"A NOVEL AND CONTROVERSIAL TECHNOLOGY." ARTIFICIAL FACE RECOGNITION, PRIVACY PROTECTION, AND ALGORITHM BIAS IN EUROPE

Andrea Pin*

INTRODUCTION

Between late 2019 and mid-2020, an unprecedented controversy reached courts in Europe.[1] At stake were the thorny issues surrounding the capabilities and the risks of using Artificial Face Recognition (AFR) during policing. While the "[c]ase law [wa]s [then] virtually non-existent,"[2] the responsibility to adjudicate in this field fell upon the shoulders of British judges, who ruled largely drawing from European Union (EU) privacy regulation, "Europe's First Amendment."[3]

It might sound quite paradoxical, and even ironic, that the two courts called to adjudicate on what they qualified as "a novel and controversial technology"[4] in light of EU regulations were the High Court of Justice[5] and the Court of Appeal of England and Wales. In fact, the UK was then in the process of transitioning out of the EU.[6] Despite Brexit, *R (Bridges) v. Chief Constable of South Wales Police* Court of Appeal's unanimous ruling has left some legacy for other states' courts as well as for the Court of Justice of the European Union (CJEU).[7] As EU law is good law within the remaining twenty-seven EU member states, and domestic judges must enforce EU rules instead of incompatible domestic rules,[8] the vast portion of the Court of Appeal's ruling that relies on EU law is an obvious point of reference. And the impact of the judgment may actually spill over even beyond the EU, given its

* Associate Professor of Comparative Law at the University of Padua, Italy.

[1] Bernard Keenan, *Automatic Facial Recognition and the Intensification of Police Surveillance*, 84 MOD. L. REV. 886, 886 (2021).

[2] EU AGENCY FOR FUNDAMENTAL RTS., FACIAL RECOGNITION TECHNOLOGY: FUNDAMENTAL RIGHTS CONSIDERATIONS IN THE CONTEXT OF LAW ENFORCEMENT 4 (2019).

[3] Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUR. L.J. 140, 140 (2019).

[4] R (Bridges) v. Chief Constable of South Wales Police [2020] EWCA (Civ) 1058, at para. 201 [hereinafter *Bridges II*].

[5] R (Bridges) v. Chief Constable of South Wales Police [2019] EWHC (Admin) 2341 [hereinafter *Bridges I*].

[6] *Brexit: What You Need to Know About the UK Leaving the EU*, BBC NEWS (Dec. 30, 2020), https://www.bbc.com/news/uk-politics-32810887 [https://perma.cc/JX4H-5HZE].

[7] *See Bridges II*, EWCA (Civ) 1058, ¶¶ 62–64.

[8] EUR-LEX, *Glossary of Summaries—Primacy of EU Law*, https://eur-lex.europa.eu/summary/glossary/primacy_of_eu_law.html [https://perma.cc/JTZ7-JP32] (last visited Dec. 13, 2021).

privacy rules' ability "to unilaterally influence global regulatory standards,"[9] thanks also to the EU's large market.[10] As U.S. companies willing to sell their products within EU territories must comply with EU regulations,[11] they will have to take into account this judgment while crafting their AFR technologies.

Perhaps even more importantly, *Bridges* seems to have deeply influenced the EU's treatment of AFR technologies. The widely known[12] Artificial Intelligence Act[13] currently under consideration by the EU devotes a specific section to AFR technologies in the context of law enforcement, and, as we will see, many details of the proposed legislation resonate with *Bridges*.[14] Although there is no guarantee that the EU will end up enacting the Bill in this form, there seems to be little doubt that *Bridges* will remain a point of reference for the years to come.

All things considered, the judgment of the Court of Appeal and the events it dealt with are a good proxy to discuss the controversial exploitation of AFR within public policies.[15] More broadly, they are a perfect chance to ponder the pros and cons of using Artificial Intelligence (AI) capabilities to monitor the civil society by "analyz[ing] large volumes of footage and . . . recogniz[ing] faces . . . through analyses that take a fraction of the time and effort needed for human inspection."[16]

AFR is getting special attention in Europe to help mitigate frequent terrorist attacks.[17] Thanks to its quick development, which—according to some statistics—has

---

[9] Fernanda G. Nicola & Oreste Pollicino, *The Balkanization of Data Privacy Regulation*, 123 W. VA. L. REV. 61, 62 (2020).

[10] *Id.* at 62–63.

[11] *Id.* at 62.

[12] Carly Kind, *Containing the Canary in the AI Coalmine—the EU's Efforts to Regulate Biometrics*, ADA LOVELACE INST. (Apr. 30, 2021), https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics [https://perma.cc/SM7A-N5VP] ("While only a week old, the Commission's proposal has already achieved an impressive feat: it has shifted the policy window away from a conversation about whether to regulate artificial intelligence, opening up a new discourse about how to regulate artificial intelligence.").

[13] *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021) [hereinafter *Proposal for Harmonised Rules on AI*].

[14] *See id.* at art. 5.

[15] Madalina Busuioc, *Accountable Artificial Intelligence: Holding Algorithms to Account*, 81 PUB. ADMIN. REV. 825, 827 (2021) ("[C]alls for mechanisms to improve AI algorithm transparency and for public regulation are sharply on the rise—for instance, of facial recognition.").

[16] Aziz Z. Huq, *Constitutional Rights in the Machine-Learning State*, 105 CORNELL L. REV. 1875, 1877 (2020).

[17] *211 Terrorist Attacks Carried Out in EU Member States in 2015, New Europol Report Reveals*, EUROPOL (July 20, 2016), https://www.europol.europa.eu/newsroom/news/211-terrorist-attacks-carried-out-in-eu-member-states-in-2015-new-europol-report-reveals [https://perma.cc/43FN-CUZ8] (In 2015 there were 211 terrorist attacks within the EU); *Terrorism*

seen its failure rate decrease from 5% to 0.2% in eight years,[18] AFR could play an important role in patrolling cities, prosecuting terrorists, and discouraging emulation. This is more than just a plausible scenario, as "[i]n a number of European countries, facial recognition technologies are [already] being tested or used in different contexts in both private and public spheres."[19] The list includes Hungary, Czech Republic, Germany, France, Sweden,[20] and Italy.[21] It is no surprise, however, that it was the British courts that pioneered the case law on this subject, as its police have been particularly "active in experimenting with live facial recognition technologies."[22]

The global pandemic increased interest in the development and the deployment of AFR in Europe and elsewhere.[23] Many countries have already bet on the AFR's capabilities to fight the spread of the disease. Since this "minimally invasive technology . . . is significantly more discreet and anatomically noninvasive than other methods of collecting under-the-skin biometric data,"[24] it is becoming increasingly important.[25] Tracing the contagion,[26] identifying and isolating individuals who do not wear masks where they are compulsory[27] or violate their quarantine,[28] have become a priority for societies trying to contain the virus without freezing social mobility and the economy.[29] South Korea has implemented a holistic approach to

---

in Europe—Statistics & Facts, STATISTA (Oct. 12, 2020), https://www.statista.com/topics/3788/terrorism-in-europe/ [https://perma.cc/H4GK-KNZV] (The number fell to 119 in 2019, which was the lowest in years.).

[18] Sovantharith Seng, Mahdi Nasrullah Al-ameen & Matthew Wright, *A First Look into Users' Perceptions of Facial Recognition in the Physical World*, 105 COMPUTS. & SEC. 1, 2 (2021).

[19] *See* EU AGENCY FOR FUNDAMENTAL RTS., *supra* note 2, at 3.

[20] *See id.*

[21] Francesco Dughiero, *Acquisizioni video nel contesto urbano: la c.d. Face Recognition nel panorama italiano*, IL QUOTIDIANO GIURIDICO (Mar. 11, 2021), https://www.quotidianogiuridico.it/documents/2021/03/11/acquisizioni-video-nel-contesto-urbano-la-c-d-face-recognition-nel-panorama-italiano [https://perma.cc/4W4S-J3TW].

