Automated Facial Recognition and The Rule of Law

Abiodun Michael Olatokun

Introduction

The "Miller/Cherry" prorogation litigation was the most widely discussed case heard by a court in England and Wales this September. However it is arguably another judgment handed down last month, that of *Bridges v South Wales Police*, that will inform and influence developments in a novel area of law most significantly. This post points to a number of Rule of Law issues that arise from the judgment whilst avoiding an in-depth discussion of its competing arguments. Those interested in finding out more about *Bridges* can explore the articles from our partner organisations listed below.

The case

The case saw campaigner Edward Bridges challenge the use of 'Automated Facial Recognition' (AFR) software by South Wales Police Force. AFR had been used to locate wanted police suspects at a political demonstration he attended. The *Bridges* litigation is believed to be the first case of its kind in any jurisdiction and will likely be influential in the approach taken by jurists in this developing area of law across the world.

In outline, AFR is a form of technology deployed in the prevention of crime. AFR involves scanning the faces of people in crowded public areas for biometric information, processing that information and then attempting to match that data against the faces of individuals suspected of involvement in criminal offences.

The result

Bridges' legal team argued that:

- The use of AFR amounted to a violation of his right to respect for his private life (Article 8 ECHR) as there was insufficient domestic law to justify the use of AFR,
- The type of data processing involved in AFR did not meet the requirements of the General Data Protection Regulation or the UK Data Protection Act 2018 (DPA 2018), and,
- The use of AFR technology could disproportionately impact female and black and minority ethnic citizens because these individuals were more likely to be the subjects of 'false matches'.

The court found against him on **all three** grounds.

Though the court was satisfied that the use of AFR could amount to an interference with the claimant's privacy rights, they did not believe it to violate those rights due to the sufficiency of provisions governing the exercise of the powers in the DPA 2018 and elsewhere. AFR was also described as a non-intrusive form of surveillance akin to CCTV because it did not involve entry onto private property (such as a search with a warrant) or contact with the claimant (such as taking a fingerprint).

What Rule of Law issues does this raise?

New technologies such as AFR raise a number of challenges for the Rule of Law that will persist as data-driven and machine learning systems are incorporated into the practice of public authorities.

Specific legislative provisions

> *The Rule of Law requires public decision makers to act in accordance with the law and for them to be accountable for the exercise of their powers.*

It also requires clarity about the rights that individuals have before the law. One of the compelling arguments raised in support of Bridges' case was that there was no legislative basis for the police power to use AFR.

The Divisional Court took a different view and pointed to the DPA 2018, s34 of the Protection of Freedoms Act 2012 and the SWP's own policies as a "clear and sufficient legal framework governing whether, when and how AFR Locate may be used".

The author doubts that the legal framework is sufficiently clear; aside from the fact that the DPA 2018 exists as a means of assisting the incorporation of the EU GDPR and updating existing data laws, it is not intended to be an all-encompassing regulation to provide public law grounds and safeguards for all of the kinds of data processing to which it is applied.

More broadly, this represents a fragmentation of the legislation governing the power that is inconsistent with other widely used police powers; elsewhere in the judgment the court explains that DNA and CCTV are specifically governed by the Police and Criminal Evidence Act 1984 and the Protection of Freedoms Act 2012.

In order for citizens to understand their positions before the law and to increase their ability to challenge the use of powers that adversely affect their interests, a specific legislative provision should be enacted. This would also give Parliament an opportunity to scrutinise a power that could curtail the citizen's enjoyment of their civil liberties.

Equality before the law and equal treatment by law enforcement agencies

One of the arguments in *Bridges* cut right to the heart of ethical issues surrounding the use of artificial intelligence, the question of bias. An expert witness in the case stated that there is a known shortcoming in the ability of AFR systems generally to accurately process female faces; he was however ambivalent as to whether such bias operated in this case. The court in *Bridges*ruled that South Wales Police had met their duty to have due regard to the need to eliminate discrimination and foster good relations between groups with protected characteristics by acting on all available information when they created their equality impact assessment.

