



Kent Academic Repository

Holmes, Allison M (2023) *'Serious and Systemic'? Live facial recognition technology in the United Kingdom and its impact on adequacy under the LED*. In: Celeste, Edoardo and Costello, Roisin and Harbinja, Edina and Xanthoulis, Napoleon, eds. *Data Protection and Digital Sovereignty Post-Brexit*. Hart Publishing, UK, pp. 105-121. ISBN 978-1-5099-6648-6.

Downloaded from

<https://kar.kent.ac.uk/105905/> The University of Kent's Academic Repository KAR

The version of record is available from

<https://www.bloomsbury.com/uk/data-protection-and-digital-sovereignty-postbrexit-9781509966486/>

This document version

Author's Accepted Manuscript

DOI for this version

Licence for this version

CC BY-ND (Attribution-NoDerivatives)

Additional information

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in **Title of Journal**, Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our [Take Down policy](https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies) (available from <https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies>).

‘Serious and Systemic’? Live facial recognition technology in the United Kingdom and its impact on adequacy under the LED

Allison M Holmes

Introduction

Following the United Kingdom’s withdrawal from the European Union, data protection and data sharing by and between law enforcement authorities has taken on a new importance. Continued information sharing between UK and EU authorities post-Brexit is contingent on maintaining a high level of personal data protection and the effective protection of fundamental rights. However, the powers of law enforcement can be at odds with these rights, notably the right to private life, particularly in the adoption of novel technologies which expand the scope of police powers of surveillance. This chapter examines one such technology, namely live facial recognition (LFR) utilised by law enforcement authorities in publicly accessible spaces and how it impacts on these fundamental rights in a manner which puts these information sharing arrangements at risk.

In assessing the impact of LFR on information sharing arrangements post-Brexit, it is necessary to examine the Adequacy Decision which underpins law enforcement cooperation in this area.¹ In order to enable information sharing, the UK must ensure that it provides an adequate level of protection for personal data, in line with Article 36(3) of Directive (EU) 2016/680, the Law Enforcement Directive (LED).² This chapter argues that the use of LFR by the police in England and Wales represents a clear divergence from the EU standards governing the use of personal data.³ This is

¹ Commission Implementing Decision of 26 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (LED Adequacy Decision) C(2021) 4801 final.

² Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (LED Directive) [2016] OJ L 119/89

³ The focus of this chapter will be on the use of LFR in England and Wales. The criminal justice systems of Scotland and Northern Ireland are devolved to the Scottish Parliament and Northern Ireland Assembly respectively. The technology has not been introduced in Scotland following a report of the Scottish Parliament which noted that given the potential discriminatory nature of this technology, ‘there would be no justifiable basis for Police Scotland to invest in this technology’ (See: Justice Sub-Committee on Policing [Scotland], *Facial recognition: how policing in Scotland makes use of this technology* (SP 2020-5, Paper 678). Similarly, as of time of writing there is no reported use of the technology in Northern Ireland.

indicative of a wider trend of divergence between EU and UK law which represents a threat to the overall adequacy arrangements governing data sharing between the EU and the UK. In order to analyse the divergences between the EU and the UK exposed by LFR, this chapter offers an assessment of the extant legal bases governing the use of this technology and current proposals to amend the powers of law enforcement in the UK in respect of LFR. In undertaking this analysis, the chapter examines the deficiencies in the legal framework governing LFR which negatively impacts the protection provided to personal data and threatens the finding the UK's use of LFR provides protection that is 'essentially equivalent' to that of the EU.⁴

The Adequacy Decision

Following the referendum on United Kingdom's European Union Membership on the 23rd June 2016 and during the subsequent negotiations surrounding the future of the EU-UK relationship, the British Government emphasised the need to maintain stability and ensure "unhindered" and "uninterrupted" data flows between the UK and the EU post-Brexit.⁵ During the Brexit negotiations, law enforcement agencies, government bodies, and others repeatedly emphasised that the UK could face both economic and social isolation in circumstances where authorities could not share or receive law enforcement data on a cross-border basis. To that end, the final Trade and Cooperation Agreement governing the future relationship between the EU and UK specifically legislates for continued data sharing post-Brexit.

In particular, Part Three of the Agreement enables high level data sharing and access to EU law enforcement systems and agencies.⁶ A key facilitator of this information sharing is the Law Enforcement Directive (LED) which stipulates transfer provisions for the sharing of personal data between relevant law enforcement authorities.⁷ The Directive provides data protection safeguards by explicitly tying data transfer

⁴ As confirmed and advanced in the cases of Case C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650; Opinion 1/15 *Draft agreement between Canada and the European Union – Transfer of Passenger Name Record data from the European Union to Canada* [2017] ECLI:EU:C:2017:592; and Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximilian Schrems* [2020] ECLI:EU:C:2020:559.

⁵ House of Lords Select Committee on the EU; EU Home Affairs Sub Committee; Oral evidence: Data Protection Package; Matt Hancock, 1 Feb 2017

⁶ Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (TCA) [2021] OJ L 149/10 Part 3.

⁷ LED (n 2).

provisions to fundamental rights considerations.⁸ In the UK these provisions are given domestic effect within Part 3 of the Data Protection Act.