[22] EU AGENCY FOR FUNDAMENTAL RTS., *supra* note 2, at 11.

[23] *Facial Recognition 2021 and Beyond—Trends and Market*, I-SCOOP (2021), https://www.i-scoop.eu/facial-recognition/ [https://perma.cc/MQL2-5NL8] ("The facial recognition technology market gets driven by the COVID-19 pandemic.").

[24] Meredith Van Natta et al., *The Rise and Regulation of Thermal Facial Recognition Technology during the COVID-19 Pandemic*, 7 J. L. & BIOSCIENCES 1, 7 (2020).

[25] *Id.* at 5.

[26] Nicola Luigi Bragazzi et al., *How Big Data and Artificial Intelligence Can Help Better Manage the COVID-19 Pandemic*, 17 INT'L J. ENV'T RSCH. & PUB. HEALTH 1, 2–3, 5 (2020).

[27] Mohamed Loey et al., *A Hybrid Deep Transfer Learning Model with Machine Learning Methods for Face Mask Detection in the Era of the COVID-19 Pandemic*, 167 MEASUREMENT 1, 2 (2020).

[28] EUR. PARL., WHAT IF WE COULD FIGHT CORONAVIRUS WITH ARTIFICIAL INTELLIGENCE? (2020).

[29] Van Natta et al., *supra* note 24, at 17.

fighting the pandemic that includes "security camera footage, facial recognition technology, bank card records, and global positioning system."[30] Other tools, such as thermal-imaging wearable glasses that similarly detect temperatures of up to two-hundred people and can be paired with facial recognition software, were developed in China and marketed in the United States.[31] Australia's anti-pandemic policy similarly includes drones "equipped with thermal recognition technology."[32] The widespread requirement of wearing masks, which obstructs the face recognition process,[33] has further boosted technological development.[34] Chinese police are using a technology that can purportedly identify individuals and their temperature within groups of up to thirty people with the 95% accuracy, even though they are wearing masks.[35]

AFR raises numerous eyebrows, however, and for good reasons. AFR has the capacity to become a tool of "limitless surveillance,"[36] confirming the perception that "[w]e are surrounded,"[37] especially within the most populated urban areas.[38] The adoption of AFR tools and AFR-based policies are particularly problematic for the Old Continent. The EU has progressively developed its approach to contemporary technology around the value of privacy, both through its own regulation and by entrenching the European Convention of Human Rights (ECHR),[39] which similarly requires that its forty-seven member states—ranging from Portugal to Russia, from Finland to Cyprus—protect privacy.[40]

Bridges showcases the variety and the thickness of the legal, ethical, and political considerations that lie underneath the deployment of AFR-based police tools and its ramification within Europe and beyond.[41] More broadly, the topic of "[f]acial recognition technologies provide[s] a useful case study of the complex and unpredictable

---

[30] Sera Whitelaw, *Applications of Digital Technology in COVID-19 Pandemic Planning and Response*, 2 LANCET 435, 436 (2020).

[31] Van Natta et al., *supra* note 24, at 5.

[32] *Id.* at 6.

[33] *AI and Control of Covid-19 Coronavirus*, COUNCIL OF EUR., https://www.coe.int/en/web/artificial-intelligence/ai-and-control-of-covid-19-coronavirus [https://perma.cc/8EN4-KC58] (last visited Dec. 13, 2021).

[34] *See* Van Natta et al., *supra* note 24, at 5.

[35] *Id.*

[36] FRANK PASQUALE, NEW LAWS OF ROBOTICS: DEFENDING HUMAN EXPERTISE IN THE AGE OF AI 131 (2020) (internal quotations omitted).

[37] JOSHUA A.T. FAIRFIELD, OWNED: PROPERTY, PRIVACY, AND THE NEW DIGITAL SERFDOM 52 (2017).

[38] *Id.* at 65, 67.

[39] Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union art. 6, Oct. 26, 2012, 2012 O.J. (C 326) 1[hereinafter Treaty on European Union].

[40] Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, E.T.S. 5 (entered into force Sept. 3, 1953) [hereinafter European Convention on Human Rights].

[41] Keenan, *supra* note 1, at 893–95.

ways that norms of procedural fairness, equality, and privacy interact when the state deploys machine-learning tools to draw inferences from otherwise unilluminating data."[42] This Article uses *Bridges* as a proxy to sketch out the main legal issues that arise from AFR's policy deployment in Europe. After a quick summary of the facts and of the judgment of the court of first instance, it provides a detailed account of the Court of Appeals' judgment. Then it focuses on how the Court of Appeals balanced competing interests and how this resonates with EU rules. Finally it compares *Bridges* with the Artificial Intelligence Act issued by the European Commission.

I. THE MAGNITUDE OF THE PROBLEM AND THE FIRST EUROPEAN CASE

The EU has the reputation of having created "a *unicum*, an innovative and pervasive right to data protection and right to privacy, that has transfigured . . . other legal systems."[43] The EU Charter of Fundamental Rights[44] protects private life[45] and personal data.[46] The EU abides by the ECHR,[47] which also protects private life.[48]

---

[42] Huq, *supra* note 16, at 1900.

[43] Nicola & Pollicino, *supra* note 9, at 67.

[44] Charter of Fundamental Rights of the European Union, Oct. 26, 2012, 2012 O.J. (C 326) 2.

[45] *Id.* at art. 7 ("Everyone has the right to respect for his or her private and family life, home and communications.").

[46] *Id.* at art. 8, stating:

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

[47] *See* Treaty on European Union, *supra* note 39, at art. 6, stating:

> 2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties.
> 3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law.

[48] *See* European Convention on Human Rights, *supra* note 40, stating:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and

The most relevant body of law in the field of data protection, however, is the General Data Protection Regulation (GDPR),[49] which entered into force in 2016 replacing an earlier piece of legislation on the same subject.[50] As AFR processes facial images "through specific technical means allowing the unique identification or authentication of a natural person," it captures biometric data that is accorded special protection under the GDPR.[51]

The AFR has the potential of becoming a dangerous tool of mass surveillance for at least two reasons, which *Bridges* emphasized. First, it is much less socially transparent than other means of biometric surveillance such as fingerprints. In fact, it collects people's personal information without requiring cooperation or even knowledge of the individuals whose information is collected.[52] Second, its scale of surveillance is vast. *Bridges* dealt with the South Welsh police's deployment of AFR within a two-year span, between May 2017 and April 2019.[53] The police deployed their AFR tool during events of some popular interests, including the final match of the Champions League soccer finals, for a total of fifty deployments.[54] Thanks to the software's capacity to process up to fifty people per second,[55] the total sum of faces processed within the two years amounted to 500,000,[56] which makes up roughly for one-sixth of the total Welsh population. Of course, this does not mean that such a high portion of Welsh population was caught on AFR cameras. Many non-Welsh individuals likely participated in the events during which the technology was deployed, such as during the soccer final, and many might have been caught on camera more than once. But the number is still indicative of the type of surveillance to which AFR can give birth to. As the judicial dispute exemplifies and this Article explains, the EU's response to what seems to be a formidable privacy threat consists of putting boundaries on such a powerful technology, without ruling it out. Both EU law and *Bridges* keep the door open to AFR but set some limits and requisites.

> is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[49] Council Regulation 2016/679 of April 27, 2016, General Data Protection Regulation, 2016 O.J. (L 119) 1.

[50] *Id.*

[51] *See* EU AGENCY FOR FUNDAMENTAL RTS., *supra* note 2, at 5.

[52] *Bridges II*, EWCA (Civ) 1058 ¶ 23.

[53] *Id.* ¶ 11.

[54] *Id.*; *2,000 Wrongly Matched with Possible Criminals at Champions League*, BBC (May 4, 2018), https://www.bbc.com/news/uk-wales-south-west-wales-44007872 [https://perma.cc/QPQ2-G7KH].

[55] *Bridges II*, ¶ 16.

