting it for pose, size, and orientation to maintain consistency across several photos. Feature extraction involves isolating the unique features of the face, such as texture, geometry, and landmarks, which are then encoded into a facial template. Finally, the matching process compares the facial template against a database of stored templates to ascertain the individual's identify or verify their claimed identity (6). FRT systems can operate in two primary modes: verification (1:1 matching) and identification (1 matching). Verification entails contrasting a person's facial template with a single saved template, such as when a person uses facial recognition to unlock a smartphone. Identification, on the other hand, involves comparing the facial template to a database of multiple templates, such as in law enforcement applications where a suspect's face is matched against a database of known offenders. The versatility of FRT in both verification and identification scenarios has contributed to its widespread adoption across various sectors.

Key Applications and Industries

Due to its ability to boost security, expedite processes, and enhance user experiences, FRT has found employment in a variety of industries. Some of the most prominent applications of FRT include:

Law Enforcement and Security: One of the earliest and most well-known applications of FRT is in law enforcement and security. Police forces around the world use FRT to track individuals of interest, identify suspects, and keep an eye out for any threats in public areas. For example, FRT has been deployed in major cities such as London and New York for surveillance purposes, where it is used to scan crowds for individuals on watch lists (7). Additionally, FRT is increasingly used in border control and airport security, where it facilitates the rapid and accurate identification of travellers, enhancing security while reducing the need for manual checks (8).

Retail and Marketing: In the retail sector, FRT is being used to personalize customer experiences and enhance security. Retailers deploy FRT to identify repeat customers, analyse shopping behaviour, and tailor marketing strategies to individual preferences. For example, some stores use FRT to recognize loyal customers as they enter and offer personalized discounts or product recommendations based on their previous purchases. Additionally, FRT is used in anti-theft measures, where it helps to identify known shoplifters and prevent retail crime.

Banking and Financial Services: The financial sector has also embraced FRT for its ability to enhance security and streamline customer verification processes. Banks and financial institutions use FRT for identity verification in online banking, where customers can authenticate transactions or access accounts by scanning their faces (9). This application of FRT reduces the risk of fraud and identity theft, providing a more secure and convenient alternative to traditional methods of authentication, such as passwords or PINs.

Healthcare: In the healthcare industry, FRT is being utilized to enhance patient care and streamline administrative processes. Hospitals and clinics use FRT to verify patient identities, ensuring that medical records are accurately matched to the correct individual. This technology is also used in telemedicine, where it facilitates secure remote consultations by verifying the identity of both patients and healthcare providers (10). Additionally, FRT is being explored for its potential in monitoring patients' emotional and physical states, offering insights that could enhance personalized care.

Social Media and Entertainment: These platforms have integrated FRT into their services to enhance user experiences and improve content management. For instance, platforms like Facebook admitted using FRT to automatically tag individuals in photos, making it easier for users to organize and share images (11). In the entertainment industry, FRT is employed in gaming and virtual reality applications to create more immersive and personalized experiences.

Current Trends and Developments

The development of FRT is characterized by rapid advancements in technology and expanding use cases, driven by improvements in machine learning, artificial intelligence, and big data analytics. One of the most significant trends in FRT is the shift towards deep learning algorithms, which have dramatically increased the precision the effectiveness of facial recognition systems. Convolutional neural networks (CNNs) are an example of a deep learning model that can process vast volumes of data and identify intricate patterns in facial features, enabling FRT systems to achieve near-human levels of recognition accuracy (12). Another notable trend is the increasing integration of FRT in conjunction with additional biometric technology, including iris scanning and fingerprint identification, to create multi-modal biometric systems. These systems offer enhanced security and accuracy by combining multiple biometric modalities, reducing the likelihood of false positives or negatives. For example, multi-modal systems are being explored for use in national identification programs and secure access control in sensitive facilities (13). The expansion of FRT into new applications is also a key trend. Beyond traditional uses in security and identification, FRT is being adapted for use in areas such as emotion detection, age estimation, and health monitoring. These new applications are being driven by advances in computer vision and affective computing, which allow FRT systems to interpret subtle facial cues and expressions. For instance, emotion detection systems using FRT are being developed for use in customer service, where they can assess customer satisfaction in real-time, or in education, where they can monitor student engagement and emotional well-being (14). However, the swift advancement and widespread use of FRT have sparked considerable ethical and legal issues, specifically relating to privacy, consent, and bias. FRT has drawn criticism for its potential to violate civil liberties and contribute to the establishment of a surveillance state when it comes to its application in law enforcement and monitoring (15). Additionally, the issue of algorithmic bias in FRT systems has garnered considerable attention, with research highlighting disparities in recognition accuracy across different demographic groups (16). These concerns have prompted calls for greater transparency, accountability, and regulation in the deployment of FRT. In response to these concerns, several governments and organizations have begun to put into effect the rules and regulations controlling the usage of FRT. For example, processing biometric data, such as facial images, must adhere to the guidelines outlined in GDPR Article 9. This processing must be transparent and need specific consent. Similarly, in the United States, several cities and states have enacted or proposed legislation to ban or restrict the use of FRT by law enforcement agencies and private companies (17). These regulatory developments reflect a growing recognition of the need to strike a balance between the privacy and individual rights protection and the advantages of FRT.

Results and Discussion

GDPR Framework and its Application to FRT

Core Principles of the GDPR

At its core, the GDPR is founded on numerous important guidelines that control how personal data is processed. The foundations of the regulation is formed by these principles and are particularly relevant when applied to emerging technologies like FRT, which processes sensitive biometric data.

Lawfulness, Fairness, and Transparency: Under Article 6 of the GDPR, personal data must be processed in a lawful, fair, and transparent manner. As outlined in Article 6(1) of the GDPR, data processing must adhere to the principle of lawfulness by depending on one of the approved legal bases, such the data subject's consent, the fulfilment of a contract, or the data controller's lawful interests. Fairness dictates that personal information must never be used in a way that is unjust, misleading, or detrimental to the data subject. As stipulated by GDPR Article 12(1), transparency obliges data controllers to provide clear and accessible information to data subjects about how their data is being processed, including the purposes, legal basis, and any third parties involved. These principles are particularly crucial in the context of FRT, where the potential for covert data collection and processing poses significant risks to individuals' privacy and autonomy.