For information sharing between the EU and the UK to be permitted under the LED, there are several distinct mechanisms which may be used, namely adequacy decisions, appropriate safeguards, or derogations to specific situations.⁹ While initially following the UK's withdrawal then Minister of State for Digital and Culture Matt Hancock would not be drawn on what mechanism would be used to ensure these transfers, subsequent agreements have provided a clear indication that adequacy decisions were the preferred mechanism for the continued sharing of data.¹⁰ Adequacy decisions have a range of benefits. They represent the highest standard of protection for onward transfers of data guaranteed by any of the data sharing mechanisms provided for within the data protection instruments. This in turn means that fundamental rights are better protected. Further, they represent a positive development in terms of operational capabilities for law enforcement authorities because an adequacy decision removes the need for specific authorisation of transfers of personal data, resulting in an efficient mechanism for data sharing between relevant bodies.

In order for a third country to be considered as providing an adequate level of protection for personal data, there must be 'a level of protection of fundamental rights and freedoms ... essentially equivalent to that guaranteed within the European Union'.¹¹ The criteria considered in assessing adequacy include consideration of the rule of law, respect for human rights and fundamental freedoms, the relevant legal framework, protection of the rights of data subjects, and mechanisms for ensuring effective remedies.¹² Similarly, independent supervisory authorities who ensure compliance with the data protection rules and possess adequate enforcement powers are required.¹³ The final criteria for consideration are the international commitments of

⁸ LED (n 2) Article 35(3) and Recital 67.

⁹ LED (n 2) Articles 36-38

¹⁰ Withdrawal Agreement 2019 Art 71.

¹¹Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* [2020] ECLI:EU:C:2020:559 [96]. Emphasis added from original.

¹² LED (n 2) 36(2)(a)

¹³ LED (n 2) Art 36(2)(b)

the third country and their participation in legally binding conventions or instruments, particularly those which relate to data protection.¹⁴

These elements were considered in the evaluation of the UK as a third country for the purposes of an Adequacy Decision under the LED. The close alignment between UK and EU data protection law was highlighted, with the structure and main components of the UK legal framework under Part Three of the Data Protection Act 2018 (DPA) governing law enforcement processing given considerable weight in the decision to award adequacy.¹⁵ The Decision also noted the extant oversight and redress mechanisms which provide remedies for data subjects whose rights might be impacted.¹⁶ Notably the Decision identifies the importance of the Information Commissioner and the Commissioner for the Retention and Use of Biometric Material as independent oversight mechanisms, with specific competencies in the area of law enforcement data processing.¹⁷ Finally, the evaluation of the UK domestic regime considered the compliance with international instruments, and in particular the adherence to the European Convention on Human Rights (ECHR) and the Council of Europe Data Protection Convention (Convention 108) and the subsequent amendments modernising this Convention (Convention 108+).¹⁸ The compliance with the ECHR in particular is highly important to the finding of adequacy and the need for continued adherence to this instrument was stressed by the Commission.¹⁹

Following this evaluation of the UK framework, two Adequacy Decisions were adopted on the 28th June 2021 for the GDPR and LED respectively. Both decisions include additional safeguards to ensure continued compliance by the UK with the data protection obligations under the Adequacy Decision. Under Article 3 LED, the Commission is obliged to monitor the legal framework which underpins the decision, 'including the conditions under which onward transfers are carried out and individual rights are exercised, with a view to assessing whether the United Kingdom continues to ensure an adequate level of protection within the meaning of Article 1'. This monitoring includes an obligation by Member States and the Commission to inform

¹⁴ LED (n 2) Art 36(2)(c)

¹⁵ LED Adequacy Decision (n 1) Recitals 20-54.

¹⁶ *ibid* Recital 158.

¹⁷ *Ibid* Recitals 93-108.

¹⁸ *ibid* Recital 20; See also the European Convention on Human Rights and Convention for the protection of individuals with regard to the processing of personal data Convention 108/108+.

¹⁹ LED Adequacy Decision (n 1) Recitals 269; 277.

one another if there are indications that interferences with personal data by public authorities in the UK go beyond what is strictly necessary or lack effective legal protection.²⁰ If adequate protection is no longer ensured, the adequacy decision may be suspended, amended, or repealed.²¹ In particular, regard has to be had to the effectiveness of the exercise of individual rights in the areas covered by the adequacy decision, as well as the operation and oversight of relevant bodies. As such, while the current data protection framework within the UK meets the requirements for adequacy, developments in the data protection regime which alter these considerations concerning fundamental rights and oversight may impact on that finding.

Case Study: Live Facial Recognition

It is within this context that the case study of live facial recognition technologies in public spaces offers a useful reference point to see how divergences in policies concerning the protection of personal data in the law enforcement sphere could impact on the finding of adequacy. In evaluating the impact of LFR, the legal framework which governs the use of these powers, the role of watchlists, and the oversight arrangements must be considered against the potential impact on individuals rights. Live facial recognition involves several distinct data processing operations. Members of the public are scanned as they pass fixed and mobile camera points. This can occur both on private property and within public spaces, the latter of which is the subject of analysis in this chapter. The images collected on the basis of this scan are then processed by a facial recognition algorithm which creates a biometric template.²² This template is compared to a database which has been created from similarly processed images which is known in the deployment as a 'watchlist'. If the algorithm detects a match, an alert is sent to the system and a decision is subsequently made on whether to intervene.