[56] *Id.*

A. The Issues of Bridges

In October 2018, Edward Bridges, a civil liberties campaigner living in Cardiff, sued the South Wales Police for using AFR Locate, a tool based on the *NeoFace Watch* software that the police used to experiment patrolling areas in which public events were held between 2017 and 2019.[57] The Divisional Court of the Queen's Bench Division, which acted as a court of first instance, found that the usage of AFR Locate was legitimate. Then Bridges appealed on narrower grounds.

What follows is a summary of the facts of the case and of the Divisional Court's ruling, and a thorough analysis of the Court of Appeal that focuses on the main take-aways for EU and the State Parties of the European Convention of Human Rights. It will therefore devote most of its attention to the first two complaints and elaborate on the Court of Appeal's analysis of AFR's discriminatory potential.

B. AFR Locate

The South Wales Police deployed AFR Locate in an overt manner. They installed the cameras that captured faces on poles, posts, or police vehicles; they posted warnings about its usage; police officers handed out leaflets explaining to the people roaming within the patrolled area that their face images could be captured and processed.[58]

AFR Locate operates by looking for face matches from a South Wales Police database of photographs.[59] The watch-list has the technological capacity of two-thousand images, but the list utilized during the experimentation oscillated between four-hundred and eight-hundred people.[60] The list included persons wanted on warrants, individuals who had escaped custody, people suspected of having committed crimes, persons in need of protection, individuals whose presence at a certain event was of concern, people of interest for intelligence purposes, and persons considered to be vulnerable.[61] The system generates a "similarity score" between the faces on the watch-list and those that are detected.[62] The score quantifies the probability that a given individual corresponds to one on the watch-list.[63] The operator of the system sets "a threshold value for similarity scores above which the software will alert the operator of a potential match."[64] When the software identifies a possible match, a police officer compares the camera image with the watch-list one.[65] Only if the

---

[57] *Id.* ¶ 1, 4.
[58] *Id.* ¶ 19.
[59] *Id.* ¶ 13.
[60] *Id.* ¶ 13.
[61] *Id.*
[62] *Id.* ¶ 9.
[63] *Id.*
[64] Keenan, *supra* note 1, at 887.
[65] *Bridges II*, ¶ 15.

officer confirms the match will other officers stationed nearby be notified.[66] AFR Locate also collects metadata, such as time and location, that is associated with the image, and the matches between the watch-list and the captured face image.[67]

The *Standard Operating Procedures and Data Protection Impact Assessment* in force at the Southern Welsh Police put limits on the storage of the information gathered by AFR Locate.[68] AFR Locate does not retain the facial biometrics in case of no match and the camera feed is deleted after thirty-one days, in accordance with UK regulations on standard feed retention.[69] The facial image of a match record is stored within AFR Locate for up to twenty-four hours, while information about the match lasts within the system for thirty-one days.[70] AFR Locate also deletes the watch-list's images within twenty-four hours after the deployment.[71]

C. The Facts of the Case and the Divisional Court's Ruling

Bridges complained that AFR Locate had captured his image on two occasions.[72] The first event he mentioned took place on December 21, 2017, while he was visiting a busy shopping area of Cardiff.[73] The second occasion was on March 27, 2018, when he was attending the *Defence Procurement, Research, Technology and Export-ability Exhibition*.[74] He claimed that in neither case he had been warned that he could be caught on camera by AFR Locate.[75]

On the first occasion, AFR Locate operated for eight hours and searched for matches within three watch-lists, which included people being suspected of having committed a serious crime, people wanted on warrants, and suspects.[76] AFR Locate then returned ten possible matches, out of which two turned out to be wrong.[77] On the second occasion, the police deployed AFR Locate in consideration of what happened during an earlier annual *Exhibition*, when bomb hoax calls had disrupted the event.[78] The watch-list included people who had been arrested in the past at the same event, or those with outstanding warrants, and other suspects.[79] There was one match, which turned out to be correct.[80]

---

[66] *Id.*
[67] *Id.* ¶ 21.
[68] *Id.* ¶ 18.
[69] *Id.* ¶ 10.
[70] *Id.* ¶ 10.
[71] *Id.*
[72] *Id.* ¶ 25.
[73] *Id.*
[74] *Id.*
[75] *Id.* ¶ 27.
[76] *Id.* ¶ 26.
[77] *Id.*
[78] *Id.* ¶ 28.
[79] *Id.*
[80] *Id.* ¶ 29.

Bridges complained both that the police had used such technology against him twice and that they could do so in the future (interestingly enough, there was no evidence that AFR Locate had captured Bridges's facial images, as the recordings had been duly destroyed in the meantime, in compliance with the police rules).[81] More specifically, he complained that the usage of AFR Locate was in breach of (1) Article 8 of the ECHR, which protects private life; (2) data protection regulation, as enshrined in the Data Protection Acts (DPA) of 1998 and 2018; and (3) the *Public Sector Equality Duty* (PSED).[82] The Divisional Court issued its ruling on September 4, 2019. It conceded that, despite being "manifest in public," "AFR-derived biometric data [wa]s information of an intrinsically private character" and was therefore covered by Article 8 of the ECHR.[83] Article 8 ECHR states that:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[84]

The Divisional Court found that AFR Locate met Article 8's requirement.[85] In fact, the Court noted, the police enjoyed a legal basis for such practice: using cameras to obtain biometric data fell within their common law powers and was justified by the public interests involved, which revolved around safety and crime prevention and prosecution.[86]

Regarding the DPA, the Divisional Court also found that the usage of AFR was compatible with the existing regulations.[87] In fact, in pursuance of Article 35 of the GDPR, the DPA required that "where a type of processing is likely to result in a high risk to the rights and freedoms of individuals," "a data protection impact assessment" was needed.[88] In the Divisional Court's eyes, the police had duly completed such an assessment.

In a nutshell, the Divisional Court found that the common law police powers provided the police with the necessary legal ground; that the process was carried out

---

[81] *Id.* ¶ 34.
[82] *Id.* ¶ 52.
[83] *Id.* ¶ 36.
[84] European Convention on Human Rights, *supra* note 40.
[85] *Bridges II*, EWCA (Civ) 1058 ¶ 2.
[86] *See id.* ¶ 38.
[87] *Id.* at 86.
[88] *Id.* ¶ 29.

on the basis of a policy document that the police had duly put in place; that a data protection impact assessment had been carried out; and that AFR Locate was strictly necessary for the purpose of law enforcement.[89]

Finally, the Divisional Court considered and dismissed the claim that the use of AFT Locate could cause impermissible gender or ethnic discrimination, which were prohibited under the DPED.[90] The Court, in fact, found no evidence that the software that AFR Locate was discriminating against female or minority ethnic individuals by producing higher rates of positive matches.

The Divisional Court disagreed with the police on a key point. The police had put forward the argument that only individuals included in the watch-lists could claim that their biometric information had been processed and therefore seek legal protection.[91] In fact, the Court noted, everyone captured by the cameras had been processed and uniquely identified, regardless of whether the software had returned any matches with the watch-lists.[92]

II. THE COURT OF APPEAL'S RULING

When Bridges appealed, he had already won on a key point. The Divisional Court had decided that face recognition ending with no match still constituted *processing* biometric data as defined under the DPA.[93] This meant that *anyone* caught on camera was covered by regulations regarding sensitive personal data. Of course, given that the recordings were canceled shortly after the deployment of AFR Locate, it was impossible to determine whether someone who was not within a watch-list had been caught on camera, as happened to Bridges. As a result, anyone claiming to have been in the surroundings during an AFR Locate deployment could sue in court.

When appealing the first ruling, Bridges distilled a series of claims. Some of them revolved around the protection of his private life under Article 8 of the ECHR and the Human Rights Act 1998, which the UK introduced to domesticate the ECHR's protection; some pertained to the protection that the UK granted him in pursuance of the EU's GDPR; one argued for the violation of equality under the PSED.[94] All in all, virtually all the claims that Bridges made stemmed either from EU law or the ECHR. The ruling is therefore extremely relevant for the great deal of countries that are EU members or parties to the Convention.