Purpose Limitation: This principle, as outlined in Article 5(1)(b) of the GDPR, mandates that personal data cannot be treated in a way that is inconsistent with its intended uses and may only be collected for defined, explicit, and legal purposes. This principle is intended to prevent data controllers from repurposing data in ways that could infringe on the rights and expectations of data subjects. In the context of FRT, this means that biometric data collected for one purpose, such as security screening, cannot be repurposed for unrelated activities, such as marketing or profiling, for example—without the data subject's express consent.

Data Minimization: According to GDPR Article 5(1)(c), this principle mandates that personal data be acquired in a way that is adequate, relevant, and restricted to what is necessary for the purposes for which it is processed. This principle aims to limit the amount of personal data collected to the minimum necessary to achieve the intended purpose, thereby reducing the risk of misuse or unauthorized access. In the context of FRT, data minimization is particularly relevant, as the collection of biometric data inherently involves the processing of sensitive information that could have significant implications for privacy if mishandled (18).

Accuracy: Article 5(1)(d) of the GDPR states that personal data must be accurate and, where necessary, kept up to date. Data controllers are required to take all reasonable steps to ensure that any inaccurate data is promptly corrected or deleted. This principle is critical in the deployment of FRT, where inaccuracies in facial recognition algorithms can lead to false positives or negatives, potentially resulting in significant harm to individuals, such as wrongful arrests or denial of services.

Storage Limitation: Article 5(1)(e) of the GDPR, requires that personal data be retained in a form that allows the identification of data subjects for no longer than is necessary for the purposes for which the data is processed. This principle requires data controllers to establish clear retention periods for the data they collect and to ensure that data is securely deleted or anonymized once it is no longer needed. In the context of FRT, this means that biometric data should not be stored indefinitely, and retention periods should be strictly defined and justified.

Integrity and Confidentiality: This principle is stipulated in Article 5(1)(f) of the GDPR, requires that personal data be processed in a manner that ensures appropriate security. This includes protection against unauthorized or unlawful processing, accidental loss, destruction, or damage, through the use of suitable technical and organizational measures. This principle is particularly pertinent to FRT, where the sensitivity of biometric data necessitates robust security measures to protect against breaches, hacking, and other forms of data compromise.

Accountability: Article 5(2) of the GDPR, imposes the responsibility on data controllers to demonstrate compliance with all other data protection principles. It requires them to implement measures that ensure and verify adherence to these principles. This principle underscores the importance of a proactive approach to data protection, requiring organizations to document their data processing activities, conduct regular audits, and establish internal policies and procedures that uphold GDPR standards. In the context of FRT, accountability is key to ensuring that the deployment of the technology is both legally compliant and ethically sound.

Lawful Basis for Processing FRT Data

The GDPR outlines several lawful bases for processing personal data, one of which must be satisfied for any data processing activity to be considered lawful. The lawful bases that are most pertinent to the processing of FRT data are consent, contract fulfillment, and legal compliance, protecting essential interests, carrying out official duties or serving the public interest, and pursuing legitimate interests.

Consent: The requirement for explicit consent as a legitimate justification for processing biometric data under the GDPR is outlined in Article 9(2)(a). This provision specifically applies to the handling of specific types of personal data, including biometric data, where express consent has been granted by the data subject. To be valid, such consent must be freely given, explicit and unequivocal, providing the ability for data subjects to revoke their permission at any time. In practice, obtaining valid consent for FRT can be challenging, particularly in situations where individuals may not be fully aware of the technology's deployment or its implications. For example, in public spaces where FRT is used for surveillance, it may be difficult to obtain meaningful consent from individuals who are unaware that their faces are being scanned and processed (19).

Legitimate Interests: Another acceptable justification for processing could be the data controller's or a third party's legitimate interests as described in Article 6(1)(f) of the GDPR, provided that the data subjects' liberties and rights do not conflict with these interests. In the context of FRT, legitimate interests might include security and fraud prevention, where the deployment of the technology can be justified as necessary to protect property or individuals (20). The requirement for conducting a careful balancing of interests when relying on legitimate interests as a lawful basis for processing is found in Recital 47 of the GDPR. This recital emphasizes that data controllers must consider the data subject’s reasonable expectations, the relationship between the data subject and the data controller, and the potential impact on the data subject's rights and freedoms.

Public Interest and Official Authority: Processing carried out in the public interest or in the exercise of official authority is another potential lawful basis for using FRT, particularly within the framework of law enforcement or public safety. Article 6(1)(e) of the GDPR specifies this premise. For example, law enforcement agencies may use FRT in order to identify suspects or preventing criminal activity, provided that such processing is appropriate and vital in relation to the objectives pursued (21). However, the use of FRT in this context raises significant ethical and legal concerns, particularly regarding the potential for mass surveillance and the infringement of civil liberties.

Special Categories of Data: Biometric information handled with the intention of uniquely identifying a person is protected under the GDPR is classified as a special category of personal data, which is subject to additional safeguards as outlined in Article 9(1). The processing of such data is generally prohibited unless one of the specific conditions outlined in Article 9(2) is met, such as obtaining explicit consent, processing for substantial public interest, or processing for the establishment, exercise, or defence of legal claims. These additional safeguards reflect the delicate quality of biometric data and the heightened dangers connected to its processing.

Data Minimization and Purpose Limitation

The principles of data minimization and purpose limitation are central to the GDPR's framework for safeguarding personal data, particularly in the context of technologies like FRT, where the potential for excessive data collection and misuse is significant.

Data Minimization: The GDPR's data minimization principle, as specified in Article 5(1)(c), mandates that personal data collected must be adequate, relevant, and limited to what is necessary for the intended purposes. In the context of FRT, this means that data controllers ought to only gather the biometric information required for that particular purpose, whether it be security, identity verification, or another legitimate purpose. For example, if FRT is deployed for access control to a secure facility, the system should only collect and process facial images that are directly relevant to verifying individuals' identities and should not capture additional data that is unrelated to this purpose. The goal of this principle is to stop the over-collection of data, which could increase the possibility of exploitation or illegal access.

