2024 International Conference on Intelligent and Innovative Computing Applications (ICONIC)
7th-9th November 2024, Pearle Beach Resort & Spa, Flic en Flac, Mauritius
https://doi.org/10.59200/ICONIC.2024.010

The Face of Surveillance: A Systematic Review of Ethical and Legal Implications in Public Facial Recognition

Boanerges Beya
University of Pretoria
Pretoria, South Africa
u19288680@tuks.co.za

Monique Hanslo
University of South Africa
Pretoria, South Africa
nickyhanslo@gmail.com

Ridewaan Hanslo
University of Johannesburg
Johannesburg, South Africa
ridewaanh@uj.ac.za

Abstract
Due to its use of biometric data, which can be abused to exploit people, facial recognition technology (FRT), which is becoming more and more integrated into our daily lives, raises serious ethical and legal problems. To determine these consequences for the usage of FRT in public areas, this research conducts a systematic literature review. The public is frequently harmed by FRT, as seen by the recurrent themes of privacy, bias, and consent that emerged from the analysis of twenty different ethical and legal implications derived from the synthesized literature. Furthermore, the study shows that research on these topics come primarily from a small number of countries, none of which are African. This therefore provides a gap for future research into the potential implications of using FRT in African communities. The findings aim to inform policymakers to protect individual rights and ensure that FRT's advancement aligns with societal values and human rights.

Keywords: Biometrics, Surveillance, Discrimination, Data Protection, Human Rights

1. Introduction

Facial Recognition Technology (FRT) analyses facial patterns and compares it to a database of faces to establish a match. This technology has evolved from its early-stage development in the 1960s, with its applications spanning various sectors (Li et al., 2020). The rapid advancement and promising potential of FRT has led to its widespread adoption in different economies, industries, and general spaces. With such sophisticated technology being used in places like streets, malls, and other public environments, there are some ethical concerns and challenges that arise from potential infringements on privacy, surveillance and the potential for bias and discrimination. In some regions, law enforcement organizations are now using cameras equipped with FRT to detect offenders and hunt for missing people (Wang & Deng, 2021). There is also the legal landscape surrounding the use of such technology, along with questions concerning data protection, consent, human rights, and all required regulatory frameworks. The relevance of this topic stems from the extreme impact this technology has on individual rights, societal norms, and the potential impact on the life of an individual. The outcome of this research can be used to inform policy makers, protect individuals' privacy and their rights, and ensure that such technological advancements align with fundamental rights and societal values.

The growth in FRT is a result of immense advancements in computer vision, machine learning, and artificial intelligence; all also further enabled by the vast amounts of data available (Zhang, Feng & Sadeh, 2021). With the emergence of deep convolutional neural networks (CNN), FRT performance have recently increased considerably. However, its potential for unfairness raises concerns (Wang & Deng, 2020).

For instance, according to Garvie (2016), a year-long investigation involving 100 police stations indicated that African Americans are more likely to be stopped by law officers because of the FRT systems used. Furthermore, legal frameworks across varying regions and jurisdictions seem to be evolving too slow to adequately protect individuals' rights. For this paper the research problem consists of the condition associated with the topic which is the widespread adoption and increasing integration of FRT into everyday life, with the undesirable consequence being the potential violations of privacy, biases, and the

creation of a surveillance society, where individuals are constantly monitored and identified without their explicit consent (Kostka, Steinacker & Meckel, 2021). Therefore, the research question for this paper is: *What are the ethical and legal implications of using facial recognition technology in public spaces?*

The purpose of this paper is to identify and highlight the ethical and legal implications present in the use of FRT, more especially in public spaces as members of the public are directly affected. Furthermore, this research aims to shed light on the complexities and severity of the issue, and to contribute to the development of ethical guidelines and legal frameworks while ensuring that the technological progress and adoption of FR systems align with societal values, human rights and the common good. This review will address the undesirable consequence by shedding light on the problems that come with FRT by systematically reviewing articles and journals that address and speak of the legal and ethical implications associated with the technology and how individuals can be, are being and have been affected by its use in public spaces.

In the following sections, this paper will include a deeper look at the topic in the related works section. The research methodology section contains all the different data sources, selection criteria, Prisma flowchart, data extraction table, and the data analysis technique. The paper also includes an experiment and results section outlining all the findings and presenting the research results, as well as a section dedicated to the evaluation and discussion.

2. Related Works

According to Kaur, Krishan, Sharma, and Kanchan (2020), automated FRT is a relatively new concept. It first appeared in the 1960s, with the development of the first semi-automated system for facial recognition (FR). It was based on a procedure in which the observer found face features on images of the subject. Following that, distances, and ratios specific to a reference point were determined, allowing comparisons to be made, as all face characteristics have the same reference point (Mohammad, 2020). The domain of automated FRT was founded by Woody Bledsoe, Helen Chan Wolf, and Charles Bissom. In the 1970s, 21 subject-specific features, such as lip thickness, hair color, and skin complexion were used for FR, which caused inherit biases as well as the problem that the measurements were taken and calculated manually. In 1987, Sirovich and Kirby (1987) used the Principal Component Analysis (PCA) method, which is a mathematical technique used in data analysis and dimensionality reduction to simplify complex data while preserving its important pattern and structures, to try and address the facial-recognition problem. This was regarded to be a turning point in the field of face recognition because it demonstrated the ability to appropriately code and normalize a facial image.