---

[89] *See id.* ¶¶ 50–51.
[90] *See Bridges II*, EWCA (Civ) 1058 ¶ 52.
[91] *Id.* ¶ 89.
[92] *Id.* ¶ 53.
[93] *See id.*; *supra* notes 87–88 and accompanying text.
[94] *Id.* ¶ 91.

A. The Legal Background for the AFR Locate's Deployment and Article 8 ECHR's Protection of Private Life

The first issue that the Court tackled was whether the deployment of AFR Locate was consistent with Article 8 of the ECHR.[95] As to the requisite that there be a sufficient legal ground, the Court of Appeal's *prima facie* answer was in the positive.[96] The Court of Appeal shared the Divisional Court's view that the legislation and the policy of the South Wales Police provided some background for the deployment of AFR.[97]

The Court then turned to the specificities of the case at stake. The case—the Court noted—was novel.[98] The South Wales Police had mistakenly analogized the capture of facial features with taking photographs or using CCTV cameras.[99] But the two scenarios differed on three decisive grounds. First, AFR Locate "involve[d] the capturing of the images and processing of digital information of a large number of members of the public, in circumstances in which . . . the vast majority of them will be of no interest whatsoever to the police."[100] Second, the gathering of facial biometrics was different from ordinary photographs, as it concerned "sensitive" personal data.[101] Third, the data was "processed in an automated way."[102]

Overall, the Court found that AFR and its protocol were so invasive of individual privacy that they needed to be based on a particularly detailed legal framework.[103] The Court of Appeal's in-depth analysis found that the unique potential of AFR required a more robust and detailed legal framework than what the South Wales' Police had put in place.[104] Compared with the requirements of Article 8 of the ECHR, the protocols on the deployment and utilization of AFR Locate gave too much discretion to the police in handling the technology.[105]

More specifically, the Court noted, the legal background failed to specify two critical aspects of the AFR's deployments: who could be included in the watch-list, and the criteria determining where AFR could be deployed.[106] The South Wales Police documents in this field only required the existence of a "proper law enforcement purpose," for which the deployment had to be considered as "necessary."[107] But no further specification was available. Moreover, the document itself specified

---

[95] *See id.* ¶ 2.
[96] *Id.* ¶ 92.
[97] *See id.* ¶ 69.
[98] *Id.* ¶ 86.
[99] *Id.* ¶ 85.
[100] *Id.* ¶ 87.
[101] *Id.* ¶ 88.
[102] Id. ¶ 89.
[103] *See* Keenan, *supra* note 1, at 891.
[104] *Bridges II*, EWCA (Civ) 1058 ¶¶ 90, 93–94.
[105] *Id.* ¶ 91.
[106] *Id.*
[107] *Id.* ¶ 92.

that the software discarded the facial biometrics for which there was no match in the watch-list, but did not make this procedure an explicit requirement as a requisite for the deployment of AFR Locate.[108] Overall, there was no guarantee that the discretionary usage of the software could not target specific individuals by trying to locate and track them down: "it will often, perhaps always, be the case that the location will be determined by whether the police have reason to believe that people on the watch-list are going to be at that location."[109] To put it shortly, behind a veneer of neutrality, the police could exploit AFR Locate to arbitrarily chase specific individuals.

B. The Protection of Privacy and the Discretionary Policy Powers

The Court of Appeal then moved on to address the challenges revolving around EU law. The Court recalled that, according to the DPA 2018 that incorporated the GDPR's privacy regulation,[110] the processing of personal data for law enforcement purposes was legitimate only if was done with the subject's consent or was necessary.[111] More specifically, "sensitive processing"—a concept that included AFR Locate's operations—was allowed only when "strictly necessary" for the purpose of enforcing the law and had to be carried out in accordance with an appropriate policy document.[112]

The Court reviewed the relevant documents in place, focusing on the *Surveillance Camera Code of Practice*, which the British Secretary of State for the Home Department had issued in June 2013.[113] The Code, the Court noted, did make general reference to AFR, but did not deal with it specifically.[114] Another document of interest for the Court was the guidance published by the Surveillance Camera Commissioner in March 2019, entitled *The Police Use of Automated Facial Recognition Technology with Surveillance Camera System*.[115] The Court also noted that this text used very general terms, without specifying who could "be put on a watch-list" and "where AFR [could] be deployed," although both aspects were critical for its legitimacy.[116] Neither did the South Wales Police *Standard Operating Procedure* document, which described how AFR Locate worked and standards for narrowing down the pool of people that could end up on the list.[117] As a result, the Court was of the view that the existing legal framework did not provide enough details to circumscribe and

---

[108] *Id.* ¶ 93.
[109] *Id.* ¶ 96.
[110] *See* Celine Castets-Renard, *Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making*, 30 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 91, 131 (2019).
[111] *Bridges II*, EWCA (Civ) 1058 ¶ 101.
[112] *Id.* ¶ 102.
[113] *Id.* ¶ 114.
[114] *Id.*
[115] *Id.* ¶ 119.
[116] *Id.* ¶ 120.
[117] *Id.* ¶¶ 128–29.

later to review specific deployments of AFR Locate, therefore leaving too much discretion to the police.[118]

The Court concluded by noting that, notwithstanding the breadth of AFR deployments—AFR Locate was being tested "in all event types ranging from high volume music and sporting events to indoor arenas"[119]—no public authority in the UK had issued sufficient guidelines or protocols to constrain it.[120] The Court thus found ample evidence that AFR Locate did not have adequate boundaries.

C. The Requisites of the Privacy Assessment

The third ground for appeal also revolved around the compliance of AFR Locate's deployment policies with the regulations stemming from the UK's membership in the EU.[121] Now at stake was Section 64 of the Data Protection Act 2018, which requires that a "Data Protection Impact Assessment" before biometric processing.[122] The Assessment should include a description of the processing operations, "the risks to the rights and freedoms of data subjects," the measures intended to protect them, and the additional safeguards that should be put in place.[123] Once again, Bridges claimed that the Assessment did not consider the protection of Article 8 of the ECHR adequately, and that it overlooked the fact that AFR Locate processed the facial biometrics also of those who did not have a match in the watch-lists.[124] He thus reiterated his concern for the AFR Locate's "ambitious scale of the collection" of biometric data and its "blanket and indiscriminate basis."[125]

The Court of Appeal repeated its statement about the excessive discretionary powers of the police in deploying AFR Locate.[126] The Court now agreed with Bridges that the Data Protection Impact Assessment had also failed to address the selection of the individuals to put on watch-lists and the locations within which the software would be deployed.[127] Consequently, the Assessment had failed to address the discretionary powers that surrounded the watch-lists and the places where the software had to be deployed.[128]

---

[118] *Id.* ¶¶ 121–24.
[119] *Id.* ¶ 130.
[120] *Id.*
[121] *Id.* ¶ 145.
[122] The Data Protection Act 2018, c.12 (UK), https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [https://perma.cc/KH8U-Q8HK].
[123] *Id.*
[124] *Bridges II*, EWCA (Civ) 1058 ¶ 145.
[125] *Id.* ¶ 148.
[126] *Id.* ¶¶ 164–202.
[127] *Id.* ¶ 152.
[128] *Id.* ¶ 153–54.