Purpose Limitation: In accordance with Article 5(1) (b) of the GDPR, personal data must be acquired for specific, explicit, and lawful purposes and cannot be used in a way that is inconsistent with those purposes. This principle is critical in guaranteeing that personal data, once obtained, is not repurposed for activities that the data subject did not consent to or that could infringe on their rights. Regarding FRT, this indicates that biometric data obtained for one purpose, such as identification in a security context, should not be used for unrelated purposes, such as marketing or behavioural profiling, without obtaining additional consent from the data subject. The principles of data minimization and purpose limitation are intended to restrict the scope and duration of data processing activities, thereby minimizing the risk of privacy violations and ensuring that personal data is used transparently and in a manner that respects individual rights. These principles are especially crucial in the context of FRT, where there is a significant potential for data to be repurposed in ways that were not originally intended or understood by the data subject.

Procedural Safeguards under GDPR for FRT

Data Protection Impact Assessments (DPIAs)

The GDPR mandates that Data Protection Impact Assessments (DPIAs) be conducted in situations where data processing is likely to result in a high risk to the rights and freedoms of individuals, as specified in Article 35(1). Given the sensitive nature of biometric data, which includes facial recognition data, and the potential for significant privacy risks, DPIAs are particularly crucial in the deployment of FRT. The primary purpose of a DPIA is to systematically analyse, identify, and mitigate the risks associated with data processing activities. For organizations planning to implement FRT, conducting a DPIA, as mandated by Article 35 of the GDPR, is not only a regulatory obligation but also a crucial step in ensuring that the deployment of such technology adheres to the principles of data protection by 'design and by default,' as outlined in Article 25. A comprehensive DPIA for FRT should include several key components. First, it must provide a comprehensive explanation of the activities involved in processing, such as its type, extent, context, and purpose. This involves specifying how FRT will be used, the categories of data which can be obtained, including the justification for using biometric data. For instance, in a law enforcement context, a DPIA might assess the application of FRT for monitoring in real-time and the implications for individual privacy rights, particularly regarding the potential for mass surveillance. Second, the DPIA must assess the processing's need and appropriateness in light of its intended goals. This requires a careful evaluation of whether using FRT is required in order to achieve the stated objectives and whether less intrusive alternatives could be used instead. For example, a DPIA might explore whether the security objectives of an organization could be achieved through less invasive means, such as manual identification checks, before resorting to FRT. Third, the DPIA must identify and assess the dangers to data subjects' liberties and rights. In the context of FRT, these risks may include unauthorized access to biometric data, the potential for data breaches, inaccuracies in algorithms for facial recognition, as well as the implications of false positives or negatives. Additionally, the DPIA should consider the risk of bias and discrimination, particularly given the well-documented concerns about the differential accuracy of FRT across different demographic groups. The assessment should also address the potential for the technology to be used in ways that could infringe on individuals' rights, such as surveillance without consent or profiling based on facial characteristics. Finally, the DPIA must outline the measures and safeguards that will be implemented to mitigate identified risks. Technical protections like encryption and anonymization, together with organizational ones like staff training, frequent audits, and access limits, could be included. For instance, an organization deploying FRT might implement strong encryption protocols to protect stored facial templates and restrict this data's access to authorized personnel only. Additionally, the organization might establish a process for regularly reviewing the effectiveness of these safeguards and updating them in response to new risks or technological developments. Additionally, according to GDPR Article 36(1), if a DPIA shows that processing would put a considerable risk that cannot be lessened; the data controller ought to consult with the appropriate Data Protection Authority (DPA) before completing the processing. This consultation process ensures that potential privacy risks are thoroughly assessed and addressed before the deployment of FRT, providing an additional layer of oversight and accountability

Transparency and Accountability

The GDPR places a strong emphasis on accountability and transparency. According to Articles 12 and 5(2), respectively, organizations must show that they are in compliance with their data protection obligations and give data subjects' clear and accessible information about how their data is being processed. In the context of FRT, ensuring transparency involves informing individuals about the deployment of facial recognition systems, the purposes for which their biometric data will be used, and the rights they have concerning their data. This is particularly important given the often-covert nature of FRT, where individuals may be unaware that their facial data is being collected and processed. To achieve transparency, organizations have to give data subjects' comprehensive privacy notices that detail the use of FRT. As stated in Articles 12 and 13 of the GDPR, these notices should contain information on the legal justification for processing, the categories of data gathered, the objectives of processing, and the privacy rights of data subjects, including the ability to access, correct, and erase their data. These notices ought to be composed in simple, unambiguous language, and made readily available to individuals, for example, through signage when the data was being collected or on the organization's website. In addition to being required by law, transparency helps to build confidence amongst the data controller and data subjects. Given the intrusive nature of FRT, where the technology can capture and process personal data without an individual's active participation, ensuring that data subjects are fully informed is critical to upholding their autonomy and rights under the GDPR. For instance, in public spaces where FRT is used, clear signage indicating the presence of facial recognition systems and providing information on data processing practices is necessary to guarantee that individuals are aware that there is surveillance and their associated rights. This approach aligns with the transparency obligations under Article 12 of the GDPR. Article 5(2) of the GDPR establishes accountability, which puts the onus of proving adherence to data protection principles on data controllers. This entails putting in place strong data security safeguards, carrying out frequent audits, and keeping thorough records of all processing operations, especially when sensitive biometric data is involved. For organizations deploying FRT, accountability measures might include keeping records of when and where facial recognition systems are used, how data is handled, and the decisions made based on that data. Furthermore, organizations are expected to regularly review their processing activities and the associated risks, adapting their practices in response to new legal requirements or technological advancements. The designation of a Data Protection Officer (DPO) is a vital component of accountability under the GDPR, particularly in cases where the processing entails extensive surveillance of areas open to the public, which is often the case with FRT. Article 37(1)(b) of the GDPR specifies this requirement. In addition to making sure that GDPR regulations are followed, the DPO is in charge of managing data protection plans and serving as the organization's point of contact with the appropriate DPAs. In the context of FRT, the DPO's role is vital in monitoring the deployment of the technology, advising on best practices, and addressing any potential data protection concerns that arise. Another key element of accountability is the implementation of data protection by design and by default, as mandated by Article 25. This principle requires organizations to integrate data protection considerations into the development and operation of FRT from the outset, rather than as an afterthought. For instance, an organization might design its facial recognition system to minimize data collection, store data for the shortest possible time, and apply methods like anonymization or 'pseudonymization' to protect individual identities (22). By embedding these principles into the design of FRT systems, organizations can make certain that their use of the technology is aligned with GDPR requirements and reduces the potential for privacy breaches.

