ASSEDEL, 11 Rue de Bruxelles 67000 Strasbourg, France, www.assedel.org,

info@assedel.org

***July 2025***

# Artificial Intelligence and the Law: The Need to Strengthen the Existing Regulatory Framework for Live Facial Recognition by Law Enforcement in the United Kingdom

TABLE OF CONTENTS

## I. INTRODUCTION

Live facial recognition (LFR) technology has rapidly expanded in use across the United Kingdom, transforming the landscape of policing and surveillance. Police forces now deploy LFR to identify persons of interest in public spaces, with major deployments reported in cities such as London, Cardiff, Bridgend, and Southend. The proliferation of this technology, however, has raised significant concerns. This report prepared by ASSEDEL (L'Association européenne pour la défense des droits et des libertés) argues that, in the current UK context, the adoption of live facial recognition technology by law enforcement operates within an inadequate regulatory framework which threatens fundamental rights and exacerbates racial biases. In the absence of comprehensive statutory regulation and robust oversight mechanisms, the continued and expanding use of LFR risks undermining public confidence, enabling discriminatory practices, and eroding the bedorck democratic values of privacy and civil liberty.

## II. THE DEPLOYMENT OF LIVE FACIAL RECOGNITION

LFR systems enable police to scan faces in real time using fixed or mobile cameras placed in public venues such as shopping streets, stadiums, and transport hubs. Collected facial images are compared against police watchlists, typically comprising individuals wanted for priority offences, missing persons, or vulnerable persons at risk. While images of non-watchlisted individuals are reportedly deleted immediately after scanning, criticism persists regarding the breadth and opacity of watchlist composition and matching criteria.

Recent deployments highlight the routine use of LFR by several forces, including the Metropolitan Police, South Wales Police, Essex Police, and Suffolk Police. The Metropolitan Police have taken steps towards permanent installation of LFR cameras in urban areas, a move viewed by critics as a normalization of mass biometric surveillance. Police communicate that such technologies are applied solely for serious crimes, child safeguarding, and high-profile events, with deployments purportedly marked by clear signage for public transparency. Nonetheless, extensive use at concerts, sporting events, and city centers characterizes a shift from exceptional to routine surveillance.

## III. THE UNITED KINGDOM'S LEGAL AND REGULATORY LANDSCAPE

LFR operates in a complex and contested legal environment. While police assert that their use of LFR is governed by data protection law, human rights, and the necessity and proportionality principle, analysts and campaigners argue that the regulatory framework is fragmented, ambiguous, and inadequate. Crucially, there is no specific statute or act of parliament explicitly authorizing or regulating police use of LFR, resulting in what has been characterized as a regulatory Wild West – that is, lacking any legal framework.

The 2020 Court of Appeal ruling in the Bridges v. South Wales Police case found that previous LFR deployments violated privacy rights and data protection laws due largely to the lack of clear rules governing the regulation of technology and the excessive discretion afforded to individual officers. Specifically, the ruling highlighted that officers had broad, unchecked powers to decide where and when to use LFR, without sufficient statutory guidance or oversight. This absence of constraints made the surveillance disproportionately intrusive, impacting the privacy of ordinary

people without reasonable suspicion or justification. Furthermore, the way data was collected, stored, and shared was found to be insufficiently controlled, breaching the UK's data protection regime (implemented under the EU General Data Protection Regulation (GDPR) at the time). The court was particularly concerned about the lack of transparency around "watchlists"—the databases against which faces were matched—which could include individuals not suspected of any wrongdoing, raising the risk of mass surveillance without cause.

Notwithstanding this hallmark ruling, law enforcement in the United Kingdom has continued to employ LFR, largely because there remains no dedicated statutory framework explicitly regulating its use. In other words, while the ruling established important legal principles, it did not outlaw police use of LFR outright. Instead, law enforcement agencies have leaned on broader, more flexible legal interpretations such as general data protection laws, human rights obligations, and internal policies to justify their ongoing deployments. These interpretations often balance the asserted benefits of LFR for crime prevention and public safety against privacy concerns, emphasizing necessity and proportionality, though critics argue that such internal guidelines lack adequate enforceability and independent oversight.

The Information Commissioner's Office (ICO), the UK's independent data protection authority, acknowledges the potential of LFR to aid law enforcement in identifying suspects, finding missing persons, and preventing crime. However, the ICO emphasizes that the technology involves processing highly sensitive biometric data, which is afforded the highest level of protection under data protection law. Therefore, the ICO highlights that using LFR demands the strictest ethical standards, ensuring that surveillance is necessary, proportionate, and transparent.

In July 2025, the UK government announced plans to develop a new governance framework for LFR, in response to criticism from policymakers, privacy experts, and civil society groups. While discussions indicate movement towards clearer policies, as of the present, there is no dedicated statutory basis or parliamentary act specifically regulating the technology's use by law enforcement agencies. In contrast, the European Union's Artificial Intelligence Act strictly limits the use of biometric surveillance in public spaces, requiring judicial or independent administrative authorization and restricting police to its use only for serious, clearly defined threats. Comparative analysis suggests that continued expansion of LFR under the UK's fragmented legal framework positions the country as an outlier among liberal democracies, most of whom have adopted or are considering statutory bans or moratoria on police LFR.

## IV. A BREACH OF HUMAN RIGHTS: PRIVACY AND RACIAL BIAS

The blanket biometric surveillance treats every bystander as a potential suspect, eroding the presumption of innocence and invading individuals' private life within public realms. This mass collection and processing of biometric data intrude deeply on an individual's privacy, potentially chilling freedom of movement, assembly, and expression — all fundamental rights interconnected with the right to privacy under Article 8 of the European Convention on Human Rights. . The symbolic effect of surveillance—transforming public space into monitored territory—raises important questions about consent, especially as LFR is regularly deployed at political demonstrations, protests, festivals, and high-traffic public areas.