Live facial recognition necessarily engages data protection considerations. Fundamentally, it is concerned with the processing of biometric data. Biometric data is defined as 'personal data resulting from specific technical processing relating to the physical, psychological or behavioural characteristics of a natural person, *which allow*

²⁰ *ibid* Article 3(2) - (3)

²¹ *ibid* Article 3(4)

²² Pete Fussey, Bethan Davies & Martin Innes, "Assisted" facial recognition and the reinvention of suspicion and discretion in digital policing' 61(2) *Brit J of Criminology* 325,326.

or confirm the unique identification of that natural person, such as facial images and dactyloscopic data'.²³ In creating biometric templates utilised for identifying individuals on set 'watchlist', LFR necessarily satisfies these criteria. The classification of this information as biometric data is significant as the relevant data protection instruments identify biometric data as 'special category data', recognising that the processing of this category of data poses a particular risk to the rights and freedoms of natural persons.²⁴ Both individuals' rights to data protection and private life are implicated by the processing of this data.²⁵

The potential impact on fundamental rights occasioned by the use of this data is even more significant when the use of LFR occurs in public spaces. Public spaces are broadly defined. The UK Information Commissioner's Office (ICO) has stated that in this context public spaces generally include spaces outside of a domestic setting, whether publicly or privately owned.²⁶ This encompasses areas open to the public such as public squares, transport, or buildings but it can also extend to 'privately owned premises such as shops, offices, and leisure venues'.²⁷ Applying this technology to public spaces extends it beyond targeted use against individuals of interest to application to the wider public. Broad and indiscriminate use in public spaces has the potential to result in collateral intrusion of the rights of individuals whose biometric data is processed by the technology in a manner which is disproportionate to the aims sought.

Given the broad interference with individual rights which can result from the use of LFR in public spaces it is necessary to evaluate whether it meets the criteria required for that interference to be justified. To that end, the use of the technology must be in accordance with law, strictly necessary, and proportionate to the aims which are sought to be achieved.²⁸ Such an assessment is also important to determine the impact the use of this technology might have on the continued adequacy arrangement

²³ See TCA (n 6) 523(d); LED (n 2) Art 3(13).

²⁴ LED (n 2) Recitals 51-52 & Article 10.

²⁵ Information Commissioner's Opinion, 'The use of live facial recognition technology in public places' (ICO 18 June 2021).

²⁶ *Ibid* 12.

²⁷ Gloria Gonzalez Fuster, & MA Nadolna Peeters, 'Person identification, human rights and ethical principles: rethinking biometrics in the era of artificial intelligence' (European Parliament 2021) 10; UNESCO similarly defines a public space as 'an area or place that is open and accessible to all peoples'. Luca Montag et al, 'The rise and rise of biometric mass surveillance in the EU' (EDRi, EIJI Brussels 7 July 2021) 8.

²⁸ ECHR Art 8(2)

between the UK and the EU as a failure to guarantee fundamental rights when data is processed in this manner is contrary to the requirements of the adequacy decision.

i. Legal framework

For the use of LFR to amount to a justified interference, it must be in accordance with law. In England and Wales, there is no explicit statutory authority for the use of LFR. Rather, police powers in this area rely on common law, statute, and delegated legislation to provide legal underpinnings for the use of the technology. In England and Wales, the powers of the police derive from common law and are not subject to exhaustive definition. They include ‘all steps which appear to him necessary for keeping the peace, for preventing crime, or for protecting property from criminal damage... and they would further include the duty to detect crime and to bring an offender to justice’.²⁹ The common law power of the police can be extended to proactive powers provided that they enable the prevention and detection of crime. It has been further recognised that the common law powers of the police extend to obtaining and storing information for policing purposes.³⁰ However, relying on common law powers as the legal basis for LFR requires a broad interpretation which fails to account for the sensitive nature of the data involved and the potential intrusive nature of the technology. To ensure that the use of this technology meets the necessary quality of law, an explicit statutory provision would provide for a stronger basis.

However, there remains no direct statutory authority for the use of LFR. Rather existing instruments contain provisions which are interpreted in a manner which is then applied to the technology. The use of LFR is governed then by provisions within the Data Protection Act 2018, the Protection of Freedoms Act 2012, and the related Code of Practice provided for by that statute.³¹

Part three of the Data Protection Act 2018 provides authority for the processing of personal data for law enforcement purposes.³² Any authority which processes sensitive data under this Act is required to ensure that the data is processed in a lawful

²⁹ *Rice v Connolly* [1966] 2 QB 414 [419].

³⁰ *Catt v Commissioner of Police of the Metropolis* [2015] UKSC 9 [7].

³¹ Protection of Freedoms Act 2012 s 31(3); Surveillance Camera Code of Practice (3 March 2022).

³² Law enforcement purposes are defined under Data Protection Act 2018 s 31 as: ‘The purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’

and fair manner.³³ Such processing will only be lawful where either consent has been obtained for the processing or where the processing is strictly necessary for law enforcement purposes.³⁴ Both requirements for processing further call for the controller to have an appropriate policy document in place at the time of processing.³⁵

It is unlikely that the consent of the data subject will be an acceptable lawful basis for the processing of data because of the manner in which LFR is deployed in public spaces. Individuals may not be on advance notice of the areas in which LFR will be in operation at a particular time and are not able to effectively exercise their freedom to choose whether to engage with such monitoring. Therefore law enforcement authorities must meet the requirement that the processing is 'strictly necessary' for a set purpose as defined within the Act.³⁶

Strict necessity requires that the processing is 'necessary for the exercise of a function conferred on a person by an enactment or rule of law, and is necessary for reasons of substantial public interest'.³⁷ In the context of LFR, this further requires that alternatives to LFR are considered prior to the deployment of this technology.³⁸ It is important to note that in evaluating the strict necessity of the measure, the assessment should not be generalised but one of direct personal evaluation.³⁹ Such a threshold is unlikely to be met when utilising LFR in public spaces.