In 1997, a software was developed that worked well enough to recognize occlusions in facial photographs, including ones that were not perfectly frontal. In recent studies related to FRT, the importance of one profile of the face is highlighted, demonstrating that the sensitivity and specificity of human identification has grown dramatically using this approach. Over the course of the last two decades, the algorithms that drive FRT have rapidly developed. During the same time span, the cost of cameras fell while access to high-quality broadband grew (Feldstein, 2019). As a result, FRT is widely and frequently used in and across worldwide nations.

3. Methodology

The research technique used in this study is a systematic literature review (SLR). SLR is an exacting process that involves finding, assessing, and synthesizing all the recent scholarly research on a certain subject (Kitchenham, 2004). It offers an objective summary of the body of knowledge, emphasizing significant discoveries, patterns, gaps, and areas of agreement or disagreement. This method provides for a comprehensive and unbiased evaluation of the ethical and legal implications of FRT in public areas.

3.1. Data Sources and Search Terms

The following search terms and strings were used in the respective data source (Google Scholar) and databases to obtain the papers for screening.

3.1.1 Google scholar data source:

(“Ethical implications” OR “Moral considerations” OR “Legal implications” OR “Legal concerns”) AND (“Facial recognition technology” OR “Public space monitoring” OR "Facial tracking”)

- 1410 results

(“Ethical implications” OR “Moral considerations” OR “Legal implications” OR “Legal concerns”) AND (“Facial recognition technology” AND “Public space”)

- 162 results

3.1.2 Scopus Database

("Ethical implications" OR "Moral considerations" OR "Legal implications" OR "Legal concerns") AND ("Facial recognition technology" OR "Public space monitoring" OR "Facial tracking") AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "ECON")) AND (LIMIT-TO (EXACTKEYWORD , "Face Recognition") OR LIMIT-TO (EXACTKEYWORD , "Facial Recognition") OR LIMIT-TO (EXACTKEYWORD , "Ethics") OR LIMIT-TO (EXACTKEYWORD , "Ethical Implications") OR LIMIT-TO (EXACTKEYWORD , "Law Enforcement") OR LIMIT-TO (EXACTKEYWORD , "Surveillance") OR LIMIT-TO (EXACTKEYWORD , "Information Systems") OR LIMIT-TO (EXACTKEYWORD , "Facial Recognition Technology") OR LIMIT-TO (EXACTKEYWORD , "Ethical Issues") OR LIMIT-TO (EXACTKEYWORD , "Computer Vision") OR LIMIT-TO (EXACTKEYWORD , "Ethical Concerns") OR LIMIT-TO (EXACTKEYWORD , "Privacy"))

- 42 results

3.1.3 ScienceDirect

(“Ethical implications” OR “Moral considerations” OR “Legal implications” OR “Legal concerns”) AND (“Facial recognition technology” OR “Public space monitoring” OR "Facial tracking”)

- 37 results

3.1.4 SpringerLink

“The ethical and legal implications of using facial recognition technology in public spaces.”

- Content Type - Article
- Discipline – Computer science
- Subdiscipline – AI
- Language – English
- 85 results

3.2. Selection Criteria

3.2.1. Inclusion Criteria

- Papers that discuss or address the ethical or ethical issues concerning the use of FRT or AI in public areas (As FRT is a subset of AI)
- Papers that discuss legal frameworks, regulations, or policies related to using FRT or AI in public areas
- Papers that report and discuss FRT, Facial tracking and/or public space monitoring and its implications
- Papers that are within the last 5 – 10 years
    - Allows for the capture of recent advancements, discussions and changes that occurred while also avoiding outdated information that would be irrelevant in the field of FRT
- Papers concerning FRT that are in various disciplines
    - To get a holistic view of FRT and how it effects the different sectors
- Articles that discuss the matter of surveillance concerns related to FRT

3.2.2. Exclusion Criteria

- Papers not written in English
- Papers that do not discuss or mention any ethical or legal dimensions to the use of FRT or AI
- Publications that focus primarily on the technical aspects of FRT without investigating its ethical and legal dimensions in public areas.
- Duplicate papers that are found in more than one database.

3.3. Prisma Flowchart

The databases used to retrieve these papers are:

- Scopus – 42 papers
- ScienceDirect – 37 papers
- SpringerLink - 85 papers

The PRISMA guidelines (Figure 1), which describe the selection procedure and modifications to the number of papers throughout, were adhered to in this SLR. With the search query restricted to 2013–2023, the first search on Google Scholar produced 1410 items. After the string was refined, 162 results were returned. Using customized search terms and wildcards, when necessary, subsequent database searches in SCOPUS, ScienceDirect, and SpringerLink produced the following results: 42, 37, and 85 articles, respectively. A total of 164 publications from database searches and 326 total papers for screening were the outcomes of this.

Automatic database filters were used to eliminate 80 papers that did not match the discipline, date range, language, or content type criteria, as well as 11 duplicate papers, before they were screened. 185 of the 235 papers that were left were eliminated throughout the screening process

because they did not match the inclusion or exclusion criteria. 50 papers remained for the eligibility evaluation.

A final selection of 30 papers was made for this evaluation after an additional 20 were disqualified for the reasons listed below.