Data Security Measures

The GDPR places strict requirements on the implementation of suitable technical and organizational measures by data controllers and processors to guarantee a security level commensurate with the risk, as outlined in Article 32. Given the sensitivity of biometric data, especially facial recognition data, these security measures are critically important. Biometric data is unique and irreplaceable, and a breach involving such data could result in severe and irreversible consequences for the individuals affected. Security measures for FRT data must comprehensively address both the storage and transmission of this sensitive information. One of the primary technical safeguards is encryption, which protects biometric data both at rest and in transit by transforming it into a format that can only be accessed by authorized users with the decryption key. This guarantees that the data is shielded from unwanted access. Additionally, implementing secure storage solutions, such as dedicated biometric databases with restricted access, is crucial to protect against unwanted access and make sure that the data is used exclusively for its intended purpose. Access controls are a crucial element of data security, particularly for sensitive data like FRT data. Organizations must enforce strict access control policies to ensure that only authorized personnel have access to this data. This includes implementing multi-factor authentication, role-based access controls, and conducting regular audits of access logs to detect any unauthorized access attempts. Additionally, data controllers should establish procedures for continuous observation and testing of security measures to guarantee they remain effective against emerging threats, in line with the requirements set out in Article 32 of the GDPR. Incident response plans are also an essential aspect of data security. Even with the best preventive measures, data breaches can still occur, and organizations must be ready to respond swiftly and effectively. The GDPR, under Article 33, requires data controllers to notify the relevant DPA within 72 hours of becoming aware of a breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. For breaches involving FRT data, organizations must assess the potential impact on affected individuals and, if necessary, notify them of the breach. An effective incident response plan should incorporate protocols for locating and stopping the breach, evaluating its effects, and communicating with both the authorities and affected data subjects. The adoption of anonymization and pseudonymization techniques, which can reduce the dangers associated with processing biometric data, is another crucial component of data security. Anonymization, as referenced in Recital 26, involves transforming data so that it can no longer be attributed to a specific individual, thereby reducing the potential impact of a data breach. According to Article 4(5), 'pseudonymization' is a means of processing data to ensure it cannot be connected to a particular data subject without further information, which is to be securely stored apart. While anonymization may not always be feasible for FRT data due to its inherently identifying nature, pseudonymization can still provide significant protection by ensuring that there is no direct connection between the data and an identifiable individual.

Rights of Data Subjects

With regard to personal data, the GDPR gives data subjects a number of rights that are especially relevant to FRT, where there is a high potential of privacy infringement.

Right to Access: In accordance with GDPR Article 15, data subjects have the right to request confirmation from the data controller on the processing of their personal data. If processing is occurring, they are entitled to access that data, along with information on the reasons behind the processing, the types of data in question, and the recipients or groups of recipients to whom the data has been or will be sent. In the context of FRT, this right allows individuals to know if their facial data has been collected and used, and to request access to that data. For example, a person who suspects that their image has been captured by a facial recognition system in a public space can request access to that data to understand how it has been processed and for what purpose.

Right to Rectification: When personal information on a data subject is erroneous or lacking; they have the right to request that the data controller correct or complete the data without undue delay, as stipulated in Article 16 of the GDPR. In the context of FRT, this could involve correcting errors in the biometric data, such as inaccuracies in the facial recognition algorithm that might lead to incorrect identification or verification. Given the potential for significant harm arising from inaccuracies in FRT, the right to rectification is crucial in ensuring that individuals are not adversely affected by erroneous data processing.

Right to Erasure (Right to be Forgotten): Data subjects are granted the right under the GDPR to have their personal data erased in specific circumstances, such as when the data is no longer necessary for the purposes for which it was collected, when consent has been withdrawn, or when the data has been unlawfully processed, as outlined in Article 17. In the context of FRT, this right is especially important due to the permanent nature of biometric data. Individuals may seek to have their facial data erased from a system if they no longer wish to be identified by that system or if they have concerns about the security and use of their data.

Right to Restrict Processing: The right of data subjects to ask for the restriction of processing in certain situations, such as when the accuracy of the data is contested, or when the processing is unlawful but the data subject opposes erasure, as provided in Article 18 of the GDPR. In the context of FRT, this could involve limiting the use of facial recognition data to specific purposes or preventing further processing until issues of accuracy or lawfulness are resolved. This right allows individuals to exert control over how their biometric data is used, especially when there are concerns about the legitimacy of the processing.

Right to Data Portability: As stated in Article 20, the GDPR gives data subjects the right to transfer their personal data to another data controller and to receive it in a structured, widely-used, and machine-readable format. While this right is more commonly associated with transactional data, such as banking or social media information, it could also apply to biometric data, allowing individuals to transfer their facial recognition data between different service providers. This right is particularly relevant in ensuring that individuals maintain control over their data and can switch service providers without losing their data.

Right to Object: In specific situations, data subjects possess the entitlement to object to the processing of their personal data, especially if it is done so in order to pursue legitimate interests or is carried out for direct marketing purposes, as stated in Article 21. Regarding FRT, this right allows individuals to disagree or object to the application of this technology, particularly in situations where they feel that there is an unacceptable intrusion of their privacy. For instance, an individual might object to FRT use in a public setting where they believe the surveillance is excessive or unjustified.

The GDPR's rights for data subjects offer a strong framework for shielding people from the hazards that could arise from using FRT.

