مجلة جامعة الشارقة للعلوم القانونية

جامعة الشارقة
UNIVERSITY OF SHARJAH

University of Sharjah Journal of Law Sciences

A Refereed Scientific journal

Vol. 22, No. 2
Dhul Hijjah1446 A.H. / June 2025 A.D.

ISSN : 2616-6526

University of Sharjah Journal for Law Sciences, Volume 22, No. 2 June 2025
https//:doi.org/10.36394/jls.v22.i2.4

Facial Recognition Technology in Law Enforcement: Navigating the Balance Between Security and Civil Liberties in the UK and Europe

Mohamed Gamil Zakaria Mahmoud(1)

Received on: 10-06-2024 **Accepted on: 19-11-2024**

Abstract:

The increasing use of facial recognition technology (FRT) by law enforcement has sparked considerable debate over its potential impacts on privacy, civil liberties, and human rights. This research provides an in-depth analysis of the regulatory, ethical, and social dimensions surrounding FRT deployment in the United Kingdom and the European Union. The study examines the contrasting regulatory frameworks, focusing on the EU's recent Artificial Intelligence Act, which adopts a preventive, rights-based approach, and the UK's reactive reliance on judicial oversight. While FRT can enhance public safety and improve crime-solving capabilities, it raises serious concerns about privacy violations, potential bias and discrimination, and the risk of function creep—where surveillance extends beyond its original purpose.

This paper advocates for a balanced "regulated deployment" approach, proposing that FRT be used under clearly defined, controlled circumstances. Recommendations include the implementation of robust legal frameworks that adhere to principles of necessity, proportionality, and non-discrimination, alongside rigorous governance structures to ensure transparency and accountability. Additionally, the paper underscores the need for global policy coordination and cross-border regulatory harmonization to address the complex ethical and legal challenges posed by FRT. By proposing comprehensive reforms and best practices, this research aims to establish a foundation for the responsible and ethical deployment of FRT that aligns with democratic values and respects individual rights.

Keywords: Facial Recognition Technology, Law Enforcement, Civil Liberties, Privacy.

(1) Faculty of Law – Ain Shams University (Cairo - Egypt)
gamil.mg.mz@gmail.com

Introduction:

Facial recognition technology (FRT) has emerged as a powerful tool in law enforcement, extending beyond mere identification to active surveillance(1). However, its rapid adoption has raised widespread concerns about potential infringements on privacy, risks of bias and discrimination, and possible erosion of civil rights and liberties. As FRT becomes increasingly sophisticated and prevalent in public spaces, debates surrounding its use have intensified, with stakeholders expressing concerns over public anonymity and privacy. Critics caution that without adequate safeguards and accountability, the deployment of FRT may compromise fundamental democratic principles by challenging expectations of privacy in public spaces.

Research has highlighted issues of bias within FRT systems, particularly with regard to gender and racial disparities, which can lead to higher false-positive rates among women and ethnic minorities.(2) These patterns raise concerns that FRT could inadvertently perpetuate historical biases, affecting marginalized communities and potentially contributing to issues of over-policing and racial profiling. Judicial reviews and due diligence assessments have begun to address the legal and ethical implications of FRT in law enforcement, as seen in cases such as R (Bridges) v Chief Constable of South Wales Police in the UK. These cases underscore the importance of

(1) Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power (p. 94). PublicAffairs. Retrieved from Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power | Social Forces | Oxford Academic (oup.com)

(2) Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power (p. 94). PublicAffairs. Retrieved from Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power | Social Forces | Oxford Academic (oup.com)

developing robust legal frameworks and governance mechanisms to guide FRT's responsible and ethical deployment.

This study aims to explore the need for balanced, rights-based approaches to FRT regulation, emphasizing the importance of frameworks that protect civil liberties while enabling law enforcement to benefit from technological advancements responsibly.

Research Methodology:

This research employs a doctrinal legal methodology, focusing on a comparative analysis of UK and EU legal frameworks regulating facial recognition technology (FRT). Primary sources include recent legislation, judicial rulings, and independent policy reports. Analytical insights draw from proportionality and human rights impact assessments, providing a balanced view regarding FRT's role in policing versus privacy concerns.

Chapter 1: Facial Recognition Technology in Law Enforcement

This chapter aims to provide a comprehensive understanding of FRT, its historical development, and its current applications in law enforcement within the UK and Europe.

What is Facial Recognition Technology?

Facial recognition may be reckoned as a cutting-edge system in biometric identification. Computer algorithms are used to match and analyze facial features from digital images or video streams against the features of known faces from a database. Sequel processing stages take place during the face detection algorithms, which identify human faces in the image or within a video field sequence frame. Feature extraction algorithms weigh and encode unique attributes found on each face, including eye distance, nose shape,

and jawline contours. The encoded features are then compared against a pre-existing database of facial data to search for potential matches.(1)

Distinguishing Facial Recognition from DNA Evidence in Criminal Identification:

Facial recognition and DNA evidence, while both used for individual identification in criminal cases, differ significantly in nature and application. DNA evidence, being biological and hereditary, offers broader functionality beyond identification, including determining parentage, aiding in immigration cases, and identifying victims of disasters. Facial recognition, primarily based on external features, is less influenced by genetics. The methods of proof also differ, with facial recognition relying on external shape analysis, while DNA evidence involves analyzing genetic material. These distinctions highlight DNA evidence's wider scope and potentially higher reliability in various forensic applications compared to facial recognition.(2)

Historical Background and Development

The history of modern face recognition is traced back to the work of Lawrence, Osuna, and Cohn in the 1960s, conducted at Stanford University's Pattern Recognition Laboratory, in which a computer algorithm is proposed to recognize human faces.(3) Necessary steps were taken in the late 1980s

(1) Ullah, N., Javed, A., Ghazanfar, M. A., & Alsufyani, A. (2022). A novel DeepMaskNet model for face mask detection and masked facial recognition. Journal of King Saud University - Computer and Information Sciences. Retrieved from https://www.sciencedirect.com/science/article/pii/S1319157821003633

(2) Al-Sharjah University Journal of Legal Sciences. (n.d.). The role of facial recognition as evidence in criminal prosecution in UAE law. Retrieved from https://slj.sharjah.ac.ae/

(3) Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the gap

and early 1990s toward accuracy and efficiency by creating the eigenface and fisher face algorithms(1)

It was around the early 2000s when both digital cameras and the internet picked up. This opened the doors to massive proliferation in digital image data and led to more development in newer, more sophisticated facial recognition algorithms. The most recent machine learning techniques, in particular deep learning with convolutional neural networks, have enabled much greater accuracy and robustness for facial recognition systems.(2)

Applications in Law Enforcement

Recently, UK law enforcement authorities and other European nations have applied this technology to increase public safety and help in criminal investigations. Some of the main areas in which this technology is employed are:

- Facial recognition technology and implementation follow the offenders with the help of video recordings or images found at the scenes of various crimes, which in turn help the Police Department clean up its investigations with the apprehension of criminals based

to human-level performance in face verification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 1701-1708). Retrieved from DeepFace: Closing the Gap to Human-Level Performance in Face Verification | IEEE Conference Publication | IEEE Xplore

(1) Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J. (1997). Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7), 711-720. Retrieved from Eigenfaces vs. Fisherfaces: recognition using class specific linear projection | IEEE Journals & Magazine | IEEE Xplore

(2) Alkishri, W., Widyarto, S., Yousif, J. H., & Al-Bahri, M. (2023). Fake face detection based on colour textual analysis using deep convolutional neural network. Journal of Internet Services and Information Security, 13(1), 67-85. Retrieved from https://jisis.org/wp-content/uploads/2023/08/2023.I3.009.pdf

on a background check.