Reason for excluding the 20 papers include:

- Reason 1 – Paper is not from a credible source and does not include reliable information
- Reason 2 – Paper's content is not relevant to the purpose/objective of this topic or is only focused on the technical aspect
- Reason 3 - Paper focuses mainly on subjects unrelated to FRT or AI and would have no contribution to the review

3.4. Data Extraction

An essential part of an SLR is data extraction. The pertinent data taken from the 30 papers were arranged and presented in an excel table. Titles, authors, publishing types, names of journals and conferences, and—above all—the extracted data—codes, criteria, concepts, dimensions, and significant themes—were all captured in this table—more room for remarks and notes allowed for a thorough documentation of the results. The study topic was ultimately addressed with the help of this organized technique, which made it possible to analyze and synthesize the acquired data effectively.

3.5. Data Analysis

Thematic analysis was used to understand and synthesize the results after data extraction and concept, code, and theme identification. Researchers can find patterns and significance in a variety of datasets by using the flexible qualitative method of thematic analysis (Alhojailan, 2012). It can be approached deductively, with analysis guided by pre-existing theoretical frameworks, or inductively, with themes emerging from the data. This study examined the ethical and legal implications of FRT in public areas using inductive methods.

4. Experiments and Results

A geographic focus of research on the ethical and legal implications of FRT was identified through data extraction. Papers from the US, Europe, and China accounted for most of the papers. This implies that many of the conversations and arguments over FRT take place in these regions. Europe and the USA stand out, as shown in Figure 2, where each location is cited in about 33% of the papers. Australia and India each provide 6%, and China comes in second with 16%. In 2% of the papers, Saudi Arabia, Brazil, and Canada are each referenced.

After the data was extracted, a thematic analysis of the thirty publications that were chosen for examination identified eighteen main topics concerning the ethical and legal implications of FRT in public areas. Table 1 presents a further categorization of these topics according to their type and dimension. Under the category of ethical implications were eight themes: privacy; bias and discrimination; trustworthiness; surveillance; consent and transparency; accuracy and accountability; mission creep; and identity challenges. Positive and negative consequences were distinguished within the legal dimension. Themes that were seen as positive included public safety and security, law and regulation amendments, justice and crime prevention, legal justifications, and law enforcement support. Human rights violations, the exploitation of biometric data, worries about data security and protection, cyberattacks, and concentration of power and control were among the negative themes. Table 1 provides explicit implications for each category along with a list of corroborating references.