However the court stopped short of saying that there had been no indirect discrimination due to a lack of evidence about how the new technology operated. Whilst there is some wisdom in that decision in *Bridges*, this raises a broader ethical question about whether systems known to produce false matches for a large, determinate proportion of the population should be deployed at all.

Continued use of AFR has implications for equality before the law and the proportionality of outcomes for social demographic groups in the criminal justice system. These issues may have been less prominent in South Wales, which has a more homogenous ethnic mix than some urban areas of the UK, but the use of AFR by the Metropolitan Police Force, London's local police, brings

issues of equality into stark relief.

A report by campaigning organisation Big Brother Watch suggested that over 98% of AFR matches in London wrongly identified innocent members of the public. This is explained by other groups such as Liberty and Future Advocacy who state that algorithmic processing of biometric data in AFR systems treats black and minority ethnic data subjects differently from their Caucasian counterparts. The consequences of these false AFR matches are redolent of suspicionless stop and search powers; misidentification and alienation of disadvantaged minority groups.

Where to from here?

South Wales Police are at the forefront of pioneering the use of this technology, but they are not alone in doing so. Police forces seek to utilise new and emerging technologies to keep the public safe. At the time of writing, several pilot exercises continue the development of AFR tools, and this judgment will likely encourage incorporation of the technology into the toolkit of the modern police force.

Whereas crime prevention presents a compelling impetus to law enforcement agencies, public perception of AFR is more nuanced. A recent poll by the Ada Lovelace Institute suggested that 54% of people were alarmed at the potential risks that AFR technology could cause. This figure should be viewed in contrast to the 49% of respondents who approved the use of the technology with appropriate safeguards. The court framed the dispute in *Bridges* by stating that,

> *"the algorithms of the law must keep pace with new and emerging technologies,"*

recognizing that they would have to consider "the central issue...whether the current legal regime in the United Kingdom is adequate to ensure the appropriate and non-arbitrary use of AFR in a free and civilized society."

Thus, there is a balance to be struck. If AFR is to be accepted by the public as a legitimate police tactic, adequate frameworks are required to ensure that its use does not encroach upon the rights of data subjects. Furthermore, to comply with the requirements of the Rule of Law, its use should be limited to provide minimal discretion to those wielding it.

The government foresaw a potential solution to this regulatory challenge in Part 7 of the DPA 2018, which provided the Secretary of State with a discretionary power to prepare a "Framework for Data Processing by Government" which would contain guidance about the processing of personal data in connection with the exercise of functions of a person with functions of a public nature who is specified or described in regulations made by the Secretary of State.

The scope for such a Framework was the subject of a meeting of the All-Party Parliamentary Group on the Rule of Law in April 2018, where the Bingham Centre convened MPs, leading experts and campaign organisations to outline these Rule of Law concerns during the passage of the DPA 2018. Speakers were confident that the Framework would provide greater clarity of the powers of data processors exercising their public functions.

The Framework would be subject to the negative resolution procedure, which would allow Parliament to scrutinise and improve the draft Framework whilst empowering the public to participate in a debate about the limits of police incursion into their civil liberties. Democratic debate in the establishment of safeguards would satisfy the 49% of the public who support use of AFR technology under guidance, whilst providing some reassurance to those that remain unconvinced that its crime-prevention

credentials overcome the privacy and discrimination problems that its untrammelled use might cause.

Helpful links:

BAILII: R (On Application of) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) (04 September 2019)

Big Brother Watch: The Lawless Growth of Facial Recognition in the UK, Big Brother Watch: Face Off: The Lawless Growth of Facial Recognition in the UK

The European Union: The General Data Protection Regulation

The Information Commissioner: Rights related to automated decision making including profiling

The Information Commissioner: Statement: Live facial recognition technology in King's Cross

The Information Commissioner: Blog: Live facial recognition technology - data protection law applies

Liberty: Resist Facial Recognition

Sapan Maini-Thompson: Facial Recognition Technology: High Court gives judgment

Swee Leng Harris: Data Protection Impact Assessments as Rule of Law Governance Mechanisms

URL: https://binghamcentre.biicl.org/comments/69/automated-facial-recognition-and-the-rule-of-law