In addition to provisions within the DPA 2018 which can apply to the area of LFR, the Protection of Freedoms Act 2012 provides for the regulation of the use of surveillance cameras. While not falling within the traditional definition of a surveillance camera, s 29(6)(d) of that Act can be interpreted to encompass LFR technology,⁴⁰ making it subject to the Surveillance Camera Code of Practice. Relevant authorities, including

³³ Data Protection Act 2018 s 35.

³⁴ *Ibid* s 35(4)(a) and 35(5)(a).

³⁵ *ibid* s 35(4)(b) and 35(5)(c) and s 42.

³⁶ *Ibid* Schedule 8 DPA. Relevant set purposes within the DPA are defined as statutory purposes, the administration of justice, and legal claims.

³⁷ *Ibid*

³⁸ ICO, 'The use of live facial recognition technology by law enforcement in public places' (ICO 31 Oct 2019) 14.

³⁹ *R(EI Gizouli) v Secretary of State for the Home Department* [2020] 2 UKSC 10 [44].

⁴⁰ The act defines 'surveillance camera systems as: (a) closed circuit television or automatic number plate recognition systems; (b) any other systems for recording or viewing visual images for surveillance purposes; (c) any system for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b); or (d) any other system associated with, or otherwise connected with, systems falling within paragraph (a), (b), or (c).

the chief officer of a police force in England and Wales,⁴¹ must have regard to this code and to any functions to which the Code relates. Also provided for within this instrument is the appointment of a Surveillance Camera Commissioner by the Secretary of State to ensure public confidence in surveillance systems by encouraging compliance with the Code, reviewing its operation, and proposing changes and advice to the Code where needed.⁴² The role of the Surveillance Camera Commissioner has now been incorporated into the wider role of the Biometrics and Surveillance Camera Commissioner effective as of February 2022.

The Surveillance Camera Code of Practice is the only instrument within the legal framework of England and Wales which explicitly addresses the use of LFR, albeit in a manner which carries little legal effect. Entering into effect in February 2022, the Code sets out guidance for the use of these systems by public authorities. Any use of facial recognition systems under the Code needs to be justified and proportionate to the purpose sought to be achieved.⁴³ Notably the Code offers no prescriptive requirements for how to satisfy the requirements, nor any specific operational, technical or competency measures which must be followed. The Code requires that authorities 'have regard' to this statutory guidance, meaning that it should be taken into account and departures from the Code must be justified.⁴⁴ However, failures to act in accordance with the code do not merit liability in either criminal or civil proceedings. Therefore, as a legal instrument, it lacks the necessary rigour to ensure that the standards it sets are complied with by the relevant authorities.

In addition to the statutory guidance, LFR is also governed by the internal policies of individual police forces. These documents set out the legal authority for the use of LFR within that select police force. The police force similarly provides procedural guidance for the deployment of the LFR technology. For example, guidance may set the rank of the authorising officer for each deployment, how they should address the legality, necessity and proportionality of the deployment, and ultimately how this is balanced with individual rights considerations.⁴⁵ However, this guidance is advisory and bears

⁴¹ Protection of Freedoms Act 2012 s 33(5)(j)

⁴² *ibid* s 34

⁴³ Surveillance Camera Code of Practice para 2.4

⁴⁴ *ibid* para 8.

⁴⁵ Metropolitan Police Service, 'MPS LFR Policy Document' <<https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document.pdf>> accessed 10/2/22.

no sanctions for failure to adhere to these set policies. Allowing the individual forces to set their own practices in this area can lead to inconsistent approaches being adopted by the various police constabularies, with some taking a more constrained approach and others using the technology more broadly.

The piecemeal governing framework for LFR was challenged in the case of *Bridges v Chief Constable of South Wales Police* wherein whether the provisions were ‘in accordance with law’ was tested.⁴⁶ In holding that the legal framework was insufficient, the Court of Appeal emphasised the level of discretion left to individual police officers to determine both where the technology was deployed and who was on the relevant watchlists.⁴⁷ The Court held that ‘the current policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary quality of law’.⁴⁸ However, the Court’s decision did not require such policies to be set out in statute. Rather the Court accepted that internal policy documents within the police could satisfy the requirements for the use to be ‘in accordance with law’ so long as it sufficiently limited the discretion of individual officers.

This interpretation was welcomed by the Government, noting that a legal framework of existing legislation and published local police policies ‘allows the police to exploit new technologies, including biometric identification and overt surveillance, for a policing purpose and where necessary and proportionate’.⁴⁹ However, this interpretation misrepresents the decision of the court and fails to recognise that the existence of the powers does not in itself render the exercise of those powers lawful. Nor does the government’s interpretation offer an adequate explanation for what those internal policies should entail. In an attempt to proscribe unified guidance for internal force policy following the case of *Bridges*, the College of Police issued an Authorised Professional Practice (APP) for the use of LFR.⁵⁰ This guidance sets out the general approach to be taken by each police force, however it is left to the discretion of the individual police forces to implement this in practice.⁵¹ Notably, this guidance is only advisory and offers no clear lines of accountability where the guidance is not followed

⁴⁶ *R(Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

⁴⁷ *ibid* [91-92].