Critical Analysis of GDPR Safeguards

Adequacy of Existing Safeguards

The GDPR is often lauded as one of the most stringent and comprehensive data protection frameworks globally, especially in its application to emerging technologies like FRT. However, the adequacy of GDPR safeguards in effectively addressing the unique risks posed by FRT has been a subject of considerable debate. While the GDPR introduces robust mechanisms for protecting personal data, including biometric data, several gaps and challenges have been identified, particularly in relation to the dynamic and often covert nature of FRT. The GDPR's focus on data protection by design and by default, which requires that data protection measures be included into the development of any data processing activity from the outset, stipulated in Article 25, is one of its main advantages. This principle is particularly relevant to FRT, where the potential for privacy infringement is significant. By requiring organizations to consider data protection implications at every stage of FRT deployment, the GDPR aims to ensure that privacy risks are minimized. However, in practice, the effectiveness of this safeguard depends heavily on the commitment of data controllers to genuinely prioritize privacy considerations over operational efficiency or profit motives. In many cases, organizations may implement FRT systems with minimal consideration of the broader privacy implications, focusing instead on the immediate benefits of the technology. Moreover, the GDPR's requirement for DPIAs, pursuant to Article 35, is crucial when data processing is probably going to put people's rights and liberties at serious jeopardy, especially in the context of FRT. DPIAs are intended to provide a thorough assessment of the risks associated with data processing activities and to identify measures to mitigate those risks. However, the effectiveness of DPIAs can be limited by several factors. Firstly, the quality of DPIAs can differ significantly based on the expertise and resources at the disposal of the data controller. Smaller organizations or those with limited access to legal and technical expertise may struggle to conduct comprehensive DPIAs, leading to inadequate assessments of the risks associated with FRT. Secondly, there insufficient standardized rules for conducting DPIAs specifically for FRT, leading to inconsistencies in how these assessments are carried out. While the GDPR provides a general framework for DPIAs, it does not offer detailed guidance on addressing the specific risks posed by FRT, such as algorithmic bias, real-time surveillance, and the potential for mass data collection. This lack of specificity can result in DPIAs that fail to fully capture the unique challenges associated with FRT, thereby undermining their effectiveness as a safeguard. Another important facet of the protections provided by the GDPR is the principle of transparency, as stated in Article 12, which requires organizations to provide clear and accessible information to data subjects about how their data is being processed. Transparency is essential in ensuring that individuals are aware of when and how their facial data is being collected, processed, and used. However, the practical implementation of transparency in the context of FRT is fraught with challenges. For instance, in public spaces where FRT is used for surveillance, it may be difficult to provide meaningful notice to individuals who are unaware that their facial data is being captured. Additionally, the technical complexity of FRT may make it challenging for organizations to convey the nuances of data processing to data subjects in a manner that is both comprehensive and understandable. Furthermore, as mandated by Article 5(1)(c), the concept of data minimization requires that the amount of personal data gathered be sufficient, pertinent, and kept to a minimum for the purposes for which it is intended. This principle is particularly challenging to enforce in the context of FRT. The nature of FRT, which often includes gathering of large volumes of data, including data from individuals who may not be directly involved in the intended processing activity, inherently conflicts with the principle of data minimization. For example, when FRT is used in public surveillance, the technology may capture data from bystanders who are not the intended subjects of the surveillance. It is difficult to guarantee that in these situations, only pertinent data is collected, and often, the principle of data minimization is more honoured in theory than in practice.

Technical Dimensions of FRT and GDPR Compliance

Algorithmic Bias and Fairness

FRT has been widely documented to display differential accuracy rates across demographic groups, with notably lower performance for women and individuals with darker skin tones. These disparities raise significant concerns under GDPR principles of fairness and non-discrimination as provided in Article 5, undermining equitable treatment and public trust. As summarized in Table 1 (See Table 1 below), addressing such biases necessitates the adoption of rigorous practices, including comprehensive bias audits, enhanced algorithmic transparency, and regular calibration of models to mitigate disparities. Addressing such biases necessitates the adoption of rigorous practices, including comprehensive bias audits, enhanced algorithmic transparency, and regular calibration of models to mitigate disparities. Additionally, embedding fairness metrics during the development and deployment phases can significantly improve alignment with GDPR mandates.

Data Storage and Security

The GDPR emphasizes the need for advanced security measures such as encryption like the Advanced Encryption Standard with a 256-bit key and pseudonymization as provided under Article 4(5) to safeguard sensitive biometric data. However, practical implementation often falls short in areas like real-time anonymization and secure data deletion. Best practices for compliance include adopting robust encryption protocols, instituting role-based access controls, and conducting frequent audits to identify vulnerabilities. Furthermore, secure data retention and disposal policies, coupled with real-time anonymization techniques, can enhance compliance and reduce risks associated with data breaches.

Compliance Gaps

While the GDPR establishes a robust framework for data protection, it lacks specificity in addressing the technical nuances of FRT. The absence of standardized protocols for bias detection and secure data management leaves critical gaps in ensuring comprehensive compliance. This underscores the urgency for tailored regulatory guidance that reflects the unique challenges posed by FRT, particularly in algorithmic fairness and data lifecycle management.

Table 1: Challenges, Best Practices, and GDPR Provisions Related to Facial Recognition Technology

Aspect	**Challenges**	**Best Practices**	**GDPR Provisions**
Algorithmic Bias	Unequal accuracy rates across demographic groups, especially women and individuals with darker skin tones.	Conduct bias audits, implement algorithmic transparency, and perform regular testing to ensure fairness.	Article 5 (Fairness, Non-Discrimination)
Data Storage	Risks of breaches due to inadequate security measures.	Use robust encryption methods (e.g., AES-256), role-based access controls, and secure storage protocols.	Article 32 (Data Security)
Data Anonymization	Difficulty in achieving real-time anonymization during large-scale data collection.	Implement pseudonymization and real-time anonymization technologies for sensitive data.	Article 4(5) (Pseudonymization)
Secure Deletion	Challenges in ensuring the secure deletion of biometric data when no longer needed.	Adopt verifiable deletion protocols and maintain audit trails for data erasure.	Article 5(1)(e) (Storage Limitation)
Standardized Guidelines	Lack of clear, FRT-specific GDPR guidelines for handling data securely and addressing biases.	Advocate for regulatory guidance tailored to FRT, including standardized protocols for data handling and bias mitigation.	Article 25 (Data Protection by Design and Default)