- The technology is often widely applied within such grounds as monitoring mass events, crowded places, and entryways into various areas.
- It is used for the search and identification of missing persons matched with their facial data against reported missing persons' databases, including children and vulnerable people.
- FRT systems could find an application in the processes of border control and immigration in checking personal identity against databases containing information related to known travelers and possible security risks, among others.(1)

The use of FRT by law enforcement is highly controversial and legally contested in the UK. The Metropolitan Police Service has been one of the leading adopters of live facial recognition technology for public events and crowd monitoring in London.(2) However, civil liberties organizations and privacy advocates for justifying potential biases and disproportionate impacts on the communities of color, as well as the lack of a comprehensive legal framework on the use of FRT.(3)

(1) Trilateral Research. (2021, October 18). Facial recognition technology as a measure to enhance public safety. Retrieved from https://trilateralresearch.com/data-governance/facial-recognition-technology-as-a-measure-to-enhance-public-safety

(2) Metropolitan Police Service. (n.d.). Facial recognition technology. Retrieved June 7, 2024, Retrieved from https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition-technology/

(3) Privacy International. (2023, November 7). UK MPs asleep at the wheel as facial recognition technology spells end of privacy in public. Retrieved from https://privacyinternational.org/long-read/5155/uk-mps-asleep-wheel-facial-recognition-technology-spells-end-privacy-public

FRT adoption by the central law enforcement agencies in European jurisdictions remains uneven. Indeed, countries are adopting such technologies at different paces. Only in 2021 did the Commission of the European Union publish a proposition for an EU-wide regulation(1) that would deal comprehensively with AI, including clauses for the use of FRT within law enforcement settings. The regulation seeks to strike an equilibrium balance between stimulating innovations and protections in essential rights and values, notably personal privacy and nondiscrimination.(2) It would, therefore, be interesting to keep abreast of some of the legal, ethical, and societal concerns that face FRT use, mainly when deployment happens or goes further in law enforcement settings.

Chapter 2: Privacy and Civil Liberties Implications of FRT Surveillance.

The use of facial recognition technology in law enforcement has drawn heated debates and scrutiny based on the potential impact it may have on individual privacy and civil liberties. Proponents claim that technology is highly efficient in terms of securing public safety and security, while critics raise essential concerns about fundamental rights and possible misuse or abuse. The chapter now turns to these multi-faceted privacy and civil liberties considerations with the use of FRT in mass surveillance by state agencies, most notably in the UK and Europe.

(1) European Commission. (2021). Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Retrieved from https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

(2) Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU artificial intelligence act — analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International, 22(4), 97–112. Retrieved from Demystifying the Draft EU Artificial Intelligence Act by Michael Veale, Frederik Zuiderveen Borgesius :: SSRN

Lack of Consent and Invasion of Privacy

The most significant issue in facial recognition technology for law enforcement is the lack of consent and notification when conducting observations and identifications in the streets or any public area without the person's permission. The practice has been very much condemned, as it is against individual privacy rights secured by Data Protection and Privacy Laws, such as the General Data Protection Regulation in Europe. The mass and wide use of FRT without discretion takes away the reasonable expectation of anonymity that people otherwise can enjoy in public spaces. Historically, public privacy was a fundamental human right by which one could move and act in public without fearing that every moment is being surveyed and without the possibility of continuous identification.(1) Wherever FRT is used without explicit consent, it deprives the person of the power to choose to disclose personal information and their identity, leading to substantial ethical and legal considerations.(2)

Privacy is more than simply protecting personal information; it also involves control over identity and personal data disclosures and the right to choose their exposure and use. Therefore, uncontrolled use of FRT in public spaces leads to potential data misuse and erosion of fundamental privacy rights. All this becomes more distressing with biometric data that cannot be replaced or renewed easily.(3) Lastly, its surreptitious use may

(1) Solove, D. J. (2008). Understanding privacy (p. 74). Harvard University Press. Retrieved from Understanding Privacy by Daniel J. Solove :: SSRN

(2) Crawford, K. (2021). Atlas of AI: Power, politics, and the planetary costs of artificial intelligence (p. 109). Yale University Press. Retrieved from: The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence on JSTOR

(3) Hartzog, W. (2018). Privacy's blueprint: The battle to control the design of new technologies (p. 203). Harvard University Press. Retrieved June 7, 2024, from: Privacy's

also lead to privacy and ethical concerns. It breaches the fundamental right to privacy and control that people have over their data, with risks of misuse and erosion of public trust in law enforcement.

Chilling Effects on Freedom of Assembly and Expression

Critics argue that the extensive use of FRT by law enforcement agencies would have a "chilling effect" on exercising fundamental rights, such as freedom of assembly, association, and expression.(1) The awareness of the potential surveillance and identification of people at protest sites or political rallies likely scares people away, thereby promoting a chilling effect in the absence of any impact or response.(2)

Numerous studies suggest that the presence of surveillance can be enough to lead to changes in behavior. This effect has been well-documented across many scenarios, from workplace surveillance to online activities and public spaces. For instance, the American Civil Liberties Union (ACLU) quoted some studies showing how surveillance can scare people from political protests or taking part in activist movements for fear of being out and victimized for doing so.(3)

Blueprint: The Battle to Control the Design of New Technologies on JSTOR

(1) Garvie, C., Bedoya, A., & Frankle, J. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology. Perpetual Line Up - Unregulated Police Face Recognition in America

(2) Browne, S. (2015). Captured and exposed: Why privacy matters. In J. van den Hoven, P. E. Vermaas, & I. van de Poel (Eds.), Handbook of ethics, values, and technological design (pp. 291-314). Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains | SpringerLink

(3) American Civil Liberties Union (ACLU). (2019). The chilling effect of surveillance. Retrieved from: Privacy and Surveillance | American Civil Liberties Union (aclu.org)

Another particular concern is the implication that this has for political participation. Public discussion and free assembly are considered the absolute basis for democratic societies. If people get the sense that involvement in protests rallies, or political gatherings of any sort could come back to haunt them, they might be dissuaded from involvement to begin with. This self-censorship undermines democracy by weakening the range of voices and opinions in public discourse. A report by the Berkman Klein Center for Internet & Society at Harvard University found that the mere awareness of surveillance causes people to shy away from discussing matters of concern over the internet that could be seen as controversial.(1) It further extends to avoidance, even at the level of physical spaces, in that knowledge of the use of FRT may cause an individual to avoid attending events in places that may be critical of government policy or places that may circulate their dissenting view. The freedom to express an idea of freedom for every single human is assured in several international human rights standards, the first one being the Universal Declaration of Human Rights and the second one being the European Convention on Human Rights. FRT directly undermines this, though, because it creates a situation where one may fear speaking one's mind. Indeed, such fear is not unfounded since some surveillance data have been used to track and target activists and dissidents.