⁴⁸ *ibid* [94]

⁴⁹ HL Deb 4 Nov 2021, cols 1391-408.

⁵⁰ College of Policing, ‘APP: Live Facial Recognition’ (17 March 2022) <<https://www.app.college.police.uk/app-content/live-facial-recognition/>> accessed 16 October 2022.

⁵¹ *ibid*

for satisfactory recourse mechanisms for individuals who may be impacted by the use of this technology.

This soft law fails to provide an adequate legal basis in domestic law and ensure the necessary requirements of the European Court of Human Rights that the measure be 'in accordance with law'. While States are generally subject to a wide margin of appreciation when the question concerns interferences with qualified rights which are a result of the investigation, detection, and prevention of crime, they must still ensure that the interferences with fundamental rights occasioned by the use of the technology can be justified. This requires that the measure be compatible with the rule of law, as evidenced by the accessibility and foreseeability of the provisions.⁵² The provisions should not be so broad as to confer a wide discretion dependent upon the will of the individuals who apply it;⁵³ the open and discretionary nature of the APP guidelines do not confer the general quality of law that ECtHR precedent requires. Similarly to the Court of Appeal in *Bridges*, the ECtHR takes a relativist approach, noting the need to treat the surveillance differently depending on the impact on individuals.⁵⁴ In so doing, the ECtHR has held that due regard should be had to 'the possibility of rapid technological advances in this domain in particularly concerning technology for facial recognition and facial mapping'.⁵⁵ Particular attention must be paid to the interference with rights 'where the powers vested in the state are obscure, creating a risk of arbitrariness where the technology available is continually becoming more sophisticated'.⁵⁶

In order to evaluate whether the UK is diverging from the EU standards in its data protection policies, it is useful to contrast the use of LFR in the UK with the proposed provisions of the EU Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (hereafter AI Act).⁵⁷ The proposed Act will be *lex specialis* to the General Data Protection Regulation and the Law Enforcement Directive, ensuring the provisions of the LED governing the processing

⁵² *Sunday Times v United Kingdom* App no 6538/74 (ECtHR, 26 April 1979) [48-50] and *Malone v United Kingdom* App no 8691/79 (ECtHR, 2 August 1984) [67].

⁵³ *Re Gallagher* [2019] UKSC 3 [17]

⁵⁴ *R.E. v United Kingdom* App no 62498/11 (ECtHR, 27 Oct 2015) [17]

⁵⁵ *Gaughran v United Kingdom* App no 45245/15 (ECtHR, 13 June 2020) [80]

⁵⁶ *ibid* [86].

⁵⁷ Proposal for a Regulation of the European Parliament and of the Council Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (21 April 2021) COM (2021) 206 final.

of biometric data remain relevant in this area. However, the AI Act goes beyond the LED and provides specifically for the use of live facial recognition technologies within public spaces. The Act more precisely defines the areas in which the use of LFR in publicly accessible spaces is permitted than the internal policy documents and general guidance utilised in England and Wales. The approach of the UK Government relying on existing policy which does not adequately consider the technology is in contrast to the proposed EU AI Act. Notably at EU level policy requires that Member States implement national legislation concerning the use of real-time biometric technologies by law enforcement in publicly accessible spaces prior to its use.⁵⁸ The differing policy concerning legislation surrounding the police use of novel technologies is an element of wider diverging approaches to individuals' personal data between the EU and the UK.

ii. Use of watchlists

Further divergences are evident in the policies concerning the watchlists utilised in LFR deployments. Watchlists consist of biometric templates of individuals of interest, identified with reference to a particular deployment of LFR. Images of the public are compared against these watchlist to alert the police when a match is made. As these images and their processing is 'sensitive' it must only be done where 'strictly necessary'.⁵⁹ However there remains little legal certainty around the creation of these watchlists with the choice for the images for each deployment left to the discretion of the individual police forces.

This concern becomes particularly salient when the guidance from the College of Policing on the use of LFR is examined. While this guidance notes that individual force policy documents should detail their criteria for developing a watchlist, the APP sets out overarching advice regarding the creation of watchlists. Notably, this guidance provides a list of individuals who may be included in the LFR watchlist. The criteria for inclusion are those 1) wanted by the courts; 2) suspected of having committed an offence or where there are reasonable grounds to suspect an individual might commit an offence; 3) subject to bail conditions or other legal restrictions; 4) missing persons deemed at risk of harm; 5) those presenting a risk of harm to themselves or others;

⁵⁸ *ibid* Art 5(4).

⁵⁹ DPA 2018 s 35(5).

and finally 6) a victim or witness to an offence, or a close associate of an individual within any of the set criteria.⁶⁰

The criteria within the guidance are broadly construed and each criteria presents a unique set of issues which mean they are likely to fall foul of the requirements of necessity and proportionality in assessing their impact on fundamental rights. Several of the criteria pertain to those individuals who are suspected of or have committed a criminal offence. However, there is no threshold set for the seriousness of the offence for which the individual is suspected; both those who have committed minor summary offences and those who have committed serious crimes can be caught by the same provision. An appropriate evaluation of the proportionality of including an individual on the watchlist should have regard to the need to balance the individuals' rights against the need of the police to prevent, investigate and detect crime. The use of these powers against individuals who are suspected of only low-level offences is likely to be disproportionate to the objective sought to be achieved.