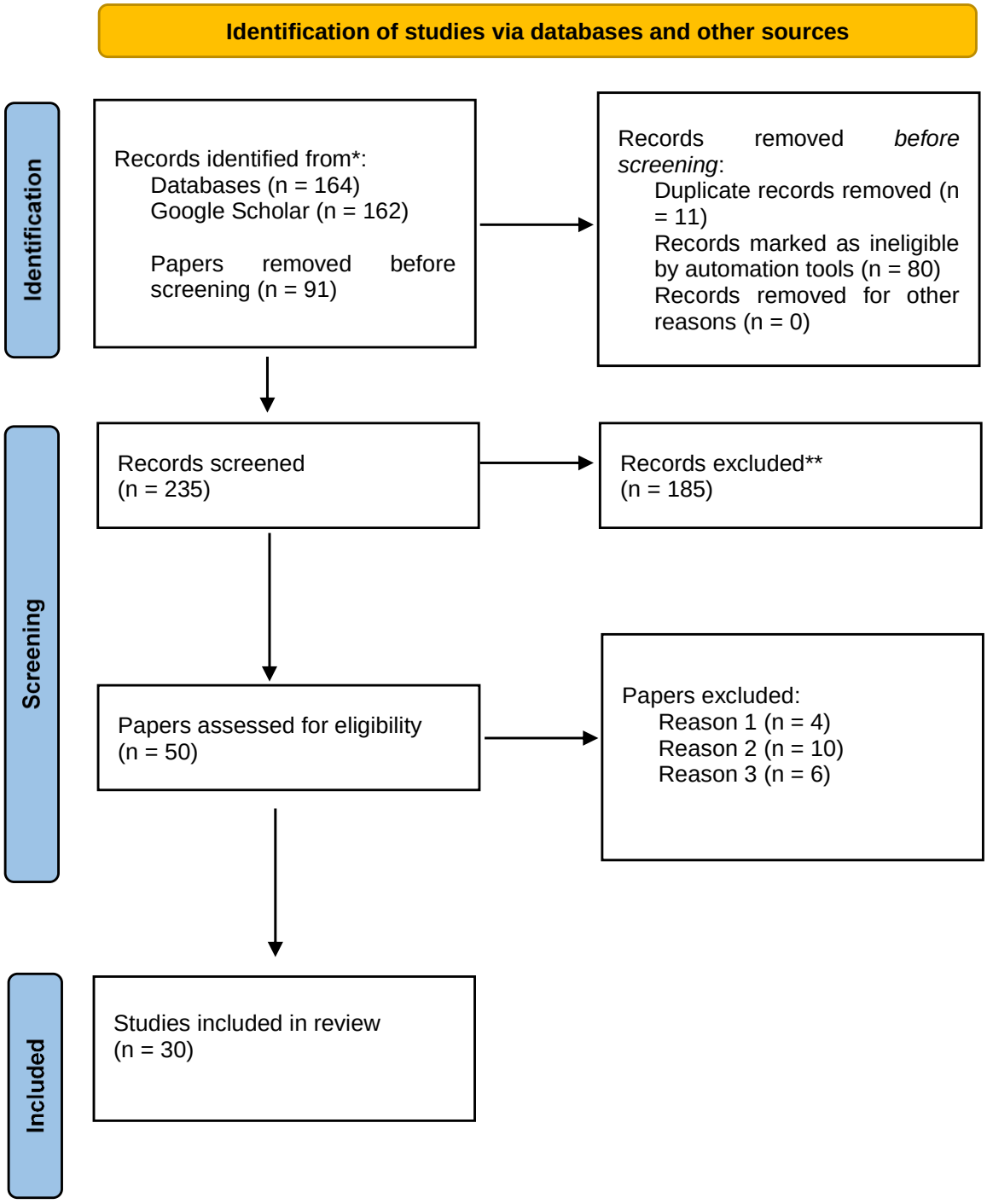

Figure 1. Prisma Flowchart

4.1. Themes

4.1.1. Ethical Dimension

4.1.1.1. Privacy

Numerous studies have shown that the widespread use of FRT in public settings poses a serious danger to privacy (Waelen, 2022). Concerns over the loss of individual privacy rights are raised by FRT's natural potential to record sensitive personal information, such as biometric data, activities, and emotions (Zhang, 2021).

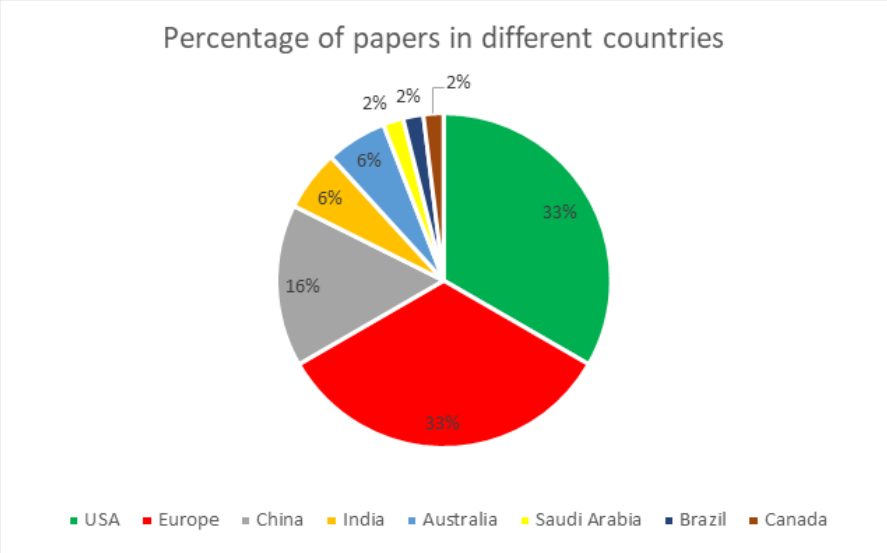

Figure 2. Frequency of the papers per region

Table 1. Representation of findings

Dimensions	**Categories**	**Themes**	**Implications**	**Sources**
Ethical	Negative	Privacy Bias and Discrimination Trustworthiness Surveillance Consent and Transparency Accuracy and Accountability Mission creep Identity challenges	Decreased individual privacy Decreased Human dignity Creates racial division Divided public opinion Bias and discrimination towards underrepresented groups Diminished individual reputation Decreased citizen-government trust. Creates social classification and categorization Increased individual identity crisis	(Akhtar, 2019); (Almeida et al., 2020); (Andrejevic & Selwyn, 2019); (Brown et al., 2021); (Chen & Wang, 2023); (Chilson & Barkley, 2021); (Chochia & Nässi, 2021); (De Keyser et al., 2021); (Guo & Kennedy, 2022); (Kamila & Jasrotia, 2023); (Khogali & Mekid, 2023); (Kostka, 2021); (Martinez-Martin, 2019); (Mobilio, 2022); (Moraes, 2020); (Neuwirth, 2023); (North-Samardzic, 2019); (Ong, 2021); (Paik, 2022); (Roundtree, 2021); (Royakkers et al., 2018); (Saheb, 2023); (Sarabdeen, 2022); (Shore, 2022); (Waelen, 2022); (Smith & Miller, 2021); (Wen & Holweg, 2023); (Zhang et al., 2021)
Legal	Positive	Security and public Safety	Increased public security and safety Amendment of existing laws and regulation	(Andrejevic & Selwyn, 2019); (Brown et al., 2021); (Chen & Wang, 2023); (Chilson & Barkley, 2021); (Chochia

Dimensions	Categories	Themes	Implications	Sources
		Law and regulation amendments Justice and crime prevention Legal justifications Law enforcement support	Creation and enactment of new laws and regulations Increase in justice and overall crime prevention Legal justification requirement to use FRT in public Increased support to law enforcement duties	& Nässi, 2021); (De Keyser et al., 2021); (Kamila & Jasrotia, 2023); (Khogali & Mekid, 2023); (Kostka, 2021); (Milossi, 2021); (Ong, 2021); (Roundtree, 2021); (Saheb, 2023); (Sarabdeen, 2022); (Smith & Miller, 2021); (Wen & Holweg, 2023)
	Negative	Human rights violation Use biometric data Data protection and security Cyberattacks Concentration of power and Control	Increased protests and civil unrest Potential abuse of power Decreased in individual autonomy Cybercrime threats expose inherent FRT vulnerabilities Exacerbated imbalance of power Threat to democracy	(Akhtar, 2019); (Almeida et al., 2020); (Andrejevic & Selwyn, 2019); (Chilson & Barkley, 2021); (Guo & Kennedy, 2022); (Milossi, 2021); (Roundtree, 2021); (Royakkers et al., 2018); (Saheb, 2023); (Sarabdeen, 2022); (Shore, 2022); (Smith & Miller, 2021); (Wen & Holweg, 2023); (Zhang et al., 2021)