Identified Gaps and Challenges

Despite the strengths of the GDPR, several gaps and challenges have been identified in its application to FRT, which call into question the adequacy of existing safeguards in protecting individual rights. One of the most significant challenges is the issue of algorithmic bias in FRT systems. Research has shown that FRT systems can exhibit significant accuracy disparities across different demographic groups, particularly in terms of race and gender. For example, studies have found that FRT systems are more prone to incorrectly identify people with darker complexions and women, leading to potential discrimination and the reinforcement of existing social inequalities (23). The fairness and non-discrimination principles of the GDPR are intended to address such issues, but in practice, the regulation does not provide specific guidelines for identifying and mitigating algorithmic bias in FRT systems. This gap leaves room for the deployment of FRT systems that may perpetuate bias, despite nominal compliance with GDPR. Another significant gap is the consent process under the GDPR relating to FRT. The GDPR requires that consent be freely given, specific, informed, and unambiguous, as outlined in Article 4(11). However, obtaining meaningful consent for the use of FRT is often challenging, particularly in public or semi-public spaces where individuals are unaware that their facial data is being collected. In such contexts, the power dynamics between data subjects and data controllers can make it challenging to verify that consent is truly voluntary and informed (24). For example, in situations where FRT is used as part of security measures in public transportation systems, individuals may feel compelled to authorize the use of their face data in order to obtain essential services, so compromising the voluntary nature of their consent. The issue of data subject rights, particularly the right to erasure (right to be forgotten), also presents significant challenges in the context of FRT. Under certain conditions, such as when the data is no longer required for the purposes for which it was originally collected or when consent is lost, individuals are entitled to have their personal data erased under the GDPR, as stated in Article 17. However, when it comes to FRT, the irrevocable nature of biometric data, once captured and stored, complicates the practical implementation of 'the right to erasure.' Unlike other categories of personal data, which can be deleted or anonymized, biometric data such as facial templates may be difficult, if not impossible, to completely erase without compromising the integrity of the underlying FRT system (25). This raises concerns about the extent to which individuals can truly exercise control over their biometric data once it has been collected and processed. Moreover, the GDPR's framework for international data transfers presents another area of concern. FRT systems often rely on cloud-based services for data storage and processing, which may involve the transfer of biometric data across borders. The GDPR places strict restrictions on the sharing of personal information with third parties, demanding that such transfers are only made to jurisdictions that provide an adequate level of data protection or are subject to appropriate safeguards. However, ensuring that these conditions are met in practice can be challenging, particularly in cases where FRT data is processed by third-party vendors located in jurisdictions with weaker data protection laws (26). The complexity of international data flows and the difficulty in enforcing GDPR standards globally raise significant challenges in ensuring that biometric data is adequately protected throughout its lifecycle.

Challenges in Applying Article 9 to Public Settings

Article 9 of the GDPR classifies biometric data, such as facial recognition data, as a "special category" of personal data due to its sensitive nature. The regulation imposes strict conditions on processing this data, generally prohibiting its use unless specific exemptions are met, such as explicit consent, substantial public interest, or other narrowly defined legal grounds.

Explicit Consent in Public Surveillance

One of the primary conditions under Article 9 is the requirement for explicit consent before processing biometric data. However, obtaining explicit consent in public settings, where FRT is often deployed for surveillance or security purposes, is inherently challenging. For instance: Impracticality of Consent Mechanisms: In public spaces like airports, train stations, or large events, where FRT is used for crowd monitoring or security screening, obtaining consent from every individual is logistically unfeasible. Many individuals are unaware that their biometric data is being captured, processed, and stored, undermining the GDPR's emphasis on transparency and informed consent.

Coercion Concerns: In situations where individuals must pass through FRT-enabled checkpoints (e.g., at border controls or stadium entrances), the concept of "freely given" consent becomes questionable. Individuals may feel they have no real choice but to comply, thereby rendering the consent invalid under GDPR standards.

Substantial Public Interest and Overreach: Article 9 allows for the processing of biometric data without consent if it is deemed necessary for reasons of substantial public interest. While this exemption enables the use of FRT for critical purposes such as preventing crime or ensuring public safety, it also introduces risks:

Broad Interpretation: The definition of "substantial public interest" is often broad and open to interpretation, leading to potential misuse. For example, law enforcement agencies may deploy FRT extensively under the guise of public safety, raising concerns about overreach and potential infringements on civil liberties.

Accountability Gaps: The lack of clear guidelines on what constitutes substantial public interest creates accountability gaps. It becomes difficult to ensure that FRT deployments in public settings are proportionate, necessary, and compliant with GDPR principles.

Mass Surveillance and Non-Compliance Risks: FRT's capacity for real-time, large-scale data collection in public settings makes it a powerful tool for surveillance. However, this capability directly conflicts with GDPR principles: Risk of Mass Surveillance: When deployed in public spaces, FRT can facilitate mass surveillance, capturing and processing biometric data from individuals who may not be relevant to the intended purpose. This undermines the GDPR's principle of data minimization in Article 5, which mandates that only data strictly necessary for the purpose should be collected.

Transparency Challenges: Article 13 of the GDPR requires individuals to be informed about the purposes and legal basis for data processing. In public settings, however, it is often impossible to provide adequate notice to everyone being monitored, especially in large crowds. This lack of transparency erodes public trust and complicates compliance with GDPR obligations.

Potential for Algorithmic Bias: In public settings, where FRT is applied to diverse populations, the risk of algorithmic bias becomes more pronounced:

Discrimination Concerns: Research has shown that FRT systems often exhibit reduced accuracy for specific demographic groups, particularly women and individuals with darker skin tones (27). In public surveillance contexts, these biases could lead to disproportionate targeting or misidentification, raising serious ethical and legal concerns under GDPR principles of fairness and non-discrimination.

Ethical Issues and Marginalized Populations

FRT raises significant ethical concerns, particularly regarding its impact on marginalized populations. These issues are exacerbated by disparities in algorithmic accuracy, which undermine social trust and fairness.

Disparities in Algorithmic Accuracy

As earlier stated, studies have demonstrated that FRT systems often perform less accurately for specific demographic groups, particularly women and individuals with darker skin tones. For example, Buolamwini and Gebru found that commercial FRT systems misclassified darker-skinned women at rates of up to 34.7%, compared to just 0.8% for lighter-skinned men. Such disparities can lead to:

Misidentification: Higher rates of false positives or negatives among marginalized groups, resulting in unfair treatment in law enforcement or access to services.