The other impacts of this extend beyond the physical, which includes those impacts on political activity and freedom of speech. There is a high probability that in such a situation, constant monitoring can induce

(1) Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. Berkeley Technology Law Journal, 32(2), 1175-1230. Retrieved from Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study by Jon Penney :: SSRN

vulnerability and powerlessness on the part of an individual, which might be eventuated in anxiety and stress. This sense of surveillance can induce high alertness, making people shy away from routine social interactions and activities geared toward community life. (1)

However, this is a huge risk, posing fundamental alterations to several core democratic values and personal liberties while law enforcement agencies use this for enhanced public safety. This is likely to extend further to create chilling effects on political participation and self-censorship, undermining the very same democratic processes and rupturing individuals' rights to privacy and freedom of expression. Thus, there needs to be legal solid frameworks concerning the use of FR technology involving transparency and public oversight at societal levels or risk this system infringing on civil liberties.

Bias, Discrimination, and Disproportionate Impacts

The most intense controversy about facial recognition technology is around bias and discrimination in its use, linking it with multiple fields, most notably law enforcement. Probably the most critical issue is the potential for FRT to yield higher error rates and biased outcomes, in particular when identifying women and people from ethnic minorities. Some factors that may introduce the biases encompass the nature of training data and the environments within which the technology is applied. These show that FRT systems report differing rates of accuracy about the characteristics of people. For example, Buolamwini and Gebru (2018) demonstrated that facial analysis algorithms tended to have higher error rates when the

(1) Mac, R. (2020, July 8). What constant surveillance does to your brain. VICE. Retrieved from https://www.vice.com/en/article/pa5d9g/what-constant-surveillance-does-to-your-brain

subjects considered were women and darker-skinned compared to male and lighter-skinned individuals. This is mainly because datasets used to train these systems are generally more biased towards light-skinned male faces.(1)

Conditions like low lighting or degraded images may, therefore, cause extra bias. This is especially a problem within law enforcement contexts where high, militarily-based stakes ride on FRT-based decisions. There are instances, for example, in which identification errors have caused wrongful arrests and legal action, catalyzing further system-wide bias against marginalized communities (poor communities as an example).(2)

The realization of FRT, as available information shows, causes disproportionate harm to communities already biased against it. It raises deeply embodied aspects concerning equality and non-discrimination. The international human rights law and conventions focus on the general concepts in all life forms: equality and non-discrimination.(3)This goes broadly or falls in violation of individuals' rights under race, gender, or ethnicity, provided through deploying the FRT systems that come with prejudice, which result in violations of them. Therefore, FRT can introduce more trouble into these communities through backed ways of life, creating social inequalities and prejudices. This then means over-surveillance and

(1) Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 1-15. Retrieved from Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification — MIT Media Lab

(2) Garvie, C., Bedoya, A., & Frankle, J. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology. Retrieved from https://www.perpetuallineup.org/

(3) United Nations. (1966). International Covenant on Civil and Political Rights. Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

policing of the affected populations more than the others; thus, human beings are ordinal to these biases. Over-surveillance could lead to many results, ranging from increased incidences with law enforcers to low levels of trust in public institutions to growing feelings of alienation.(1)

The current bias is also exaggerated in several ways by introducing FRT into police practices. First, if FRT is deployed in geographic areas highly populated by ethnic minorities, such a decision naturally over-surveys them and leads to reinforcing the stereotyping and discrimination even more. Secondly, biased outcomes from the use of FRT could potentially lead to the influence of policing strategies, hence propagating racial profiling and other discriminatory law enforcement practice approaches. Worse, feedback loops generated by biased data may only exacerbate the problem at hand. With more agencies using FRT, data generated by these systems, which might already be prejudiced, are fed back into the system used to train the technology, thereby strengthening and magnifying these previous disparities.(2)

Ethically, this may mean considering the broader societal implications of FRT use. Guaranteed sources of diverse and representative training data are crucial to curbing these biases. Besides, it has also been determined that techniques like Cluster Analysis (CA) and Confirmatory Factor Analysis

(1) Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. NYU Law Review, 94(2), 192-233. Retrieved from Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice by Rashida Richardson, Jason Schultz, Kate Crawford :: SSRN

(2) Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1–15. Retrieved from https://proceedings.mlr.press/v81/buolamwini18a.html

(CFA) may also help bring bias to realization, and any discriminatory feature in FRT should be corrected to ensure that the technology does not to aid discrimination.(1) This potential for bias and discrimination within facial recognition technology raises significant challenges, especially for vulnerable populations. These challenges require efforts to develop and deploy FRT systems in ways that respect principles of equality and non-discrimination. In doing so, one has to pay particular attention to having legal solid frameworks, ethical guidelines, and continuous scrutiny that help avoid the magnification of already existing biases and the protection of the rights and freedom of everyone.

The Erosion of Privacy: Function Creep and Anonymity Risks The big problem with FRT is what's often called "function creep." By "function creep," I mean that what is allowed for specific, narrow security purposes expands and extends into more generalized and broader surveillance activities. Frequently, this happens without much attention and public oversight, leading to wide-ranging privacy harms. Integrating FRT into multiple surveillance systems and databases enables mass tracking of movements, associations, and activities of people. This all-pervasive surveillance infringes upon privacy rights and can extend massive monitoring with data accumulation on an unprecedented scale.