Although there may be less obstacles related to FRT, privacy issues are nonetheless inextricably linked to the fundamental purpose of the technology (Akhtar, 2019). Moreover, privacy is acknowledged as a primary problem in FRT discourse, linked to more general concerns like data protection, monitoring, and human rights abuses (North-Samardzic, 2019).

4.1.1.2. Bias and Discrimination

FRT frequently functions without the express consent of the people whose photos are taken and analyzed (Waelen, 2022). The possibility of algorithmic bias in FRT systems is a persistent worry since it might result in discriminatory outcomes, especially in law enforcement settings (Akhtar, 2019). As an illustration of the disproportionate effect on underprivileged groups, a study conducted in Brazil revealed that 90.5% of those detained utilizing FRT were Black (Moraes et al., 2020). These prejudices have the potential to uphold current disparities and violate the rights of marginalized groups of people based on age, sex, color, and ethnicity (Zhang, 2021).

4.1.1.3. Trustworthiness

The public's acceptance of FRT in public areas is greatly influenced by trust (Zhang, 2021). According to Moraes et al. (2020), the absence of explicit public permission and the lack of transparency around the deployment and functionality of FRT degrade public trust in both governments and enterprises participating in the technology. Widespread adoption of FRT systems depends on public confidence in their accuracy and dependability, yet present procedures frequently betray that confidence.

4.1.1.4. Surveillance

According to Akhtar (2019), FRT is widely utilized by the state for monitoring in public areas, which raises ethical questions about identity loss, infringement on the rights to obscurity, anonymity, and assembly, and possible modification of the public domain. According to Andrejevic and Selwyn (2019), FRT surveillance is regarded as exceptionally hazardous, endangering both democracy and individual liberties. Nonetheless, there is hope for reducing these risks due to legal precedents such as the Dutch court's decision to reject an automated surveillance system (Chochia, 2021).

4.1.1.5. Consent and Transparency

Concerns regarding data mining and privacy issues are raised by the frequent deployment of FRT in public areas without clear public knowledge or authorization (Chochia, 2021). Although there are laws protecting biometric and personal data, such as the General Data Protection Regulation (GDPR) Art. 9, they are not globally enforced, leaving people exposed in areas where they are not. The problem is made worse when law enforcement violates citizens' right to privacy by using FRT and gaining unauthorized access to civilian databases (Sarabdeen, 2022). Furthermore, the public's ability to choose or opt out is denied by a lack of openness surrounding the FRT algorithms and deployment (Kamila and Jasrotia, 2023).

4.1.1.6. Accuracy and Accountability

For FRT to be used ethically, accuracy is essential. If accuracy concerns and appropriate restrictions are not resolved, the UN Office of the High Commissioner for Human Rights (OHCHR) advises stopping real-time FRT in public areas (Sarabdeen, 2022). Serious repercussions, including assassinations and damage to people's reputations and well-being, can result from inaccurate FRT (Mobilio, 2023). Accountability measures are therefore necessary to guarantee responsible use and lessen the potential harm that may result from imprecise FRT systems.

4.1.1.7. Mission Creep

Concerns about mission creep, which is the progressive enlargement of a project's objectives beyond its initial purpose (Guo and Kennedy, 2022), are pertinent when it comes to the application of FRT. Inconsistencies between the declared goals of FRT providers and the technology's actual application may increase public mistrust of both firms and governments (De Keyser et al., 2021).

4.1.1.8. Identity Challenges

When FRT misidentifies people or fails to recognize them correctly based on demographic characteristics, it might lead to identity issues (Waelen, 2022). These mistakes may have a detrimental effect on one's sense of respect and self-worth, which could have long-term psychological repercussions (Waelen, 2022). The difficulties with FRT and identity are further made worse by the possibility of identity theft due to cyberattacks that steal biometric data (Chochia, 2021).

4.1.2. Legal Dimension – Positive Category

4.1.2.1. Security and Public Safety

It is claimed that by discouraging small-time criminality and fostering a sense of security, the deployment of FRT in public areas enhances security and public safety (Chochia, 2021). For example, FRT is recommended in schools to reduce events such as shootings by registering and accounting for every individual there (Andrejevic and Selwyn, 2019). However, privacy and individuality are sacrificed in order to reap these possible benefits.

4.1.2.2. Law and Regulation Amendments

Current laws, policies, and regulations must be updated and amended considering the widespread use of FRT in public areas (Wen and Holweg, 2023). This is essential to stop technological abuse and safeguard the rights of those who are impacted by it. New laws must be passed to close any gaps in the current legal frameworks and avoid FRT being used as a means of state monitoring, as has happened in this instance in China (Brown et al., 2021).