Reinforcement of Biases: Algorithmic inaccuracies perpetuate existing social inequalities, raising concerns about systemic discrimination and inequality.

Undermining Social Trust: These biases erode public confidence in the fairness and legitimacy of FRT applications, particularly in high-stakes contexts like law enforcement or public surveillance. Marginalized communities, already vulnerable to discrimination, may view FRT as a tool of oppression rather than one of safety, leading to reduced trust in institutions.

Comparative Analysis

A comparative analysis of data protection frameworks in other jurisdictions reveals additional insights into the challenges of regulating FRT and the potential gaps in the GDPR's approach. For instance, The US has approached data protection in a more fragmented manner with a patchwork of federal and state laws governing the use of biometric data. The Illinois Biometric Information Privacy Act (BIPA) is one of the most stringent state-level regulations, requiring explicit consent for the collection of biometric data and providing individuals with a private right of action to sue for violations (28). While BIPA offers strong protections for individuals, its application is limited to the state of Illinois, and there is no comprehensive federal law governing biometric data across the United States. The California Consumer Privacy Act (CCPA), for example, requires businesses to disclose data practices and grants individuals opt-out rights, but it lacks the stringent protections of GDPR or BIPA, particularly for biometric data. This fragmented approach emphasizes the difficulties in maintaining uniform data protection laws across jurisdictions and emphasizes the significance of all-encompassing legal frameworks such as the GDPR. In contrast, countries such as Canada and Australia have adopted more centralized approaches to data protection. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) 2000 and Australia's Privacy Act 1988 provide frameworks for the protection of personal data, including biometric data, with provisions for obtaining consent, ensuring data accuracy, and implementing security measures. However, these frameworks are generally less prescriptive than the GDPR and do not specifically address the distinct difficulties poised by FRT, such as algorithmic bias and real-time surveillance (29). This comparison underscores the relative strength of the GDPR's safeguards, while also highlighting areas where additional guidance or legislative amendments may be necessary to address the specific risks associated with FRT. Another relevant jurisdiction is China, where the deployment of FRT is widespread and often integrated into state surveillance programs (30). While China has recently introduced the Personal Information Protection Law (PIPL), which shares some similarities with the GDPR, including principles of data minimization and transparency, the broader context of state surveillance and the lack of independent oversight raise substantial concerns regarding the safety of individual rights (31). The Chinese approach illustrates the potential risks of FRT when used in contexts where data protection is subordinated to state interests, highlighting the importance of strong, independent regulatory frameworks like the GDPR in safeguarding individual rights.

Recommendations for Enhancing GDPR Safeguards

Given the identified gaps and challenges in the GDPR's application to FRT, several recommendations can be made to enhance the effectiveness of its safeguards:

Development of Specific Guidelines for FRT: There is a need for more detailed guidance from DPAs on the specific risks associated with FRT and how to address them (32). This could include standardized templates for conducting DPIAs specifically for FRT, as well as guidelines on addressing algorithmic bias, ensuring meaningful consent, and implementing transparency measures in public spaces.

Strengthening the Right to Erasure: The GDPR could be amended to include specific provisions on the right to erasure in the context of biometric data, including FRT. This could involve developing technical solutions for securely deleting biometric data or anonymizing it in a way that makes it unusable for identification purposes.

Enhanced Accountability Mechanisms: The GDPR's accountability requirements could be strengthened by requiring more rigorous oversight of FRT deployments, including mandatory audits by independent third parties and more stringent reporting requirements for data breaches involving biometric data. Additionally, organizations could be required to publish regular transparency reports detailing their use of FRT and the measures they have implemented to protect individual rights.

Addressing International Data Transfers: The GDPR's framework for international data transfers could be enhanced by developing specific protocols for the transfer of biometric data, including FRT data, to ensure that it is adequately protected regardless of where it is processed. This could involve stricter requirements for data localization or the development of binding corporate rules (BCRs) specifically for biometric data.

Conclusion

In conclusion, while the GDPR represents a significant advancement in data protection, its current safeguards reveal critical gaps in addressing the unique challenges posed by FRT, including algorithmic bias, consent in public surveillance, and the irrevocable nature of biometric data. The regulation's strengths—such as data protection by design, DPIAs, and transparency—are often undermined by inconsistencies in implementation and a lack of specific guidelines for emerging technologies. Comparative insights from jurisdictions like the United States, Canada and China underscore the need for a globally harmonized approach to FRT regulation. To strengthen the GDPR, detailed guidance on FRT-specific risks, enhanced accountability mechanisms, and robust protocols for international data transfers are essential. Addressing these challenges is vital to ensuring that the GDPR continues to safeguard individual rights amidst the rapid advancements of biometric technologies.

Abbreviations

BCR: Binding Corporate Rules, CNNs: Convolutional Neural Networks, DPIAs: Data Protection Impact Assessments, DPAs: Data Protection Authorities, DPO: Data Protection Officer, EDPB: European Data Protection Board, EU: European Union, FRT: Facial Recognition Technology, GDPR: General Data Protection Regulation, BIPA: Illinois Biometric Information Privacy Act, PIPA: Personal Information Protection Act, PIPEDA: Personal Information Protection and Electronic Documents Act.

Acknowledgment

The authors have no particular acknowledgments to make for this article.

Author Contributions

PETER I. GASIOKWU (PhD) conceptualized the study, led its design, and contributed extensively to the drafting of the manuscript, focusing on GDPR safeguards and data protection principles. UFUOMA GARVIN OYIBODORO originated the research idea, developed the methodological framework, conducted data analysis, and enriched the manuscript with a critical evaluation of algorithmic bias and comparative insights. MICHAEL O. IFEANYI NWABUOKU (PhD) structured the manuscript, refined the arguments on procedural safeguards and international data transfers, and reviewed the work for intellectual rigor, ensuring the recommendations were robust and actionable.

Conflict of Interest

The authors declare that there are no conflicts of interest related to this research.

Ethics Approval

Since this study did not involve human or animal subjects, ethics approval was not required.

Funding

The research did not receive any specific grants or financial support.