The development of the watchlists further calls into question the necessity and proportionality when the wider criteria for inclusion are considered. Notably the guidance covers individuals who are not suspected of any criminal offence. Given the impact on individuals' rights to private life and data protection occasioned by the use of the technology, there needs to be a strong justification case made for including these individuals on the watchlist. However, the guidance fails to provide this justification nor clarity on the approach which should be taken to ensure the interference is permissible. For instance, individuals who are classed as presenting a risk of harm to themselves or others are also eligible for inclusion. This criterion is vague and open to wide interpretation. Here harm is broadly defined, including a risk of harm in relation to a person's welfare or financial harm. The level of harm required is assessed as medium risk, meaning that the harm is likely but not serious.⁶¹ The guidance on applying this criterion lacks clarity, setting the threshold as 'likely', but

⁶⁰ College of Policing, 'APP: Live Facial Recognition' (17 March 2022) <<https://www.app.college.police.uk/app-content/live-facial-recognition/>> accessed 18 March 2022 para 2.5.

⁶¹ College of Policing, 'APP: Missing Persons' (24 March 2022) <<https://www.college.police.uk/app/major-investigation-and-public-protection/missing-persons/missing-persons>> accessed 20 August 2022.

then subsequently noting that finding their location is ‘critical to ensure their safety’.⁶² Such contradictory language adds to the ambiguity of these provisions.

These issues are similarly evident in the criterion which permits the inclusion of victims, witnesses, and/or those who are close associates on the watchlists. The application of the technology to these individuals is likely to be a disproportionate interference with the rights of those individuals. While the guidance offers suggestions as to how the proportionality of the inclusion of these individuals could be demonstrated, this set of suggestions fails to offer an adequate safeguard for the rights of those individuals. As these individuals are not the subject of investigations, any interference with their rights will only be proportionate in exceptional circumstances. The guidance does not offer a clear framework for how this threshold would be met. Nor does the guidance as a whole reflect the data protection requirements governing the ‘sensitive’ data which is used in LFR. Any inclusion on the watchlist, due to the sensitive nature of the data involved, requires that the processing be ‘strictly necessary’, however, this requirement is not mentioned within the guidance.

Within the approach to the watchlists, there is a clear divergence from EU policy. At EU level, in the creation of watchlists, three specific uses are permitted: targeted searches for specific potential victims of crime; prevention of specific, substantial, and imminent threat to life or physical safety of natural persons or a terrorist attack; detection, localisation, identification or prosecution of a perpetrator or suspect of a crime with a max sentence of at least three years.⁶³ This final criteria sets out thirty two categories of offences which would meet this criteria.⁶⁴

Setting out distinct circumstances in which the powers can be used follows the reasoning in extant European case law that the protection of the fundamental right to

⁶² College of Policing, ‘Watchlists’ (21 March 2022) < <https://www.college.police.uk/app/live-facial-recognition/watchlist> > accessed 15 August 2022.

⁶³ EU AI Act (n 57) Art 5(1)(d)

⁶⁴ *Ibid* Art 5(1)(d)(iii). These offences are set out in the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002 p 1) Article 2(2). These categories of offences include: participation in a criminal organisation; terrorism; human trafficking; child sexual exploitation; illicit trafficking in narcotics; illicit trafficking in weapons; corruption; fraud; laundering of the proceeds of crime; counterfeiting currency; computer-related crime; environmental crime; facilitation of unauthorised entry and residence; murder or GBH; illicit trade in human organs; kidnapping and hostage-taking; racism and xenophobia; swindling; racketeering and extortion; counterfeiting and piracy of products; forgery; illicit trafficking in hormonal substances; illicit trafficking in nuclear materials; trafficking in stolen vehicles; rape; arson; crimes under the jurisdiction of the ICC; unlawful seizure of vessels; sabotage.

respect for private life and the protection of personal data should only be interfered with in so far as is strictly necessary.⁶⁵ Such a qualification enables the principle of proportionality to be given due regard.

The categories of crime set out in the EU AI Act relate solely to 'serious crime'. This follows the approach of the ECtHR and CJEU wherein a relevant factor in assessing the justification for the surveillance is the seriousness of the crime involved. A more serious crime will permit a more serious interference with the right to private life guaranteed under Article 8.⁶⁶ As such, the watchlist used for deployments under the AI Act represents a more proportionate measure. This offers an important safeguard for fundamental rights. In contrast, the guidance of set out by the College of Policing imposes no qualification that the offence must be a serious offence, nor is it limited to suspects and perpetrators. With the lack of relevant safeguards and the blanket and indiscriminate processing that results following the use of the technology, it is unlikely that such a broad approach would meet the requirements of strict necessity and proportionality under EU law, demonstrating an interference with fundamental rights in the processing of this personal data.