4.1.2.3. Justice and Crime Prevention

FRT is a useful tool for law enforcement since it helps locate missing people and criminal suspects, which may speed up the process of solving crimes (Saheb, 2023). By warning authorities of known risks, FRT can improve public safety by serving as a deterrent to criminal activity.

4.1.2.4. Legal Justification

Legal justification for the gathering, handling, and archiving of biometric data is required for the implementation of FRT in public areas (Chochia & Nässi, 2021). For judicial authorities, FRT can offer important evidence that helps identify

suspects and ensure justice (Chochia & Nässi, 2021). Nonetheless, for the use of FRT for law enforcement to be deemed legally acceptable, it must closely conform to all applicable laws and regulations (Akhtar, 2019).

4.1.2.5. Law Enforcement Support

By speeding up the resolution of crimes and improving public safety, FRT can greatly assist law enforcement; however, this is only possible if police enforcement organizations follow the applicable laws and rules governing its usage in public areas (Almeida et al., 2020; Chilson & Barkley, 2021; Fontes et al., 2022; Guo & Kennedy, 2022; Moraes, 2020).

4.1.3. Legal Dimension – Negative Category

4.1.3.1. Human Rights Violation

Since there is no set framework for implementing FRT, there are serious concerns regarding human rights breaches when it comes to its deployment (Almeida et al., 2021). Many universal human rights, such as the right to privacy, freedom of speech, individual liberty, anonymity, expression, association, and assembly, may be violated by FRT (Wen and Holweg, 2023). The foundations of a democratic society are put in jeopardy by this limitation of freedom. Since it places a strong emphasis on equality, inclusiveness, privacy, and just legal procedures, current human rights law, such as the Human Rights Act, may provide a more thorough framework to resolve these issues (Almeida et al., 2021). To safeguard personal information and lessen the hazards associated with biased and incompatible FRT systems, a strong legal and regulatory framework is necessary (Milossi, 2021).

4.1.3.2. Use of Biometric Data

As sensitive personal information, biometric data must be handled carefully and in accordance with human rights laws and privacy rules (Chochia & Nässi, 2021). FRT's intrusive biometric data collection methods give rise to worries about mass monitoring and possible illegality, especially in European courts (Akhtar, 2019). Biometric data collection and misuse have the potential to erode freedom of speech and expression and cause self-censorship (Sarabdeen, 2022).

4.1.3.3. Data Protection and Security

It may be illegal to use FRT in public areas due to current data protection laws and regulations. This is demonstrated by a case where the police violated people's right to privacy and data protection by using FRT to scan everyone instead of just identifying suspects (Chochia, A, 2021). Moreover, common law nations' legal systems have not sufficiently changed to handle privacy concerns brought on by biometric data-using technologies such as FRT (Almeida et al., 2021).

4.1.3.4. Cyberattacks

Cyberattacks on FRT systems have the potential to cause data breaches, and unlawful access to private biometric data and surveillance footage (Roundtree, 2021). Significant privacy violations, identity theft, fraud, and legal implications for the offending corporation are all possible outcomes of such breaches. Cyberattacks on FRT systems may also result in a decline in public confidence, issues with national security, and possible manipulation of the technology itself (Moraes et al., 2020).

4.1.3.5. Concentration of Power and Control

According to Andrejevic and Selwyn (2019), the implementation of FRT may result in a concentration of power in the hands of businesses or governments. With the use of monitoring and the threat of consequences for noncompliance, corporations may now influence public behavior, undermining individual autonomy and changing the balance of power between the people and the government.

5. Evaluation and Discussion

The examination of 30 papers yielded 18 different themes pertaining to the ethical and legal implications of FRT use in public areas. Eight themes—privacy, bias, trust, surveillance, consent, accuracy, mission creep, and identification challenges—were classified as having ethical implications. The other 10 topics were divided into five good and five negative categories, categorized as legal implications: human rights violations, biometric data use, data protection and security, cyberattacks, concentration of power and control, and security, justice and crime prevention, legal justifications, and law enforcement support.

Most studies on the consequences of FRT concentrate on a few numbers of nations, mainly the USA, Europe, and China, indicating that these areas are leading the way in the adoption of FRT. This draws attention to a major research vacuum concerning the application of FRT in African settings. Owing to either underreporting or a lack of broad use, further research is required to fully comprehend the possible effects of FRT

deployment in African societies, environments, and communities.

While the data analysis of 30 studies yielded 18 distinct themes, in turn, it helped identify the specific ethical and legal concerns of FRT use in public settings. Reduced human dignity, racial division, split public opinion, prejudice and discrimination against marginalized groups, tarnished personal reputations, weakened citizen-government trust, social categorization and classification, and heightened risk of identity crisis are just a few of the ethical implications. Table 1 contains specifics on these implications along with the sources that back them up.

Positive and negative legal implications of FRT in public areas are distinguished. The need for legal justification of FRT use, improved justice and crime prevention, updated laws and regulations, and enhanced safety and public security are among the positive effects (Table 1). Negative effects include a rise in demonstrations and social disturbance, possible power abuse, a decline in personal liberty, vulnerability to cybercrime, a worsening of power disparities, and a possible threat to democracy (Table 1).