Legal scholars, however, have underlined a breach in the main principle of "obscurity" in unfettered facial recognition surveillance. Obscurity implies that the individual can expect not to be identified or remain anonymous in their transactions within public areas. The erosion of such

(1) Suresh, H., & Guttag, J. V. (2020). A framework for understanding unintended consequences of machine learning. Communications of the ACM, 64(2), 62-71. Retrieved from : [1901.10002v3] A Framework for Understanding Unintended Consequences of Machine Learning

a principle through the deployment of FRT could fundamentally alter the open and accessible nature of public regions. This will set up new thresholds of personal privacy, most likely creating a "surveillance society" in which people are under constant monitoring.(1)

Anonymity in public space has been cherished for a long time as part of one's freedom and privacy. Anonymity allows persons the freedom to move and wander, free to do whatever is rightful, and to express themselves without fear of surveillance and identification. The massive use of FRT for surveillance would negate that right since it will subject people to identification and probable tracking without their will or knowledge.(2)

The ability for an individual to remain unidentified and obscure, often referred to as public obscurity by legal scholars and privacy advocates, is an important privacy defense. This principle is critical to protecting the openness of public spaces and how people can participate in public life, free of unwarranted surveillance. The ubiquity of FRT undermines this principle, resulting in a massive shift in how public spaces operate and opening the doors for a surveillance society.(3) However, function creep is not limited to breaches of privacy and has wider societal consequences. As FRT is integrated with more sorts of surveillance, it could also be used for

(1) Kerr, O. S. (2009). The Fourth Amendment and the global Internet. Stanford Law Review, 62(1), 1005–1054. Retrieved from: The Fourth Amendment and the Global Internet on JSTOR

(2) Brayne, S. (2020). Predict and surveil: Data, discretion, and the future of policing (p. 87). Oxford University Press. Retrieved from: Predict and surveil: Data, discretion, and the future of policing, by Sarah Brayne: A review by Karolina La Fors - Karolina La Fors, 2021

(3) Taylor, L., Floridi, L., & Van der Sloot, B. (Eds.). (2017). Group Privacy: New Challenges of Data Technologies. Springer. Retrieved From: Group Privacy: New Challenges of Data Technologies | SpringerLink

cases far away from the initial concept, such as to identify political activists, monitor public gatherings (by police or private companies), or maybe even commercial data harvesting. This prolonged use could undermine public trust and create a scenario where the state power can be potentially abused or privacy rights violated.(1)

Compounding this are concerns surrounding the unchecked use of FRT, with little transparency in how it is regulated and minimal accountability over application. In the absence of clear rules and procedural safeguards, it is possible that FRT may be used at the whim of law enforcement and other interests to the detriment of individual rights. It should be an especially troubling fact in democratic societies, where the preservation of civil rights is so emphasized.(2) You need to use tough legal frameworks and oversight mechanisms to protect the concept of public obscuration. Regulations must ensure that the use of FRT is fair, accountable and proportionate to the security goal. Through public consultations and impact assessments, authorities can identify the range of risks and benefits and in some cases realise suitable ways to demonstrate and enlighten the public on how FRT is used in a manner that respects individual privacy and civil liberties.(3)

(1) Lyon, D. (2007). Surveillance Studies: An Overview. Cambridge: Polity Press. Retrieved From:Surveillance studies : an overview : Lyon, David, 1948- : Free Download, Borrow, and Streaming : Internet Archive

(2) Richards, N. M. (2013). The dangers of surveillance. Harvard Law Review, 126(7), 1934-1965. Retrieved from The Dangers of Surveillance by Neil M. Richards :: SSRN

(3) European Commission. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Chapter 3: Comparative Analysis of UK and European Regulatory Approaches.

With advancements in this technology and its growing adoption, it is imperative to look out for the legislative and regulatory pathways being pursued by various jurisdictions. This chapter conducts a comparative analysis of the regulatory developments and policy approaches guiding law enforcement use of FRT in the UK vs the EU, underscores the main contrasts, and maps potential lacunae.

United Kingdom - Mosaic of Current Laws and Principles

However, there is no one piece of national legislation in the UK that specifically governs the use of live facial recognition by law enforcement. Rather, some existing laws and human rights principles oblige police forces when deploying FRT:

1. Protection of Freedoms Act 2012: Provides a general statutory basis for police surveillance systems including closed-circuit television (CCTV) and automatic number plate recognition (ANPR). However, its breadth may not cover live facial recognition as a new and unique challenge.(1)

2. Data Protection Act 2018 (adopting GDPR): The UK's data protection regime, in line with the EU's General Data Protection Regulation (GDPR), requires face data processing to subscribe to principles like purpose limitation, data minimization, transparency,

(1) McCahill, M., & Finn, R. L. (2018). Surveillance, capital and resistance: Theorizing the surveillance subject (p. 152). Routledge. Retrieved from : Surveillance, Capital and Resistance: Theorizing the Surveillance Subject | Request PDF

non-discrimination.(1)

3. Human Rights Act 1998 - incorporates the European Convention on Human Rights into UK law, entrenching principles of privacy, freedom of expression and protection against discrimination. These are demonstrations of the rights that police forces must uphold in their usage of FRT.(2)

4. The Equality Act 2010, which protects against discrimination by a public authority on the grounds of race or sex, has implications for bias and accuracy issues in FRT systems.(3)

There are exposed gaps and uncertainties in the current UK laws when it comes to regulating the use of FRT by law enforcement. The key case in this regard is the judgment of the Court of Appeal in Ed Bridges v. South Wales Police (2020) which considers several of the most important questions about FRT.

(1) Data Protection Act 2018, c. 12. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(2) Human Rights Act 1998, c. 42. https://www.legislation.gov.uk/ukpga/1998/42/contents

(3) Equality Act 2010, c. 15. https://www.legislation.gov.uk/ukpga/2010/15/contents

Background of the Case

The case was brought by Ed Bridges, a former Liberal Democrat councilor and civil liberties campaigner, who had his face scanned twice by South Wales Police's live facial recognition technology. It was in Cardiff city Centre the first time and at an entirely peaceful protest the second. Mr. Bridges claimed that the South Wales Police's use of FRT was unlawful and a breach of his rights under the European Convention on Human Rights (ECHR), such as Article 8 (right to a private life) and 10 (freedom of expression) in particular.

In August 2020, the Court of Appeal(1) found in favour of Ed Bridges on several important grounds:

1. No Clear Legal Basis: The court concluded that the use of the technology by the South Wales Police did not have a clear specific law. The lack of a specific legal framework led people to be unable to predict when and in what situations someone may process their biometric data.

2. Insufficient Safeguards: The case found that there were insufficient safeguards to ensure that FRT is used in a way that is both proportionate and to prevent arbitrary interference with an individual's privacy rights. The court also condemned the absence of independent oversight and the lack of clear guidance about where and when FRT could be used.

3. Proportionality: The court doubted whether the use of FRT by South Wales Police satisfied the necessity and proportionality test under

(1) Court of Appeal. (2020). Ed Bridges v. South Wales Police. Retrieved from Microsoft Word - R (Bridges) -v- CC South Wales _ors Judgment.docx

human rights law. The government failed to establish that it could not have achieved its objectives through less invasive means.

While the court did not rule discrimination was the prevailing factor in this instance, it was noted that it has an effect that is important to evaluate and prevent thorough holistic screenings.