iii. Oversight arrangements

Within the finding of adequacy, a key determinant was the oversight and redress mechanisms for infringements of data subjects' rights. In finding the UK to be essentially equivalent to the EU in this regard, the adequacy decision emphasised the operational and functional independence of both the Information Commissioner and the Biometrics Commissioner.⁶⁷ The Information Commissioner's Office is the primary oversight body concerning biometric data and therefore regulates the compliance with the DPA which is engaged in the use LFR.⁶⁸ The powers of the ICO encompass both the issuing of advice and enforcement notices for breaches of data protection provisions. In the context of LFR, the ICO has largely confined itself to its advisory

⁶⁵ *Tele 2 v Post-och telestyrelsen* (Joined Cases C-203/15 and C-698/15) [2016] ECLI 970 para 96; See also judgments of 16 December 2008, C- 73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi and Satamedia* (C-73/07)[2008] ECLI 727 [56]; C-92/09 and 93/09 *Volker und Markus Schecke and Eifert* [2010] ECLI 662 [77]; , C-362/14 *Maximilian Schrems v Data Protection Commissioner* (2015) ECLI 650 [92-96]; C-293/13 and C-594-12 *Digital Rights Ireland v Minister for Communication & Ors* [2014] ECLI 238 [52].

⁶⁶ See *Ministerio Fiscal* C-207/16, ECLI:EU:2018:788.

⁶⁷ LED Adequacy (n 1) recitals 93-99 and 50

⁶⁸ DPA 2018 s 116 and Schedule 13 provides that the Information Commissioner must monitor and enforce these provisions

capacity. In line with their statutory powers, the ICO has issued an opinion concerning the protection of personal data in the context of the use of LFR by law enforcement.⁶⁹ The purpose of this opinion is to provide guidance for law enforcement through all stages to the data processing involved in the use of LFR, but it is not a binding legal framework for the use of these powers. The ICO is empowered to issue enforcement notices for data protection breaches occasioned by the use of the technology.⁷⁰ However, such powers have yet to be exercised in this law enforcement context and it remains unclear whether these powers could extend to wider fundamental rights breaches beyond data protection occasioned by the used of the technology.

In addition to the data protection oversight offered by the ICO, the use of LFR also engages the role of the Biometrics and Surveillance Camera Commissioner. The Commissioner is independent of government and issues reports on their functions, namely, for the purposes herein, on compliance with the Surveillance Camera Code of Practice and how the code is working.⁷¹ However, the Commissioner has no enforcement or inspection powers regarding surveillance camera systems. As the updated Code of Practice classes LFR as a surveillance camera system, this means that the Commissioner has no enforceable oversight role with regard to this technology. The Commissioner is only able to provide advice and guidance but no redress for individuals impacted by the deployment of this technology.⁷² This creates a lacuna in the oversight mechanisms for individuals whose rights may be impacted in a manner which effectively places them outside both the ICO and the Biometric Commissioner's remit.

For these individuals, oversight is left to the individual police forces who utilise the technology. The College of Policing guidance notes that 'Chief officers must establish their own internal governance arrangements for LFR. This should involve chief officer and PCC (or equivalent) oversight, with separation from operational decisions and decision makers where possible, to ensure sufficient independence and rigour when reviewing a force's use of LFR'.⁷³ However, there is no requirement within this guidance for either *ex ante* or *ex post* review of the technology by a body independent

⁶⁹ ICO (n 38) and DPA 2018 s 116(2) read in conjunction with Schedule 13(2)(d).

⁷⁰ Data Protection Act 2018 s 149(2)(c).

⁷¹ Protection of Freedoms Act 2012 ss 34-35.

⁷² Protection of Freedoms Act 2012 s 34.

⁷³ College of Policing (n 60) at 3.2.4.

of the police. Such a lack of independent oversight is counter to the principles within the Adequacy Decision.⁷⁴

Independent oversight is crucial in determining whether the use of the technology goes beyond that which is 'strictly necessary'. The Courts will take several factors into account, including the existence of effective safeguards and guarantees against abuse. Such an assessment will examine with existence of judicial and/or independent scrutiny, and the affected parties' rights to remedy and redress for alleged violations of their rights. It is this independent review which ensures that these powers are not abused and provides public trust in the system. In the absence of such a check on the powers of authorised bodies, questions will arise over the validity and proportionality of their actions.

A lack of independent oversight of surveillance measures is at odds with the extant jurisprudence on surveillance technologies. Independent scrutiny is crucial to ensure that the exercise of these powers comports with the rule of law and guarantee that those in power can be held accountable for their actions. It is worth noting that the Courts have held that the requirement for effective oversight can be met absent formal judicial control. The lack of judicial oversight is not, in itself, sufficient to satisfy a finding that an oversight regime is inadequate.⁷⁵ However, the mechanism must meet the standards of independent oversight. The Court must be assured that the oversight body is independent of both the Government and the interested parties.⁷⁶ The use of internal scrutiny mechanisms within the relevant police force is unlikely to satisfy these criteria.

With regard to oversight the EU AI Act offers a stricter regime, more in line with relevant fundamental rights standards. The AI Act aims to introduce a requirement that any real time use of the technology by law enforcement authorities in publicly accessible spaces receive prior authorisation 'by a judicial authority or by an independent administrative authority of the Member State'.⁷⁷ By requiring *ex ante* oversight, the EU instrument proposes stronger safeguards than those set out in the

⁷⁴ LED Adequacy (n 1) at 2.5.