References

1. Martin C. Facial Recognition in Law Enforcement. Seattle Journal for Social Justice. 2020 Dec 31;19(1):311.
2. Gentzel M. Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy. Philosophy & Technology. 2021 Sep 25;34(4):1639–63.
3. Buolamwini J, Gebru T. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: Friedler SA, Wilson C, editors. Proceedings of Machine Learning Research. PMLR; 2018. 81 p. 1-15. Available from: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf
4. Petrescu RVV. Face Recognition as a Biometric Application. Journal of Mechatronics and Robotics. 2019 Jan 1;3(1):237–57.
5. Asemota MO. Facial Recognition Technology for Recruitment in the Russian Workplace. HSE Working Papers WP BRP 126/STI/2023. Moscow: National Research University Higher School of Economics; 2023 p. 10. Available from: https://wp.hse.ru/data/2023/08/17/2068455841/126STI2023.pdf
6. Krishnaprasad K, Aithal PS. A Conceptual Study on User Identification and Verification Process using Face Recognition Technique. International Journal of Applied Engineering and Management Letters (IJAEML). 2017;1(1):6–17.
7. Garvie C, Bedoya AM, Frankle J. The Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy & Technology; 2016 p. 1–119. Available from: from: https://www.statewatch.org/media/documents/news/2016/oct/usa-perpetual-lineup-face-recognition-database-report-10-16.pdf.
8. Khan N, Efthymiou M. The use of biometric technology at airports: The case of customs and border protection (CBP). International Journal of

Information Management Data Insights. 2021;1(2):1–14.

9. Karim NA, Khashan OA, Kanaker H, Abdulraheem WK, Alshinwan M, Al-Banna AK. Online Banking User Authentication Methods: A Systematic Literature Review. IEEE Access. 2024;12:741–57.
10. Martinez-Martin N. What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care? AMA Journal of Ethics. 2019 Feb 1;21(2):E180-187.
11. Johnson K. Facebook drops facial recognition to tag people in photos. Wired. 2021; Available from: https://www.wired.com/story/facebook-drops-facial-recognition-tag-people-photos/
12. Wang Z, Xu Y. Studies advanced in face recognition technology based on deep learning. Applied and computational engineering. 2024 Jan 31;31(1):121–32.
13. Bala N, Gupta R, Kumar A. Multimodal biometric system based on fusion techniques: a review. Information Security Journal: A Global Perspective. 2021 Dec 20;31(3):289–337.
14. Khare SK, Blanes-Vidal V, Nadimi ES, Rajendra AU. Emotion recognition and artificial intelligence: A systematic review (2014–2023) and research recommendations. Information Fusion. 2024;102:102019.
15. Peter D. Facial recognition technology for policing and surveillance in the Global South: a call for bans. Third World Quarterly. 2022;43(9):2325–35.
16. Perkowitz S. The Bias in the Machine: Facial Recognition Technology and Racial Disparities. MIT Case Studies in Social and Ethical Responsibilities of Computing. 2021 Feb 5;1–16. Available from: https://mit-serc.pubpub.org/pub/bias-in-machine
17. Fidler M, Hurwitz JG. An Overview of Facial Recognition Technology Regulation in the United States. In: Matulionyte R, Zalnieriute M, editors. The Cambridge Handbook of Facial Recognition in the Modern State. Cambridge: Cambridge University Press; 2024. p. 214–27.
18. Rodrigues R. Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. Journal of Responsible Technology. 2020;4:100005.
19. Wang X, Ying Cheng Wu, Zhou M, Fu H. Beyond surveillance: privacy, ethics, and regulations in face recognition technology. Frontiers in big data. 2024 Jul 3;7:1337465.
20. Mendoza I, Bygrave LA. The Right Not to be Subject to Automated Decisions Based on Profiling. In: Synodinou T, Jougleux P, Markou C, Prastitou T, editors. EU Internet Law: Regulation and Enforcement. Cham: Springer International Publishing; 2017. p. 77–98. Available from: https://doi.org/10.1007/978-3-319-64955-9_4
21. Gikay, Asress Adimi. Regulating Use by Law Enforcement Authorities of Live Facial Recognition Technology in Public Spaces: An Incremental Approach. The Cambridge Law Journal. 2023;82(3):414449
22. Sampaio S, Sousa P, Martins C, Ferreira A, Antunes L, Cruz-Correia R. Collecting, Processing and Secondary Using Personal and (Pseudo)Anonymized Data in Smart Cities. Applied sciences. 2023 Mar 16;13(6):3830.
23. Najibi A. Racial Discrimination in Face Recognition Technology. Science in the News. Harvard University; 2020. Available from: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/
24. Hill D, O'Connor CD, Slane A. Police use of facial recognition technology: The potential for engaging the public through constructed policymaking. International Journal of Police Science & Management. 2022;24(3):325–35.
25. Nakar S, Greenbaum D. Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy. Journal of Science & Technology Law. 2017;23(1):88–123.
26. Juliussen BA, Kozyri E, Johansen D, Rui JP. The third country problem under the GDPR: enhancing protection of data transfers with technology. International Data Privacy Law. 2023 Aug 1;13(3):225–43.
27. Limantė A. Bias in Facial Recognition Technologies Used by Law Enforcement: Understanding the Causes and Searching for a Way Out. Nordic Journal of Human Rights. 2024;42(2):115–34.
28. Buresh DL. Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute That Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws? Santa Clara High Technology Law Journal. 2021;38(1):39–93.
29. Bolca T. Can PIPEDA "Face" the Challenge? An Analysis of the Adequacy of Canada's Private Sector Privacy Legislation against Facial Recognition Technology. Canadian Journal of Law and Technology. 2020 Jun 1;18(1):51–90.
30. Aloamaka PC, Omozue MO. AI and Human Rights: Navigating Ethical and Legal Challenges in Developing Nations. Khazanah Hukum. 2024;6(2):189–201.
31. Weber PA, Zhang N, Wu H. A comparative analysis of personal data protection regulations between the EU and China. Electronic Commerce Research. 2020;20(3):565–87.
32. Aloamaka PC. Data Protection and Privacy Challenges in Nigeria: Lessons from Other Jurisdictions. UCC Law Journal. 2023 Jul 1;3(1):281–321.