European Union: The Artificial Intelligence Act (AI Act)

The European Union has introduced a comprehensive regulatory approach to the management of AI technologies, including facial recognition technology (FRT), through the Artificial Intelligence (AI) Act, formally designated as Regulation (EU) 2024/1689. The Act establishes comprehensive, risk-based regulations governing the deployment of AI across the EU, with particular emphasis on high-risk applications such as FRT in law enforcement. The overarching objective of the AI Act is to strike a balance between the benefits of AI innovation and the protection of fundamental rights, including privacy and non-discrimination.(1)

Key Provisions of the AI Act for FRT in Law Enforcement

The AI Act explicitly categorises real-time remote biometric identification (RBI) systems, which include FRT in public spaces by law enforcement, as high-risk AI systems. Consequently, these systems are subject to rigorous regulatory oversight and are typically prohibited, except in limited circumstances where their use is deemed indispensable. The permissible applications of RBI are circumscribed, and its use in public spaces is permitted only when it is necessary for:

(1) European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonized rules on artificial intelligence (AI Act). Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1689/oj

- The use of such systems may be permitted in cases where the objective is to locate missing persons or victims of human trafficking.
- The prevention of imminent threats to life or physical safety, such as terrorist attacks.
- The identification of suspects in serious criminal activities, including but not limited to murder, armed robbery, and organised crime.

In such high-stakes scenarios, the AI Act mandates a comprehensive assessment of the potential impact on fundamental rights prior to deployment. This ensures that the utilisation of FRT by law enforcement is in alignment with the rights and freedoms of individuals affected. In situations of emergency, deployment may proceed without prior registration or judicial approval, provided that authorisation is sought within 24 hours and all relevant data is duly documented and registered in the EU database.

Compliance, Oversight, and Accountability

In order to mitigate the risks associated with high-risk AI, the Act sets out the following compliance measures:

- The necessity for human oversight is paramount. It is incumbent upon law enforcement personnel to maintain direct oversight over FRT operations, thereby ensuring that human judgement remains central to decision-making.
- Risk Management and Data Integrity: It is incumbent upon AI providers and deployers to implement robust risk management practices, including quality checks on datasets, with the objective of preventing bias and ensuring representativeness.

- Third-Party Conformity Assessments It is imperative that high-risk AI systems, including FRT, undergo evaluations by independent third parties to verify compliance prior to deployment.
- It is essential to implement an ongoing monitoring and reporting system. The deployment and impact of FRT will be subject to continuous monitoring by the relevant regulatory authorities, who will require any deployers to report any serious incidents or instances of non-compliance in a timely manner.

Furthermore, the regulation delineates the penalties for non-compliance, thereby reinforcing the significance of adherence to the established standards for transparency, accountability, and security in the deployment of FRT systems.

A Human Rights-Centred Approach

The AI Act serves to illustrate the European Union's commitment to the protection of human rights, as evidenced by the rigorous governance structure that has been put in place with regard to the deployment of FRT systems. The stipulations of the Act give precedence to the rights to privacy, non-discrimination, and transparency. This rights-based approach guarantees that FRT applications are meticulously regulated, employed exclusively when indispensable, and in accordance with the ethical standards of society.

Disparities and Gaps in Regulatory Strategies

The regulatory approaches of the UK and the EU to facial recognition technology (FRT) diverge significantly in terms of both philosophy and methodology. This reflects the differing priorities of the two jurisdictions in addressing the challenges associated with the use of FRT in law enforcement and the private sector. The EU, through Regulation (EU) 2024/1689, implements a preventive, rights-based approach, whereas the UK predominantly follows a reactive model based on judicial oversight.(1)

In the United Kingdom, the deployment of FRT is subject to an ex-post judicial review system that relies on existing human rights and privacy laws, which are evaluated in cases as they arise. The Ed Bridges v. South Wales Police case exemplifies the difficulties inherent in this approach, as courts addressed concerns about privacy, transparency, and oversight only after the technology had already been deployed. This case-by-case approach is in stark contrast to the EU's forward-thinking strategy, as set forth in the AI Act, which establishes ex-ante regulatory standards for high-risk AI applications, including FRT. This ensures that specific, predefined requirements are met before any deployment.

The United Kingdom's approach to the use of force technology (FRT) by law enforcement lacks comprehensive legal frameworks that specifically govern the procurement, deployment, and auditing of FRT by law enforcement agencies. This regulatory gap places law enforcement in a legal grey zone, increasing the risk of rights violations as the technology

(1) Almeida, D., Shmarko, K., & Lomas, E. (2022). 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, 377–387. https://doi.org/10.1007/s43681-021-00077-w

is deployed without statutory guidance on oversight, data protection, or usage limits. In the absence of clear statutory metrics, there is a risk of what is known as 'function creep' in the UK, whereby FRT could be expanded beyond its original intent, allowing surveillance to grow without transparency or public accountability.

In contrast, the EU's AI Act establishes rigorous controls and oversight for the utilisation of FRT in law enforcement. The use of remote biometric identification (RBI) systems, including real-time FRT, is generally prohibited in public spaces, except in narrowly defined situations where there is a serious crime or imminent threat to life and safety. Prior to deployment, EU law enforcement is required to complete a fundamental rights impact assessment and to obtain judicial or administrative authorisation, thereby reinforcing a proactive commitment to the protection of privacy and data. In the event of an emergency, deployment may proceed without immediate registration or authorisation, but must be duly documented and approved retrospectively, thereby introducing an additional layer of accountability.

Moreover, the AI Act incorporates stipulations pertaining to the necessity of third-party assessments for high-risk systems, the implementation of mandatory oversight, the requirement for human intervention, and the undertaking of continuous monitoring to guarantee the sustained compliance of all parties involved. These safeguards serve to prevent the unchecked expansion of FRT and to protect civil liberties by enforcing high standards of transparency and oversight, which are largely absent from the UK's current legal structure.

Additionally, there are notable differences between the UK and EU frameworks with regard to the treatment of private-sector FRT. While the EU Act provides rigorous oversight of private sector high-risk AI applications, including in domains such as employment and finance, the UK's absence of specific regulations for private FRT deployments has resulted in the emergence of significant loopholes. The absence of restrictions on the use of FRT by private companies in the UK may result in the exploitation of this regulatory gap, leading to potential violations of privacy and the emergence of commercial surveillance practices.

This comparative analysis demonstrates that the EU's structured, rights-centred model represents a robust approach to regulating FRT, with a particular focus on civil liberties through proactive measures. The UK's reliance on judicial review serves to highlight the substantial regulatory lacunae that exist, particularly in light of the ongoing concerns surrounding the issues of function creep and lack of oversight in the private sector. In the future, it would be advantageous for both jurisdictions to harmonise their regulatory frameworks in order to achieve a more balanced approach between security and individual rights, and to address the increasing implications of AI-driven surveillance.