This study informs developers, legislators, and human rights activists about the ethical and legal implications of using FRT in public areas. The results highlight the pressing need for regulation and offer policymakers a framework for addressing the effects of FRT on people and society. The diversity of demographics and approaches among the examined publications, as well as the difficulties in evaluating each study's quality, restrict the study, nevertheless.

6. Conclusion

Concerns about possible ethical and legal transgressions are raised by the broad use of Facial Recognition Technology (FRT) and its integration into many facets of daily life (Zhang, 2021). This research used a systematic literature review (SLR) to investigate 30 studies to find themes relating to the research question: *What are the ethical and legal implications of using Facial Recognition Technology in public spaces?*

The research yielded 20 ethical and legal implications of FRT deployment in public areas by identifying 18 main themes. According to the data, several countries (the USA, Europe, China, India, Australia, Saudi Arabia, Brazil, and Canada) have a disproportionate amount of FRT research and reporting, indicating that these areas are at the forefront of FRT adoption. This emphasizes how important it is to do further study and reporting on FRT in African settings. Furthermore, there are no defined human rights or legal norms for FRT rollout because the quick expansion of FRT deployment has overtaken policy and regulatory frameworks (Almeida et al., 2021). As of right now, the only comprehensive data protection statute that addresses FRT is the European GDPR (Sarabdeen, 2022). The use of FRT in public places has 20 different ethical and legal implications, with privacy emerging as the main issue. Because of privacy issues, the Office of the High Commissioner for Human Rights (OHCHR) of the United Nations even suggests stopping real-time remote biometric recognition until appropriate regulations are in place (Sarabdeen, 2022). These implications show the complex and numerous issues connected with FRT deployment and emphasize the necessity for careful assessment and regulation to avoid potential harms.

Although this topic is very briefly discussed in the literature currently in publication, future studies could examine the possible ethical benefits of FRT in public settings (Andrejevic and Selwyn, 2019; Sarabdeen, 2022; Zhang, 2021; Chilson and Barkley, 2021; Milossi, 2021; Roundtree, 2021). Furthermore, more research is required to evaluate the relative merits of FRT, possibly with the use of primary data and non-traditional research techniques. Given the widespread deployment of FRT, another important subject for future research is the development of a uniform universal regulatory framework, as well as investigating how cybercrime risks expose inherent weaknesses in FRT systems (Roundtree, 2021).

7. References

Akhtar, M. (2019). Police use of facial recognition technology and the right to privacy and data protection in Europe. NAVEIÑ REET: Nordic Journal of Law and Social Research, 9, 324–344. https://doi.org/10.7146/nnjlsr.v1i9.122165

Alhojailan, M., & Ibrahim. (2012). Thematic analysis: A critical review of its process and evaluation.

Almeida, D., Shmarko, K., & Lomas, E. (2021). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial

intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics, 2(3), 377–387. https://doi.org/10.1007/s43681-021-00077-w

Andrejevic, M., & Selwyn, N. (2019). Facial recognition technology in schools: critical questions and concerns. Learning, Media and Technology, 45(2), 115–128. https://doi.org/10.1080/17439884.2020.1686014

Brown, T. G., Statman, A., & Sui, C. (2021). Public Debate on Facial Recognition Technologies in China. *MIT* Case Studies in Social and Ethical Responsibilities of Computing. https://doi.org/10.21428/2c646de5.37712c5c

Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. Telecommunications Policy, 47(2), 102482. https://doi.org/10.1016/j.telpol.2022.102482

Chidumije, A., Gowher, F., Kamalinejad, E., Mercado, J., Soni, J., & Zhong, J. (2021). A Survey of CNN and Facial Recognition Methods in the Age of COVID-19∗. 2021 the 5th International Conference on Information System and Data Mining. https://doi.org/10.1145/3471287.3471292

Chilson, N. A., & Barkley, T. D. (2021). The Two Faces of Facial Recognition Technology. IEEE Technology and Society Magazine, 40(4), 87–100. https://doi.org/10.1109/mts.2021.3123752

Chochia, A., & Nässi, T. (2021). Ethics and emerging technologies – facial recognition. IDP Revista de Internet Derecho Y Política, 34, 1–12. https://doi.org/10.7238/idp.v0i34.387466

De Keyser, A., Bart, Y., Gu, X., Liu, S. Q., Robinson, S. G., & Kannan, P. K. (2021). Opportunities and challenges of using biometrics for business: Developing a research agenda. Journal of Business Research, 136, 52–62. https://doi.org/10.1016/j.jbusres.2021.07.028

Feldstein, S. (2019). The global expansion of AI surveillance (Vol. 17, No. 9). Washington, DC: Carnegie Endowment for International Peace.

Fontes, C., Hohma, E., Corrigan, C. C., & Lütge, C. (2022). AI-powered public surveillance systems: why we (might) need them and how we want them. Technology in Society, 71, 102137. https://doi.org/10.1016/j.techsoc.2022.102137

Garvie, C. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law, Center on Privacy & Technology.

Guo, Z., & Kennedy, L. (2022). Policing based on automatic facial recognition. Artificial Intelligence and Law, 31(2), 397–443. https://doi.org/10.1007/s10506-022-09330-x

Kamila, M. K., & Jasrotia, S. S. (2023). Ethical issues in the development of artificial intelligence: recognizing the risks. International Journal of Ethics and Systems. https://doi.org/10.1108/ijoes-05-2023-0107

Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2020). Facial-recognition algorithms: A literature review. Medicine, Science and the Law, 60(2), 131-139.