D. The Existence of an Appropriate Policy Document

The Court of Appeal then moved to consider Section 42 of the Data Protection Act 2018. Section 42 sets out the requisites of an "appropriate policy document" in the field of sensitive processing.[129] It states that such a document needs to "[e]xplain the controller's procedures for securing compliance with the data protection principles," including the retention and erasure of personal data.[130] Bridges complained that the Divisional Court had urged the South Wales Police to provide the document with more details, thus leaving to the police itself the duty to implement them, while it should have made a judgment on the matter.[131] The Court of Appeal, however, found that the Divisional Court did assess the document's contents: the Information Commissioner—the independent privacy regulatory authority in the UK—also found the document to be in compliance with Article 42 of the Data Protection Act.[132]

E. The Public Sector Equality Duty

The fifth and final ground of appeal revolved around the Equality Act 2010, which included the *Public Sector Equality Duty* (PSED).[133] Both documents are a result of the UK's membership of the EU.[134] Section 149(1) of the Equality Act requires that public authorities "eliminate discrimination," "advance equality of opportunity," and "foster good relations" between persons who share a relevant protected characteristic and persons who do not share it.[135] *Bridges* complained that the South Wales Police failed to assess the potential AFR's discrimination in the fields of race and sex, which are protected by the Equality Act.[136]

The Court of Appeal here distanced itself from the Divisional Court. The latter had found no evidence of race or sex discrimination and dismissed the complaint rather easily, devoting a very little part of its opinion to the subject.[137] On the contrary, the Court of Appeal embarked on a rather in-depth analysis of the possibility that AFR

---

[129] The Data Protection Act 2018, *supra* note 122, at § 42.

[130] *Id.*

[131] *Bridges II*, EWCA (Civ) 1058 ¶ 157.

[132] *Id.* ¶¶ 160–62.

[133] *Id.* ¶ 163.

[134] *See* DEPT. FOR EXITING THE EU, EQUALITY ANALYSIS: EUROPEAN UNION WITHDRAWAL BILL, 2017, ¶ 8 (U.K.) ("The Equality Act 2010 consolidated decades of domestic legislation and transposed EU law. The Government is committed to ensuring that the protections in the Equality Act 2010 will continue to apply once we have left the EU. This will ensure the continued protection of people's rights not to be discriminated against, harassed or victimised in the provision of goods, services and public functions, housing, transport and education.").

[135] *Bridges II*, EWCA (Civ) 1058 ¶ 163.

[136] *Id.* ¶ 164.

[137] Andrea Pin, *Non esiste la "pallottola d'argento. L'Artificial Face Recognition al vaglio giudiziario per la prima volta*, 41 DIRITTO PUBBLICO COMPARATO ED EUROPEO ONLINE 3075, 3081 (2020).

includes discrimination.[138] Its ruling on this matter thus resonated strongly with the broader concerns aired by data scientists that AFR systems may embed racial and sex biases[139] and therefore threaten civil rights,[140] especially in the contexts of law enforcement.[141]

Bridges argued that the South Wales Police contravened the PSED's "positive duty" to evaluate the potential race and sex biases and that they did not give "due regard to the need to eliminate such discrimination."[142] After carrying out an initial assessment in 2017, Bridges argued, the police failed to follow up and review their assessment of the potentially discriminatory impact of AFR thereafter.[143]

Bridges had failed to persuade the Divisional Court. That Court had even seen an "air of unreality" in Bridges's argument that AFR Locate's algorithm could include racial or sex biases.[144] The Court of Appeal adamantly rejected the Divisional Court's approach, stating that "[o]n the contrary, [the complaint about discrimination seemed] to raise a serious issue of public concern, which ought to be considered properly by" the South Wales Police.[145]

The Court of Appeal clarified what PSED required from public powers. The PSED, it stated, is "a duty of process and not outcome."[146] The fact that what was due was a process and not a result, however, did not "diminish its importance"[147]:

> Public law is often concerned with the process by which a decision is taken and not with the substance of that decision. This is for at least two reasons. First, good processes are more likely to lead to better informed, and therefore better, decisions. Secondly, whatever the outcome, good processes help to make public authorities accountable to the public.[148]

PSED's duty of process discharged a critical role for the integration of AI-based tools within public policies, as it helped "to reassure members of the public, whatever their

---

[138] *Bridges II*, EWCA (Civ) 1058 ¶¶ 164–202.

[139] Joy Buolamwini & Timint Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research*, 81 MACH. LEARNING RSCH. 1 (2018).

[140] *Id.* at 2 ("False positives and unwarranted searches [stemming from mistaken AFR identifications] pose a threat to civil liberties.").

[141] *Id.* at 3 ("Past research has also shown that the accuracies of face recognition systems used by US-based law enforcement are systematically lower for people labeled female, Black, or between the ages of 18–30 than for other demographic cohorts.").

[142] *Bridges II*, ¶ 165.

[143] *Id.* ¶ 168.

[144] *See Bridges I*, EWCA (Admin) 2341 ¶ 153.

[145] *Bridges II*, ¶ 173.

[146] *Id.* ¶ 176.

[147] *Id.*

[148] *Id.* ¶ 176.

race or sex, that their interests have been properly taken into account before policies are formulated or brought into effect."[149]

Overall, the Court of Appeal concluded that "the PSED is so important [because] it requires a public authority to give thought to the potential impact of a new policy which may appear to it to be neutral but which may turn out in fact to have a disproportionate impact on certain sections of the population."[150] This approach required that public authorities make sure that they do "not inadvertently overlook information which [they] should take into account" in matters of quality.[151]

Having set the ground for further reflections, the Court of Appeal then noticed that the Divisional Court was "particularly impressed" by two aspects.[152] First, the Divisional Court emphasized that in cases of a positive match, the software did not trigger immediate human intervention.[153] In fact, "two human beings, including at least one police officer," had to decide "to act on the positive match."[154] Secondly, the Divisional Court was persuaded by the statements of Dominic Edgell, an officer in the South Wales Police's Digital Services Division, who testified as an expert in the field that "there was virtually no difference in the statistics as to race and gender."[155] The Court of Appeal disagreed with the Divisional Court on both grounds.

The Court of Appeal found that the human intervention was not sufficient to fulfil the PSED's duty to pursue equality.[156] In fact, "human beings [could] also make mistakes"; and this was "particularly acknowledged in the context of identification."[157] After all, the Court noted, in criminal trials juries are routinely given "warnings . . . about how identification can be mistaken, in particular where a person has never seen the person being identified before."[158] Critical for the Court, however, was that the South Wales Police had "not obtain[ed] information for themselves about the possible bias which the software they use[d] may have [had]."[159] In the Court of Appeal's eyes, such a superficial approach was sufficient to conclude that the police had not met the PSED's requirement.

As to the witnesses' testimony, the Court also disagreed with the Divisional Court. The Court of Appeal found the statements offered by Dominic Edgell, to which the Divisional Court had attached great weight, to be unpersuasive.[160] Edgell reviewed the deployments of AFR Locate after the FIFA Champions League final and between

---

[149] *Id.* ¶ 176.
[150] *Id.* ¶ 179.
[151] *Id.* ¶ 182.
[152] *See id.* ¶ 183.
[153] *Id.* ¶ 184.
[154] *Id.*
[155] *Id.* ¶ 186.
[156] *See id.* ¶ 185.
[157] *Id.* ¶ 105.
[158] *Id.*
[159] *Id.*
[160] *See id.* ¶ 191.

mid-2017 until mid-2018 and found no evidence of bias.[161] Throughout that period, AFR Locate generated 290 alerts: 82 were true positives, while 208 were false positives.[162] From the point of view of sex, within the group of individuals who alerted the system, 65% were males, and 34% of this group were true positives.[163] Within the female group, only 18%—a smaller minority—were true positives.[164] Female false alerts primarily derived from matches to two individuals within the watch-list whom the AFR software provider referred to as "lamb."[165] A person is considered a "lamb" if her face has such generic features that it generates a particularly high number of false matches.[166] From the point of view of the race, 98% of the true positives were "white north European", while 98.5% of the false positives were also "white north European."[167]

Considering the statistics, the Court was not persuaded with Edgell's view that the software did comply with PSED. It emphasized that the software could indeed have "an inbuilt bias, which need[ed] to be tested."[168] Anil Jain, a computer science scholar, reinforced this impression when he testified that AFR technology's performance largely depended on the training datasets.[169] A demographically unbalanced dataset easily results in software biases and therefore demographically uneven false alerts.[170]