Chapter 4: Judicial Perspectives and Independent Impact Assessments

While judicial rulings and independent impact assessments have been pivotal in unpacking the legal and ethical implications of this technology, the interpretation of FRT use by law enforcement raises a lot of concern over the potential violations of fundamental freedoms and guarantees of individual rights. This chapter considers the views of key court cases in the UK and the EU, as well as independent studies and opinions of experts, thereby offering an explanation of the difficulties identified as well as potential risks related to the deployment of FRT for law enforcement use.

Judicial Perspectives from Court Rulings

- UK Court Rulings:

R (Bridges) v. Chief Constable of South Wales Police [2020] EWCA Civ 1058 is a landmark case scrutinizing the use of facial recognition technology (FRT) by law enforcement in the UK. The decision by the Court of Appeal to find in favour of privacy and human rights in the case relating to the South Wales Police use of automated FRT in public space highlighted profound legal and ethical problems inherent to the deployment of such surveillant technologies.

The Court of Appeal found that the deployment of FRT by South Wales Police suffered from several fatal flaws:

1. The court wrote the existing laws did not give enough "content, detail, legislation, guidance, or authority," for the privacy infringements of the FRT. The tech's ability to collect biometric data in public spaces

warrantedheightenedscrutinyandprotection.[1]

2. As no statutory codes of practice or other binding guidance, there was no guidance to address key issues such as getting personal data without consent. This lack prevented a set of rules on how the companies needed to collect, process, and store data, bringing huge privacyissues.[2]

3. The watch lists themselves were secret, the accuracy of the databases used could not be verified by the public, and no error rate for false positives was specified. This lack of transparency left open questions about the accountability and the trustworthiness of FRT systems deployed by the police.

4. Significantly, the UK court noted there was not an express legislative requirement for Data Protection Impact Assessment DPIAs to be carried out, which played a major part in identifying and minimizing privacy risks associated with the use of FRT in advance of deployment. DPIAs help to make sure the use of such deep-dive technology is necessary and in line with the intended purpose (Information Commissioner's Office, 2020).

5. The verdict slammed the limited steps taken to inform the public about where and when FRT was being used, and by whom. To

(1) Court of Appeal. (2020). R (Bridges) v. Chief Constable of South Wales Police. Retrieved from https://www.judiciary.uk/wp-content/uploads/2022/07/R-Bridges-v-CC-South-Wales-ors-Judgment-1.pdf

(2) Information Commissioner's Office. (2020). Guidance on data protection impact assessments (DPIAs). Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

maintain trust and keep the deployment of surveillance technology transparent and accountable, effective public engagement is a must.

The judgment of the Court of Appeal in R (Bridges) v. Chief Constable of South Wales Police established what the future holds for the use of FRT by law enforcement in the UK. The ruling made it clear that the practices of today are illegal but it is for the present UK Parliament to create a proper legal structure instead. It would need to be based on the protection of fundamental rights, with corresponding safeguards, which could mean a change in the way that FRT is currently regulated and used. The judgment reinforced the importance of a robust legal framework, greater transparency and public participation, and the necessity of Data Protection Impact Assessment.

EU Court of Justice Rulings

The decisions of the CJEU with regard to biometric monitoring techniques, including facial recognition technology (FRT), highlight the necessity for the implementation of robust privacy protection and adherence to fundamental rights. The rulings of the CJEU reflect the necessity for executive and legislative bodies in member states to guarantee that biometric surveillance is conducted in accordance with established standards of data protection and does not result in arbitrary infringements of personal rights. By interpreting EU legislation and the Charter of Fundamental Rights, the CJEU plays a pivotal role in strengthening privacy protections, delineating boundaries on the deployment of surveillance technologies, and mandating compliance in order to prevent unwarranted intrusions. Key judgments include:

- Cases C-511/18 and C-512/18: In these cases, the CJEU stressed that "any measures that entail the processing of biometric data to identify individuals in public spaces must be governed by clear, precise, and accessible rules." The court further emphasized the need for member states to define both the "material and formal conditions" for such processing to ensure "sufficient clarity and precision" in the law and to prevent "any arbitrary interference with the fundamental rights to privacy and data protection." This judgment highlights the importance of strong legal frameworks and oversight to provide both legal certainty and protection against rights violations.(1)

- Case C-623/17: In this case, the CJEU ruled that "the deployment of facial recognition technology in public spaces must comply with data protection principles, particularly necessity and purpose limitation." Furthermore, the court specified that "exceptions to these principles must pursue a legitimate interest and be free from discriminatory outcomes based on race, colour, or ethnic origin." This judgment underscores the requirement that any use of FRT be "justified, proportionate, and transparent," emphasizing the need for strict adherence to data protection regulations to prevent misuse and discrimination.(2)

(1) CJEU (Court of Justice of the European Union). (2020). Joined Cases C-511/18 and C-512/18. Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-511/18

(2) CJEU (Court of Justice of the European Union). (2019). Case C-623/17. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0623

It is clear from the continued jurisprudence of the CJEU that overarching facial recognition surveillance programmes, bereft of supervision and judicial oversight, are found wanting in the protection of privacy, data protection and non-discrimination as remitted in the bosom of the EU legal order.

Some Recommendations:

Legal and Regulatory Reforms

1. It is of the utmost importance that appropriate legislation and clarity on the use of force by law enforcement agencies (LEAs) be enacted. A comprehensive framework should be based on the fundamental principles set forth in human rights legislation, including:

- The necessity of such legislation is clear. The deployment of FRT should be restricted to instances where it is indispensable for law enforcement operations.
- Proportionality is a key principle that must be adhered to in the deployment of FRT. It is imperative that the advantages of FRT utilization outweigh the potential infringements on privacy, thereby ensuring a minimal impact on individuals' rights.
- The principle of purpose limitation stipulates that any surveillance system must be deployed for a specific and defined purpose. The deployment of FRT should be limited to specific, clearly defined objectives, and not extended to broader, undefined surveillance.
- The principle of non-discrimination must be upheld. It is imperative that safeguards be put in place to prevent any discriminatory outcomes or biases in the application of FRT based on race, gender,

or other protected attributes. These principles guarantee that the utilisation of FRT is in accordance with fundamental rights and in compliance with international human rights standards.(1)

2. Enable accountability and the rule of law: Robust judicial oversight, defined as a comprehensive system in which courts are responsible for authorising, monitoring and reviewing the use of facial recognition technology (FRT), should govern the authorisation, oversight and review of FRT applications. This judicial oversight will ensure that the use of FRT remains lawful, necessary, and proportionate, while providing a pathway for individuals to challenge misuse and seek redress, thereby ensuring compliance with human rights and privacy standards.(2)

3. Deployment of facial recognition technology (FRT) systems should be governed by a legal framework that mandates data protection and equality impact assessments prior to implementation. These assessments should evaluate the potential for bias, adverse externalities, and risks to human rights.(3)