Equally as important, empirical studies have established that LFR disproportionately misidentifies individuals from Black and minority ethnic backgrounds, amplifying historic patterns of over-policing and contributing to institutional racial biases. The case of Robert Williams proves illustrative. Mr. Williams is an African American who in 2020 was mistakenly identified by police facial recognition as a suspect in a federal larceny case. He was handcuffed in front of his family, although he was later proven wrongly accused.

Moreover, the National Institute of Standards and Technology (NIST) issued a 2019 report (subsequently updated) that quantitatively documented this bias. Some facial recognition algorithms evaluated were found to be 10 to 100 times more likely to misidentify Black or East Asian faces than those of white individuals. Although these results varied across algorithms—with some showing minimal performance differences—this evidence underscores a pattern of racial disparity in biometric accuracy. Experts from NIST advise those deploying FRT to rigorously and specifically evaluate the bias in their systems.

In the United Kingdom specifically, investigations reveal alarmingly high error rates in police facial recognition matches. For instance, a report by Big Brother Watch found that the Metropolitan Police experienced less than 2% accuracy in facial recognition matches, meaning over 98% were false positives incorrectly identifying innocent people. This trend was further observed in South Wales where law enforcement had similarly poor results with a mere nine percent accuracy and 91 percent false matches. Police interventions based on such misidentifications have led to hundreds of innocent individuals being wrongfully stopped, questioned, and having their biometric data stored without their knowledge. This widespread inaccuracy disproportionately affects disadvantaged groups, as facial recognition algorithms tend to perform worse on darker-skinned faces and women, a pattern also confirmed in studies from the Massachusetts Institute of Technology.

## V. RECOMMENDATIONS

Although ASSEDEL recognizes that the most robust protective measure entails that the United Kingdom prohibit law enforcement from using LFR technology to scan and identity individuals in public spaces, ASSEDEL urges the United Kingdom and the Council of Europe, at minimum, undertake the following actions:

A. *The Government of the United Kingdom*

(1) Implement a comprehensive legal framework. The UK government should enact dedicated legislation explicitly governing biometric surveillance technologies, including facial recognition. This framework must define permissible uses, establish independent supervisory bodies, and incorporate mechanisms for redress to individuals affected by errors or misuse;
(2) Ensure that facial recognition is not deployed without prior independent approval from a judge or a designated oversight authority. This safeguard would ensure deployments are legally justified, proportionate, and necessary, subject to transparent review rather than unilateral police discretion;
(3) Develop strict criteria for inclusion on police watchlists. Individuals should only be added

to facial recognition watchlists if there is reasonable suspicion of involvement in a serious crime. Broad or arbitrary inclusion undermines privacy rights and increases the risk of misidentification and stigmatization. Clear legislative standards defining what qualifies as "serious crime" must be established to prevent mission creep;

(4) Mitigate biases in the technology. Before any deployment, LFR systems should undergo rigorous testing to quantify and minimize racial, gender, and other biases. Developers and law enforcement agencies must adhere to strict technical and ethical standards, with continuous monitoring to prevent discriminatory outcomes; and

(5) Enhance transparency and public accountability. Police forces should be required to publicly disclose when, where, and how LFR technology is used, including data on accuracy, false positives, and any legal challenges arising from its use. Data handling protocols, retention limits, and audit procedures must be documented and made subject to regular independent review.

B. *The Council of Europe (CoE)*

(1) Advocate for Strict Regulatory Frameworks. Encourage member states to adopt clear, dedicated legislation specifically governing the use of biometric surveillance technologies including LFR. Such frameworks should define permissible uses, limit discretionary power of law enforcement, and establish robust independent oversight mechanisms to enforce necessity, proportionality, and transparency;

(2) Support Judicial or Independent Authorization. Recommend that any deployment of LFR by law enforcement in public spaces require prior independent approval—ideally judicial or a designated supervisory authority—to ensure deployments are legally justified and consistent with human rights;

(3) Demand transparency and public accountability. Require public disclosure from law enforcement agencies regarding LFR use, including locations, duration, watchlist criteria, accuracy rates, false positives, data handling policies, and legal challenges arising from its use. This transparency is vital to maintaining public trust and adherence to democratic values;

(4) Encourage a moratorium pending further analysis. Support calls for a moratorium on LFR deployment in public spaces and schools across CoE member states until thorough democratic debates and impact assessments can be conducted focusing on privacy, civil liberties, and societal implications; and

(5) Integrate human rights safeguards explicitly in any Artificial Intelligence (AI) and biometric technology regulation initiatives. This would ensure respect for privacy, non-discrimination, as well as the right to freedom of assembly and expression.

## VI. CONCLUSION

Live facial recognition technology remains at the center of controversy in the United Kingdom. Although it offers the potential benefits of crime prevention and public safety, the deleterious effects arising from such technology, such as privacy and civil rights, override the salutary effects. The existing legal framework is widely regarded as inadequate for addressing the unique challenges posed by this technology, contributing to a landscape characterized by regulatory

ambiguity, function creep, and diminished public trust. Calls for statutory regulation, robust oversight, and stringent safeguards are likely to intensify as the government moves, albeit slowly, towards developing a new governance framework. Until such measures are enacted, the future of facial recognition in UK policing will remain a pressing issue for lawmakers, courts, and the public alike.