As details about the software were not available because of their commercial sensitivity, the Court of Appeal noted that the South Wales Police and its witnesses provided very generic statements, such as the routine updating of the software and witness statements that the algorithm's training did include individuals of various ethnic groups.[171] This did not satisfy the Court of Appeal, which, after Jain's testimony, was of the view that "[a]s a minimum for confirming whether an AFR system is biased, the database statistics, such as the number of males to females, and different races considered, would need to be known."[172] The Court thus concluded that the South Wales Police did not fulfil the PSED requirements, as it did not have sufficient information to verify that "the software program in this case [did] not have an unacceptable bias on grounds of race and sex."[173]

The Court accepted that the police did not have knowledge of the specifics of AFR Locate because of nondisclosure policies, but this did not exempt them from

---

[161] *See id.* ¶¶ 187, 190.
[162] *See id.* ¶ 187.
[163] *Id.* ¶ 188.
[164] *Id.*
[165] *Id.*
[166] *Id.*
[167] *Id.* ¶ 189.
[168] *Id.* ¶ 191.
[169] *See id.* ¶ 193.
[170] *See id.*
[171] *See id.* ¶¶ 195–97.
[172] *Id.* ¶ 193.
[173] *Id.* ¶ 199.

their "own, non-delegable, duty" to pursue equality under PSED.[174] The Court thus hoped that:

> [A]s AFR is a novel and controversial technology, all police forces that intend to use it in the future would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias.[175]

This last ground of appeal, which found the South Wales Police impermissibly relying on belief in the absence of software bias, is a memento for the public and institutions alike that AI tools are "uneven across racial, gender, and age lines."[176] The Court of Appeal showed deep awareness of "the potential for machine error and unfair discrimination in the context of automated decision-making and profiling."[177]

The Divisional Court's judgment that quickly dismissed the discrimination claim seemed to incorporate the belief that "generally speaking, algorithms are equalitarian and nondiscriminatory."[178] In doing so, however, the Divisional Court rejected both scientific evidence and legal values.[179] As has become apparent, AI-based technology can "encode human biases, blind spots, or otherwise normatively troubling assumptions or regularities derived from training data, outcome variables or other design margins."[180] AFR is no exception; actually, it epitomizes the phenomenon, as the biases it embeds can fight the process of face recognition itself by misidentifying facial images.[181] The problem has already surfaced time and again in the United States, where AFR techniques have misidentified criminals, leading to the arrest of innocent people just because the software returned wrong matches.[182] The Divisional Court's superficial consideration of the issue was also at odds with the heightened legal concern for the risks of discrimination. In fact, legal "discrimination may be unintended, indirect, or non-comparative. The focus [must be] on the effect on the victim."[183]

---

[174] *Id.* ¶ 199.

[175] *Id.* ¶ 201.

[176] Huq, *supra* note 16, at 1901.

[177] LEE A. BYGRAVE, *Minding the Machine v2.0*, *in* ALGORITHMIC REGULATION 252 (Karen Yeung & Martin Lodge eds., 2019) (citing Recital 17 of the GDPR).

[178] *See* JORDI NIEVA-FENOLL, INTELLIGENZA ARTIFICIALE E PROCESSO 122 (2019).

[179] *Id.* at 123–24 (describing the rigid manner in which artificial intelligence systems apply legal doctrine leading to unintended outcomes).

[180] Huq, *supra* note 16, at 1923–24.

[181] *See, e.g.*, Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [https://perma.cc/99UK-R95N].

[182] *Id.* (telling the story of "the third known Black man to be wrongfully arrested based on face recognition.").

[183] TARUNABH KHAITAN, A THEORY OF DISCRIMINATION LAW 2 (2015).

Overall, the Court of Appeal's judgment confirms the impression that, according to European law and European legal culture more broadly, human beings discharging public offices may seek *support*, and not *replacement*, in automated processes.[184] Limiting the role of AI in law enforcement may not be enough to avoid distortions, however. One of the aspects of utmost concern in deploying AI-based tools is the "interaction between the algorithmic output and the human decision-maker."[185] Humans may excessively rely on algorithms and be reluctant to scrutinize their outputs closely. As human agents may be prone to accept rather than challenge AFR Locate, the Court of Appeal's decision was right in emphasizing that police protocols embedding AI tools must be informed by a strong awareness that automated processes may include biases and try to prevent them, without relying too much on human oversight.

The Court of Appeal's approach resonates with the EU's take on discrimination and is therefore likely to have an impact on future cases and on the adoption of AFR tools. Although EU law does not prescribe specific positive measures to prevent discrimination,[186] it does, however, shift part of the burden of proof from the subject claiming to have been discriminated against to the respondent.[187] Requiring that police forces demonstrate that they have taken into proper account the risk of discrimination while deploying AFR technologies, as the Court of Appeal has done, echoes that shift.

III. BALANCING COMPETING INTERESTS: THE COURT OF APPEAL'S TAKE

In deciding that AFR Locate's deployment lacked a sufficient legal framework, the Court of Appeal made some additional observations on how to test whether the utilization of such a tool was a proportionate limitation on the rights of an individual.[188] Strictly speaking, there was no need for the Court to do so, as AFR Locate already lacked the preliminary requisite of a legal basis for such limitation. The Court of Appeal did not specify why it decided to assess the proportionality of the measure at stake; it likely did so, however, because the proportionality scrutiny is

---

[184] BYGRAVE, *supra* note 177, at 253.

[185] Busuioc, *supra* note 15, at 4.

[186] *Joint Rep. on the Application of Council Directive 2000/43/EC of 29 June 2000 Implementing the Principle of Equal Treatment Between Persons Irrespective of Racial or Ethnic Origin ('Racial Equality Directive') and of Council Directive 2000/78/EC of 27 November 2000 Establishing a General Framework for Equal Treatment in Employment and Occupation ('Employment Equality Directive')*, at 9, COM (2014) 2 final (Jan. 17, 2014) ("The Directives specifically allow but do not oblige the Member States to maintain or adopt specific measures to prevent or compensate for disadvantages linked to any of the grounds covered by the Directives.").

[187] *Id.* ("A key element necessary to ensure the correct handling of discrimination claims is the shift in burden of proof before the courts or other competent authorities. This means that where a person claiming to be a victim of discrimination can establish facts from which it may be presumed that discrimination has occurred, it is for the respondent to prove that there has been no discrimination.").

[188] *Bridges II*, EWCA (Civ) 1058 ¶ 131.

the standard way through which the EU Court of Justice, the European Court of Human Rights, and several Continental courts review public policies that interfere with fundamental rights.[189] The Court of Appeal's observations are therefore particularly significant, as they will likely provide other judges, within as well as outside the UK, with a template around which they can build their own judgments and public authorities can shape their own policies of AFR deployment.

The Court of Appeal reflected on the proportionality assessment required by Article 8 ECHR.[190] In the UK's judicial analysis, a limitation of a Convention's right is justified only if (I) "the objective of the measure pursued is sufficiently important to justify the limitation"; (II) the limitation "is rationally connected to its objective"; (III) there is no "less intrusive measure [that] could have been used without unacceptably compromising the objective"; and (IV) "having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community."[191]

The Court of Appeal focused on the last prong of this test, namely the balancing between the individual's rights and the community's interests, as this was the only part of the test that Bridges criticized.[192] The Divisional Court had found the balance struck to be legitimate, as "AFR Locate was deployed in an open and transparent way, with significant public engagement . . . [I]t was used for a limited time, and covered a limited footprint. It was deployed for the specific and limited purpose of seeking to identify particular individuals . . . ." Moreover, with the exception of Bridges, "[n]obody complained as to their treatment" and "[a]ny interference with the [appellant]'s Article 8 rights would have been very limited."[193]

In the Court of Appeal, Bridges made two arguments. First, he noted that the Divisional Court had made a proportionality assessment based on the "*actual*" result of an operation, not on its "*anticipated*" benefits.[194] In other words, Bridges argued that the assessment evaluated the results of the deployment of AFR Locate, whereas it should have considered the expectations that the police had when they decided to use this tool. The Court of Appeal dismissed this charge easily: as the police looked for significant numbers of individuals, while the matches were few, an *ex ante* proportionality assessment of the measure would have been more in favor of the police rather than of the appellant.[195]

Bridges's second argument targeted how the Divisional Court examined the "cost" side of the proportionality balance.[196] In fact, the appellant explained, measuring the

---

[189] Alec Stone Sweet & Jude Mathews, *Proportionality Balancing and Global Constitutionalism*, 47 COLUM. J. TRANSNAT'L L. 72, 74 (2008).