⁷⁵ *Klass and Ors v Germany* App no 5029/71 (ECtHR, 6 Sept 1978) para 56 and *Szabo & Vissy v Hungary* App no 37138/14 (ECtHR, 12 Jan 2016) para 77

⁷⁶ *S & Marper v United Kingdom* App No 30562/04 and 30566/04 (ECtHR, 4 Dec 2008) para 77

⁷⁷ AI Act (n 57) Article 5(3)

UK guidance and is more likely to meet the requirements of necessity and proportionality.

iv. The Public-Private Divide

Whilst the current LFR regime offers an indication that the processing of data under these mechanisms do not comply with the fundamental rights and oversight requirements of the Adequacy Decision, these concerns are amplified when examining private-public collaboration in the use of LFR. Collaborative use of LFR technology can take several forms, including where the police provide private owners of LFR with a watchlist of persons of interest to be deployed in a publicly accessible but privately owned space; where a match is generated by a privately owned system requiring police intervention; or where a privately owned company either sells the technology to a police force or where different aspects of the system may be subcontracted to a private party.⁷⁸ For the purposes of this chapter, the focus is on the first use, that of the provision of images for watchlists to private parties. This collaboration necessarily involves the sharing of biometric data, originally processed by law enforcement with private entities, and raises additional data protection concerns.

In order for these collaborations to comply with data protection law, the parameters of the relationship must be clearly defined.⁷⁹ There should be explicit contracts or agreements to detail the information sharing arrangements, having due regard for the legal basis for the processing and the necessary data protection principles.⁸⁰ As such use involves a law enforcement authority sharing the data, it must be shared for a clear policing purpose.⁸¹ Sharing of data constitutes processing under the relevant data protection instruments and therefore there must be an appropriate legal basis for the sharing of the information.⁸² However, the powers of the police to share data are

⁷⁸ Biometrics and Forensics Ethics Group, 'Briefing note on the ethical issues arising from public-private collaboration on the use of LFR' (21 Jan 2021) <<https://www.gov.uk/government/publications/public-private-use-of-live-facial-recognition-technology-ethical-issues/briefing-note-on-the-ethical-issues-arising-from-public-private-collaboration-in-the-use-of-live-facial-recognition-technology-accessible>> accessed 2/2/22.

⁷⁹ UK GDPR Art 5(2) and Articles 24-9

⁸⁰ ICO (n 38) para 4.9.2.

⁸¹ MoPI Code of Practice definition of 'policing purpose' is: protecting life and property; preserving order; preventing the commission of offences; bringing offenders to justice; and any duty or responsibility of the police arising from common or statute law.

⁸² LED (n 2) Art 3.

broadly defined and can be governed by either statute, common law, or royal prerogatives.⁸³

The sharing of information between the police and private collaborators is not currently subject to explicit statutory regulation. In fact, these uses are excluded from the remit of much of the existing guidance. For instance, while the College of Policing APP on LFR explicitly recognises the potential for police sharing data with private companies and/or other public sector organisations operating LFR systems, it states that such activities are outside the scope of the guidance.⁸⁴ Furthermore, private organisations are not subject to the Surveillance Camera Code of Practice, so the provisions on LFR set out in this instrument may not apply to private organisations utilising police generated data. Sharing in this regard is therefore governed with a piecemeal approach. Where not explicitly provided for in statute, the police may use common law powers as the basis of their information sharing, provided they are exercised consistently with the requirements of the DPA, UK GDPR, Human Rights Act 1998, as well as applicable policy documents.

The lack of a clear legal framework means that information sharing arrangements between the police and private collaborators can rely on general agreements which lack legal effect. Key questions must be raised about the parameters of the information which law enforcement could share on the basis of these agreements. General guidance exists as to key factors to consider for information sharing agreements.⁸⁵ However, these do not set enforceable conditions on law enforcement. Notably from a fundamental rights perspective there is a lack of clear guidance as to the oversight regime or access to redress mechanisms for individuals whose data might be shared in this manner. In the absence of a clear legal framework, there is a risk that this information will be shared in instances where it is neither necessary and proportionate to do so. There are also concerns about the ability to audit the use of the information by these third parties and any subsequent onward sharing of the data. In the absence of any regulation, data subjects will struggle to exercise their rights should they be impacted by these public-private collaborations.

⁸³ LED Adequacy (n 1) Recitals 29-30.

⁸⁴ College of Policing (n 60)

⁸⁵ College of Policing, 'APP: Information Sharing' (5 Feb 2020) <<https://www.app.college.police.uk/app-content/information-management/sharing-police-information/>> accessed 18/8/2021.

Conclusion

The use of LFR raises key questions concerning both the effectiveness of the exercise of individual rights in the areas covered by the adequacy decision, as well as the operation and oversight of relevant bodies. In the absence of a clear legal framework and an assessment that the use of the powers is only done where 'strictly necessary', the interference with the sensitive personal data of individuals is disproportionate.

The lack of effective oversight over the use of the technologies is similarly indicative of a regime which is failing to give sufficient protection and redress for individuals as required under the adequacy decision. The expansion of the data processing abilities of law enforcement evidenced by LFR and the risk they pose to fundamental rights raises questions about the overall adequacy of the UK data protection regime. As the powers of law enforcement to adopt and utilise new technologies which implicate individuals' fundamental rights expand, the policies of the UK begin to diverge further from those of the EU. The extent of this divergence may very well impact on any continued finding of adequacy and the future of the EU-UK data sharing arrangements.