(1) 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 USA, EU and UK regulatory frameworks. SSRN. The Ethics of Facial Recognition Technologies, Surveillance and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of USA, EU and UK Regulatory Frameworks by Denise R. S. Almeida, Konstantin Shmarko, Elizabeth Lomas :: SSRN

(2) Fussey, P., & Murray, D. (2019). Independent report on the London Metropolitan Police Service's trial of live facial recognition technology. Retrieved from: Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology - Research Repository (essex.ac.uk)

(3) Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intely

4. Strict transparency measures, like formal transparency obligations to disclose information about the intended use of FRT, how it is used and the sources of the data help maintain transparency and trust with the public.(1)

5. The framework should regulate the types of sources watchlists can come from when used in FRT systems; it should set up accuracy standards; and it should ban certain forms of data collection to ensure that privacy rights are respected and that data harvesting practices are not exacerbating bias.(2)

6. Including the perspective of the affected population, in line with their fundamental rights, should be a must, derived from broad public consultations, if inclusive and participative governance does play a central role in policymaking.(3)

Considerations for the Arab and Islamic Law Context

ligence Act. Computer Law Review International, 22(4), 97 Demystifying the Draft EU Artificial Intelligence Act by Michael Veale, Frederik Zuiderveen Borgesius :: SSRN

(1) Yeung, K., & Bygrave, L. A. (2021). Demystifying the modernized European data protection regime: Cross-disciplinary perspectives. Semantic Scholar. Retrieved from Demystifying the modernized European data protection regime: Cross□disciplinary insights from legal and regulatory governance scholarship

(2) Garvie, C., Bedoya, A., & Frankle, J. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology. Retrieved From: The Perpetual Line-Up - Center on Privacy and Technology at Georgetown Law - 121616.pdf (perpetuallineup.org)

(3) Ada Lovelace Institute. (2022). Regulating biometric data for current and future public benefit: Reviewing live facial recognition technology in UK public spaces. https://www.adalovelaceinstitute.org/report/regulating-biometric-data/

In jurisdictions with Islamic cultural and legal foundations, such as the UAE, the implementation of FRT necessitates the consideration of additional factors to ensure alignment with Islamic principles of privacy, dignity, and fairness. This encompasses the following:

1. Respect for Islamic principles on privacy(1) and dignity is of paramount importance. The tenets of Islamic law place significant emphasis on the dignity and privacy of the individual, which may present a challenge when considering the use of continuous surveillance. It is of the utmost importance that FRT applications are subjected to rigorous scrutiny with regard to settings such as public and religious spaces, with a view to ensuring that they respect the aforementioned principles.

2. Religious Oversight and Ethical Guidance: In light of the distinctive ethical stance espoused by Islamic law, the input of Islamic scholars or religious legal experts in the oversight process may prove instrumental in fostering greater acceptance of FRT. The establishment of a consultative body for the deployment of FRT in Arab jurisdictions could facilitate the assurance of religious and cultural compliance, particularly in contexts that intersect with sensitive areas of private and public life.

3. It is recommended that consultation and public engagement be undertaken. In the event of a large-scale implementation of FRT, it would be prudent to consider public consultations. This would ensure that local communities are able to comprehend and concur

(1) Nadwi, W., & Uday, M. A. M. (2024). The right to privacy: Foundations and protections in Islamic jurisprudence. International Journal of Religion, 5(12), 725–735. ijor.co.uk

with the specific applications of this technology in a culturally sensitive manner.

Robust Governance Mechanisms

1. Should have a designated AI ethics board: Establish a designated AI ethics board comprising experts from various disciplines to conduct ethical reviews, and audits and provide guidance on the ethical use of FRT systems.(1)

2. There should be manuals that can be drafted on standard operating procedures like usage of FRT, type of watch lists, logging patterns and accountability methods.(2)

3. Require Human Governance: FRT deployment should only be driven by defined senior security offerings, along with roles and responsibilities around monitoring FRTs, escalation points, and accountability mechanisms.(3)

4. Our best practice approach is that equality and bias testing be built into FRT solution procurement and the developmental lifecycle, allowing for ongoing testing, identification and control of potential

(1) Veale, M. (2021). A critical look at the risk-based approach to limiting police facial recognition. Computer Law & Security Review, 41, 105559. https://doi.org/10.1016/j.clsr.2021.105559

(2) Fussey, P., & Murray, D. (2019). Independent report on the London Metropolitan Police Service's trial of live facial recognition technology. University of Essex Human Rights Centre.

(3) European Commission. (2021). Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

biases.(1)

5. Regular third-party audits of FRT systems, to check for legal compliance, accuracy, bias and equality impacts, to ensure that FRT systems are open and enhance public trust (Ada Lovelace Institute, 2022).

6. Developing robust and straightforward avenues for public grievance and complaints should be institutionalized to facilitate the public reporting of problems for suspected abuses or FRT deployment-specific violations (Garvie et al., 2016).

Coordination of Global Policies

1. Inter-governmental bodies should collaborate towards agreeing on standard practices stipulating human rights, ethics and data protection, in relation to FRT deployment, underpinning a common and harmonized (geotriangulated) approach to FRT use (Kindt, 2013).

2. Coordinate the use of standards for interoperability: Interoperability regulations between FRT systems in different Member States are necessary to achieve cooperation in information exchange at the community level (European Commission, 2021).

3. Conduct joint policy research and capacity building: Collaboration on policy research such as FRT accuracy, bias, regulatory sandboxes

(1) Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In Proceedings of the 1st Conference on Fairness, Accountability and Transparency (pp. 77-91). Retrieved From : Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification — MIT Media Lab

> and risk management approaches will help develop international best practices and capacity-building programs for regulators and law enforcement across the world (Veale, 2021)

The implementation of a holistic regulatory regime (encompassing legal, governance, technology, and international cooperation elements) may ensure transparency in the application of face recognition technology by law enforcement authorities and in accordance with laws, which would ensure its ethical deployment while respecting the principles of necessity, proportionality, and protection of human rights.

Conclusion

The deployment of facial recognition technology (FRT) in law enforcement has far-reaching implications that extend beyond the immediate domain of security and policing. This raises significant concerns about the balance between individual privacy and rights and the collective interest in safety. As this technology matures, it becomes essential for policymakers, law enforcement, and civil society to collaborate in the development of a legal and ethical framework that responsibly governs the use of FRT, striking a balance between public security and the preservation of civil liberties.

This paper proposes a regulated deployment approach, whereby FRT is restricted to specific, controlled circumstances, with an emphasis on necessity and proportionality. This approach guarantees that while FRT can facilitate law enforcement in critical situations, it is not deployed on a broad or indiscriminate basis. The effective deployment of facial recognition technology (FRT) necessitates the establishment of robust oversight, comprehensive legal frameworks, and public accountability mechanisms to

address the inherent privacy risks, potential bias, and potential civil rights infringements that are inherent to its use.