[190] *Bridges II*, EWCA (Civ) 1058 ¶ 131.

[191] *Id.* ¶ 132 (citing the Divisional Court).

[192] *Id.* ¶ 133.

[193] *Id.* ¶ 133 (citing ¶ 101 of the Divisional Court decision).

[194] *Id.* ¶¶ 134–35.

[195] *Id.* ¶ 135.

[196] *Id.* ¶ 136.

interference did not mean considering only the infringement of the appellant's right to private life, but also of "all other members of the public" who participated in the events in which the appellant could have been caught on camera.[197] The Court also dismissed this argument on two grounds. First, it emphasized that the "substance of the complaint" of Bridges against the deployment of AFR Locate was about "him, not anyone else."[198] Second, the Court stressed, measuring the impact of an interference with a fundamental right on a group of people did not mean adding up the number of interferences arithmetically to end up with a total sum.[199] "The balancing exercise which the principle of proportionality require[d] [wa]s not a mathematical one; it [wa]s an exercise which call[ed] for judgment."[200] The Court of Appeal thus offered one important insight on how to evaluate public policies' interferences with fundamental rights—namely, that measuring the impact of the interference on a wider public does not end up in an arithmetic sum, but in a legal analysis of the interests involved.[201]

IV. *BRIDGES* AND THE ARTIFICIAL INTELLIGENCE ACT

In an attempt to keep abreast of AI developments, EU institutions are considering introducing the Artificial Intelligence Act.[202] This piece of legislation would strengthen the "legal framework for trustworthy AI"[203] through a uniform EU regulation[204] that apples "to providers of AI systems . . . irrespective of whether they are established within the [EU] or in a third country, and to users of AI systems established within the [EU]."[205] The proposal aims to lay down "the minimum necessary requirements to address the risks and problems linked to AI," avoid creating "unnecessary restrictions to trade," or jeopardizing the market of technologies,[206] while still "addressing the opacity, complexity, bias, a certain degree of unpredictability and partially autonomous behavior of certain AI systems," and ensuring "their compatibility with fundamental rights."[207] The balance that the Act strikes displays awareness of the fact that AFR technologies can "evoke a feeling of constant surveillance and indirectly

---

[197] *Id.*
[198] *Id.* ¶ 142.
[199] *Id.* ¶ 143.
[200] *Id.*
[201] *Id.* ¶ 143.
[202] *Proposal for Harmonised Rules on AI*, *supra* note 13, at 1.
[203] *Id.* at 1.
[204] *Id.* at 7.
[205] *Id.* at 20.
[206] The proposal itself states that it "will not apply to those AI systems that have been placed on the market or put into service before one year has elapsed from the date of application" of the Act itself. *Id.* at 3, 5.
[207] *Id.* at 2.

dissuade the exercise of the freedom of assembly and other fundamental rights,"[208] clearly echoing *Bridges*'s fears.

The Act takes on a "risk-based approach,"[209] as it identifies uses of AI that create acceptable, high, and low or minimal risks.[210] Each rank has its own requirement. On a general level, remote biometric identification of natural persons in publicly accessible places[211] is considered a high-risk use of AI.[212] The Act requires that high-risk practices take place only under human supervision,[213] which is one of the cornerstones of *Bridges.*

The Act, however, draws a distinction between "real-time" and "post" remote biometric identifications.[214] In the former case "the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay."[215] The distinction is relevant because the Act introduces a general prohibition of using "'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement."[216] The uses of such technology to identify individuals in "real-time" for purposes other than law enforcement thus do not suffer from the same limitation, although they are still qualified as high-risk practices.[217] The special attention that the Act devotes to AFR technologies therefore coincides with *Bridges*, as the deployment of AFR Locate was done in public spaces, through a "real-time" protocol, and for the purpose of law enforcement.[218] The analogies do not end up here, however.

---

[208] *Proposal for Harmonised Rules on AI*, *supra* note 13, at 21.

[209] *Id.* at 12.

[210] *Id.*

[211] The European Commission stated:

> Publicly accessible space should be understood as referring to any physical place that is accessible to the public, irrespective of whether the place in question is privately or publicly owned . . . in addition to public spaces such as streets, relevant parts of government buildings and most transport infrastructure, spaces such as cinemas, theatres, shops and shopping centres are normally also publicly accessible. Whether a given space is accessible to the public should however be determined on a case-by-case basis, having regard to the specificities of the individual situation at hand.

Id. at 19–20.

[212] *Annex III to the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at 4, COM (2021) 206 final (Apr. 21, 2021).

[213] *Proposal for Harmonised Rules on AI*, *supra* note 13, at 15.

[214] *Id.* at 19.

[215] *Id.*

[216] *Id.* at 13.

[217] *See* Kind, *supra* note 12.

[218] *Bridges II*, EWCA (Civ) 1058 ¶ 14.

The Act explicitly prohibits the use of "real-time" AFR recognition systems for the purpose of law enforcement, "unless and in as far as such use is strictly necessary" for the achievement of a narrow list of objectives: (1) searching for specific potential victims of crime; (2) preventing "specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack"; (3) the "detection, localization, identification or prosecution of a perpetrator or suspect of a criminal offence" for a limited list of crimes of a certain relevance.[219] The list of occasions within which law enforcement can deploy AFR technologies is strikingly similar to the types of watch-lists that the Court of Appeal scrutinized, although the Act is certainly narrower and more precise.

As is standard under EU law, the Act requires that public bodies assess whether the deployment of AFR is necessary and proportionate, "in particular as regards the temporal, geographic and personal limitation."[220] They must consider the circumstances before deploying AFR techniques. More specifically, they need to ponder "the seriousness, probability and scale of the harm" in case the AFR is or is not deployed.[221]

The teaching of *Bridges* about the necessity to adequately constrain police powers to patrol publicly accessible places finds its parallel in the Act's requisite that states willing to exploit AFR's capabilities for law enforcement purposes lay down "the necessary detailed rules" for the carrying out of such activities.[222] The Act reiterates its preoccupation about the abusive exploitation of such technique to the extent that it requires that "each individual use" of AFR is authorized by "a judicial authority or by an independent administrative authority," unless there is a "justified situation of urgency."[223]

The draft bill seems to have read *Bridges* accurately. It echoes the judgment's attempt to put boundaries to police powers, narrows its scope of utilization, and ensures that it does not target specific individuals without a reason. Overall, the Act makes clear that AFR technologies deployed in "real-time" must pursue public goals of a considerable relevance, as their sheer deployment tends to transform the patrolling of public places into mass-surveillance hubs.

CONCLUSION: IS AFR ANY GOOD? A EUROPEAN LESSON

At a superficial level, AFR deployments may not seem to be invasive. What the CJEU has already said about fingerprints could be considered as particularly revealing: "[T]his is not an operation of an intimate nature. Nor does it cause any particular physical or mental discomfort to the person affected any more than when

---

[219] *Proposal for Harmonised Rules on AI*, *supra* note 13, at 44.
[220] *Id.* at 44.
[221] *Id.*
[222] *Id.* at 44–45.
[223] *Id.* at 44.

that person's facial image is taken."[224] EU populations also seem to approve the deployment of AFR technologies, especially for police purposes.[225] But actually AFR does capture the unique features of an individual's face.[226] Although it does not require any cooperation from the individual,[227] it certainly has a deep impact on social relations, as a "false positive match . . . automatically make[s] a suspect of somebody that is perfectly innocent."[228] Cautious legal approaches discouraging vast deployments of AFR are therefore fully justified.