Khogali, H. O., & Mekid, S. (2023). The blended future of automation and AI: Examining some long-term societal and ethical impact features. Technology in Society, 73, 102232. https://doi.org/10.1016/j.techsoc.2023.102232

Kim, E., Bryant, D., Srikanth, D., & Howard, A. (2021). Age Bias in Emotion Detection: An Analysis of Facial Emotion Recognition Performance on Young, Middle-Aged, and Older Adults. Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society. https://doi.org/10.1145/3461702.3462609

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, 33(2004), 1-26.

Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. Public Understanding of Science, 30(6), 671–690.

https://doi.org/10.1177/09636625211001555

Li, K., Jin, Y., Akram, M. W., Han, R., & Chen, J. (2020). Facial expression recognition with convolutional neural networks via a new face cropping and rotation strategy. The visual computer, 36, 391-404.

Li, L., Mu, X., Li, S., & Peng, H. (2020). A Review of Face Recognition Technology. IEEE Access, 8, 139110–139120. https://doi.org/10.1109/access.2020.3011028

Martinez-Martin, N. (2019). What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care? AMA Journal of Ethics ® POLICY FORUM , 21(2), 180–187.

Matulionyte, R., & Hanif, A. (2021). A call for more explainable AI in law enforcement. 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW). https://doi.org/10.1109/edocw52865.2021.00035

Milossi, M. (2021). Remote biometric identification systems and ethical challenges: The case of facial recognition. 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). https://doi.org/10.1109/seeda-cecnsm53056.2021.9566226

Mobilio, G. (2023). Your face is not new to me – Regulating the surveillance power of facial recognition technologies. Internet Policy Review, 12(1). https://doi.org/10.14763/2023.1.1699

Moraes, T. G., Almeida, E. C., & de Pereira, J. R. L. (2020). Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces. AI and Ethics, 1(2), 159–172. https://doi.org/10.1007/s43681-020-00014-3

Neuwirth, R. J. (2023). Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA). Computer Law & Security Review, 48, 105798. https://doi.org/10.1016/j.clsr.2023.105798

North-Samardzic, A. (2019). Biometric Technology and Ethics: Beyond Security Applications. Journal of Business Ethics, 167(3), 433–450. https://doi.org/10.1007/s10551-019-04143-6

Ong, D. C. (2021). An Ethical Framework for Guiding the Development of Affectively-Aware Artificial Intelligence. 2021 9th International Conference on Affective Computing and Intelligent Interaction (ACII). https://doi.org/10.1109/acii52823.2021.9597441

Parsheera, S. (2019). Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3525324

Pearson, Y., & Borenstein, J. (2020). Robots, Ethics, and Pandemics: How Might a Global Problem Change the Technology's Adoption? 2020 IEEE International Symposium on Technology and Society (ISTAS). https://doi.org/10.1109/istas50296.2020.9462229

Power, D. J., Heavin, C., & O'Connor, Y. (2021). Balancing privacy rights and surveillance analytics: a decision process guide. Journal of Business Analytics, 4(2), 155–170. https://doi.org/10.1080/2573234x.2021.1920856

Roundtree, A. K. (2021). Ethics and Facial Recognition Technology: An Integrative Review. 2021 3rd World Symposium on Artificial Intelligence (WSAI). https://doi.org/10.1109/wsai51899.2021.9486382

Royakkers, L., Timmer, J., Kool, L., & van Est, R. (2018). Societal and ethical issues of digitization. Ethics and Information Technology, 20(2), 127–142. https://doi.org/10.1007/s10676-018-9452-x

Saheb, T. (2023). "Ethically contentious aspects of artificial intelligence surveillance: a social science perspective." AI and Ethics, 3(2), 369–379. https://doi.org/10.1007/s43681-022-00196-y

Sarabdeen, J. (2022). Protection of the rights of the individual when using facial recognition technology. Heliyon, 8(3), e09086. https://doi.org/10.1016/j.heliyon.2022.e09086

Shore, A. (2022). Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy. Telematics and Informatics, 70, 101815. https://doi.org/10.1016/j.tele.2022.101815

Sirovich, L., & Kirby, M. (1987). Low-dimensional procedure for the characterization of human faces. Josa a, 4(3), 519-524.

Smith, M., & Miller, S. (2021). The ethical application of biometric facial recognition technology. AI & SOCIETY, 37(1), 167–175. https://doi.org/10.1007/s00146-021-01199-9

Waelen, R. A. (2022). The struggle for recognition in the age of facial recognition technology. AI and Ethics, 3(1), 215–222. https://doi.org/10.1007/s43681-022-00146-8

Wang, M., & Deng, W. (2021). Deep face recognition: A survey. Neurocomputing, 429, 215-244.

Wang, M., & Deng, W. (2020). Mitigating bias in face recognition using skewness-aware reinforcement learning. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 9322-9331).

Wen, Y., & Holweg, M. (2023). A phenomenological perspective on AI ethical failures: The case of facial recognition technology. AI & SOCIETY. https://doi.org/10.1007/s00146-023-01648-7

Zhang, S., Feng, Y., & Sadeh, N. (2021). Facial Recognition: Understanding Privacy Concerns and Attitudes Across Increasingly Diverse Deployment Scenarios.