The proposed roadmap in this paper provides policy recommendations through the lenses of law, governance, technological best practices, and international cooperation. It is incumbent upon policymakers to implement robust legal frameworks that uphold the principles of necessity, proportionality, and non-discrimination. These frameworks must be supported by rigorous protocols designed to safeguard civil liberties without impeding the capacity of law enforcement agencies to utilise FRT effectively.

The advancement of FRT necessitates a commitment to ongoing innovation, with a particular focus on the enhancement of accuracy, fairness, and transparency. It is imperative that best practices in algorithm development, privacy-preserving techniques, and bias mitigation be prioritised. Furthermore, law enforcement agencies must collaborate with industry and academia to strengthen ethical standards and trust in these systems. Such collaboration has the potential to facilitate the development of technologies that adhere to fundamental ethical principles.

The deployment of FRT is contingent upon a delicate balance between the achievement of security objectives and the upholding of fundamental rights. Societies must navigate this complex landscape through a multifaceted approach that empowers policy through transparency, accountability, and public trust. By embedding FRT usage within a framework that respects democratic values, privacy, and human rights, law enforcement can responsibly harness this powerful technology while preserving the public's confidence in its applications.

References:

Almeida, D., Shmarko, K., & Lomas, E. (2022). 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, 377–387. https://doi.org/10.1007/s43681-021-00077-w

American Civil Liberties Union (ACLU). (2019). The chilling effect of surveillance. Retrieved from: https://www.aclu.org/issues/national-security/privacy-and-surveillance

Brayne, S. (2020). Predict and surveil: Data, discretion, and the future of policing. Oxford University Press.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1-15. Retrieved from https://proceedings.mlr.press/v81/buolamwini18a.html

CJEU (Court of Justice of the European Union). (2019). Case C-623/17. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0623

CJEU (Court of Justice of the European Union). (2020). Joined Cases C-511/18 and C-512/18. Retrieved from https://curia.europa.eu/juris/liste.jsf?num=C-511/18

Court of Appeal. (2020). R (Bridges) v. Chief Constable of South Wales Police. Retrieved from https://www.judiciary.uk/wp-content/uploads/2022/07/R-Bridges-v-CC-South-Wales-ors-Judgment-1.pdf

Crawford, K. (2021). Atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press.

Data Protection Act 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

European Commission. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Commission. (2021). Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Retrieved from https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonized rules on artificial intelligence (AI Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Equality Act 2010. https://www.legislation.gov.uk/ukpga/2010/15/contents

Garvie, C., Bedoya, A., & Frankle, J. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology. Retrieved from https://www.perpetuallineup.org/

Human Rights Act 1998. https://www.legislation.gov.uk/ukpga/1998/42/contents

Information Commissioner's Office. (2020). Guidance on data protection impact assessments (DPIAs). Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Kindt, E. (2013). Biometric data protection and EU law: Comparative protection of biometric data in the EU member states. Springer.

Lyon, D. (2007). Surveillance studies: An overview. Cambridge: Polity Press.

McCahill, M., & Finn, R. L. (2018). Surveillance, capital and resistance: Theorizing the surveillance subject. Routledge.

Metropolitan Police Service. Facial recognition technology. Retrieved June 7, 2024, from https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition-technology/

Nadwi, W., & Uday, M. A. M. (2024). The right to privacy: Foundations and protections in Islamic jurisprudence. International Journal of Religion, 5(12), 725–735. https://doi.org/10.61707/864v8350

Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. Berkeley Technology Law Journal, 32(2), 1175-1230.

Privacy International. (2023, November 7). UK MPs asleep at the wheel as facial recognition technology spells end of privacy in public. Retrieved from https://privacyinternational.org/long-read/5155/uk-mps-asleep-wheel-facial-recognition-technology-spells-end-privacy-public

Protection of Freedoms Act 2012. https://www.legislation.gov.uk/ukpga/2012/9/contents

Richards, N. M. (2013). The dangers of surveillance. Harvard Law Review, 126(7), 1934-1965.

Suresh, H., & Guttag, J. V. (2020). A framework for understanding unintended consequences of machine learning. Communications of the ACM, 64(2), 62-71.

Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 1701-1708).

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU artificial intelligence act — analyzing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International, 22(4), 97–112.

تكنولوجيا التعرف على الوجوه في مجال إنفاذ القانون: البحث عن موازنة بين الأمن والحقوق المدنية في المملكة المتحدة وقارة أوروبا

محمد جميل زكريا محمود[1]

ملخص البحث:

أصبح الاستخدام المتزايد لتقنية التعرف على الوجه (FRT) من قبل جهات إنفاذ القانون موضع جدل كبير، نظرًا لتأثيراتها المحتملة على الخصوصية والحريات المدنية وحقوق الإنسان. تقدم هذه الدراسة تحليلاً عميقًا للأبعاد التنظيمية والأخلاقية والاجتماعية المحيطة بتطبيقات تقنية التعرف على الوجه في المملكة المتحدة والاتحاد الأوروبي. وتستعرض الدراسة الأطر التنظيمية المتباينة، مع التركيز على قانون الذكاء الاصطناعي في الاتحاد الأوروبي، الذي يعتمد نهجاً وقائياً قائمًا على الحقوق، مقابل الاعتماد التفاعلي على الرقابة القضائية في المملكة المتحدة. ورغم أن تقنية التعرف على الوجه يمكن أن تعزز السلامة العامة وتدعم قدرات حل الجرائم، إلا أنها تثير مخاوف جدية بشأن انتهاكات الخصوصية وإمكانية التحيز والتمييز، وخطر التوسع المفرط في استخدامها لأغراض تتجاوز هدفها الأساسي

توصي هذه الورقة بتبني نهج «التطبيق المنظم» المتوازن، مشددةً على ضرورة استخدام تقنية التعرف على الوجه ضمن ظروف محددة وتحت سيطرة واضحة. وتتضمن التوصيات تطبيق أطر قانونية قوية تلتزم بمبادئ الضرورة والتناسب وعدم التمييز، إلى جانب هياكل حوكمة صارمة لضمان الشفافية والمساءلة. علاوة على ذلك، تؤكد الورقة على الحاجة إلى تنسيق السياسات العالمية وتوحيد التنظيمات عبر الحدود لمعالجة التحديات الأخلاقية والقانونية المعقدة التي تفرضها تقنية التعرف على الوجه. ومن خلال اقتراح إصلاحات شاملة وأفضل الممارسات، تهدف هذه الدراسة إلى وضع أساس لاستخدام مسؤول وأخلاقي لهذه التقنية يتماشى مع القيم الديمقراطية ويحترم حقوق الأفراد

الكلمات الدالة: تكنلوجيا التعرف على الوجوه، إنفاذ القانون، الحقوق المدنية، الخصوصية

(1) كلية الحقوق - جامعة عين شمس (القاهرة - مصر)

gamil.mg.mz@gmail.com