The EU's legal position does not endorse massive deployments of mass surveillance systems in general. In accordance with the European Convention of Human Rights and its Court's jurisprudence,[229] the Court of Justice of the EU has rejected this prospective time and again,[230] criticizing the undiscriminated collection or retention of personal data even in cases of serious threats.[231] The preoccupation that vast technological developments give rise to forms of mass surveillance has also lately surfaced in the Artificial Intelligence Act, now under consideration of EU bodies.[232] The priority in protecting information about individuals is of such paramount importance that it has even put EU law and its Court in route of collision with the U.S. antiterrorism measures.[233]

The Court of Appeal's judgment seems to reflect the EU's approach within the context of AFR deployments. Although the UK is not part of the EU anymore, national regulations stemming from EU law have shaped so much of the Court of Appeal's ruling that domestic judges of other national jurisdictions within the EU are likely to look at *Bridges* as a rather authoritative precedent. Even the Court of

---

[224] Case C-291/12, Michael Schwarz v. Stadt Bochum, ECLI:EU:C:2013:670, ¶ 48, (Oct. 17, 2013), https://curia.europa.eu/juris/document/document.jsf;jsessionid=AB0F2E0B9A60A6193F5E6DBDC3E36905?text=&docid=143189&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7530581.

[225] *See* EU AGENCY FOR FUNDAMENTAL RTS., *supra* note 2, at 19.

[226] *See id.* at 5, 7.

[227] *See* Seng et al., *supra* note 18, at 4 (explaining that AFR can work "passively," or "does not need a conscious interaction with the system").

[228] Matt Burgess, *Facial Recognition Tech Used by UK Police Is Making a Ton of Mistakes*, WIRED (May 4, 2018, 7:00 AM), https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival [https://perma.cc/8JCE-FEDA] (quoting Martin Evison).

[229] *See* Big Brother Watch v. United Kingdom, Eur. Ct. H.R. 1, 91, 124–25 (2018).

[230] *See* Cases C-293/12 and C-594/12, Digital Rts. Ireland Ltd. v. Minister for Comm'n, Marine and Nat. Res., ECLI:EU:C:2014:238, ¶ 57 (Apr. 8, 2014); Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 ¶ 93 (Oct. 6, 2015); Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559, ¶ 183 (July 16, 2020).

[231] *See* Maximillian Schrems v. Data Protection Commissioner, Eur. Ct. H.R. 1, 15 ¶ 33 (2015).

[232] *Proposal for Harmonised Rules on AI*, *supra* note 13, at 21, 27.

[233] C-362/14, *Schrems*, ECLI:EU:C:2015:650, ¶¶ 86–88; C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559, ¶¶ 190–91 (July 16, 2020).

Justice of the EU, which has the monopoly of EU law interpretation,[234] is unlikely to ignore it. And, given that even in the United States the judicial rulings on this matter are a handful at best,[235] the impact of *Bridges*'s might be influential also across the Atlantic.

Regardless of the UK's departure from the EU, that country is likely to retain a moderate approach to the AFR and its immense capabilities. Within the UK, there is increasing political and social awareness that also in sensitive fields, like defense and security, AI exploit data that "is invariably uncertain, incomplete and contradictory . . . [s]ometimes it is also intentionally misleading,"[236] and that AI's outputs must therefore be handled with caution. This is encouraging new models of interaction between AI-based tools and human agents. The UK government's agenda sees the software "work[ing] in closer partnership with the humans involved," and protocols "ensur[ing that] the ensuing decisions and plans can be understood and justified."[237] This line of thinking clearly resonates with the preoccupations of the Court of Appeal and corroborates the scenario of AI supporting, and not replacing, humans in the context of AFR deployments.

There are therefore visible signs that a culture is building up in the EU as well as the UK that is conscious of the threats posed by AFR techniques, even when they are deployed to serve police purposes. Such culture is particularly needed as police corps in more than one EU countries have started testing AFR,[238] and the EU is presently funding "several research projects on the potential application of facial recognition technology in the area of security and border management."[239] Whilst "[r]oughly half of all American adults are already profiled in one or another American law enforcement agencies' facial-recognition database,"[240] if EU courts follow *Bridges*'s groundbreaking ruling, until EU enacts its draft bill on *Artificial Intelligence*, it is very unlikely that EU member states will build up comparable facial databases of their citizens and alien residents.

Bridges ruled out the hypothetical development of technologically advanced mass-surveillance systems by putting strong limitations on how watch-lists can be compiled and utilized.[241] But the perils of AI are not circumscribed to such a possibility.

---

[234] Nicola & Pollicino, *supra* note 9, at 63.

[235] *See* Huq, *supra* note 16, at 1904 (stating that "lawsuits challenging the use of facial recognition have not yet been lodged" in the United States).

[236] U.K. AI COUNCIL, AI ROADMAP 33 (2021), https://www.gov.uk/government/publications/ai-roadmap.

[237] *Id.*

[238] Most notably, police forces in Hamburg, Berlin, and Nice. *See* EU AGENCY FOR FUNDAMENTAL RTS., *supra* note 2, at 12.

[239] *Id.* at 17.

[240] *See* Huq, *supra* note 16, at 1900.

[241] *See* Keenan, *supra* note 1, at 10.

AI's mistakes are among the core concerns within the sphere of AFR deployments.[242] More specifically, some individuals might be more vulnerable to AFR technologies than others because of their ethnic background or their gender.[243] The Court of Appeal echoed such widespread concerns[244] and displayed a heightened knowledge of the problem, as it stigmatized the South Wales Police's superficial approach to the possibility that AFR Locate may develop biases. On the contrary, it stated that AFR Locate's algorithm needed both to be sufficiently transparent so that public institutions can review it and to include a diversified training dataset.[245]

Correcting biases is sometimes problematic. As some have pointed out, anti-discrimination laws may prevent from "assess[ing] and mitigat[ing] bias in algorithmic systems," because adjustments intended to fight prejudices can be perceived as incorporating biases themselves.[246] Thankfully, AFR technologies do not seem particularly problematic in this respect. Taking care of potential biases here does not seem to include adjusting the *treatment* of the AFR's matches to mitigate its potentially discriminatory impact. AFR tools may be improved simply by making the training more balanced.[247]

The Court of Appeal's prudent approach to AFR was grounded in the reality that "complex algorithms . . . may mask discriminatory practices."[248] The ruling, however, was still quite optimistic about AFR Locate's capabilities. The Court was not aware of the performance of AFR Locate during the UEFA Championship final in Cardiff. AFR's deployment then covered one whole week.[249] As the South Wales Police admitted in responding to an individual's inquiry about the treatment of

---

[242] EU AGENCY FOR FUNDAMENTAL RTS., *supra* note 2, at 4 ("[t]he risk of errors in matching faces is the most frequently raised fundamental rights concern.").

[243] Dave Gershgorn, *The Facial Recognition Backlash Is Here*, ONEZERO (Dec. 18, 2020), https://onezero.medium.com/the-facial-recognition-backlash-15b5707444f3 [https://perma.cc/4X6D-AYCP]; EU AGENCY FOR FUNDAMENTAL RTS., GETTING THE FUTURE RIGHT: ARTIFICIAL INTELLIGENCE AND FUNDAMENTAL RIGHTS 15 (2020) [hereinafter GETTING THE FUTURE RIGHT], https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights ("facial recognition systems detect gender well for white men, but not for black women").

[244] Daniel E. Ho & Alice Xiang, *Affirmative Algorithms: The Legal Grounds for Fairness as Awareness*, 2020 U. CHI. L. REV. ONLINE *134, *135 (2020), https://lawreviewblog.uchicago.edu/2020/10/30/aa-ho-xiang/ [https://perma.cc/PN5V-YK3J].

[245] *Bridges*'s approach thus mirrors the observation that "[e]ven if the algorithms used are properly designed, the inclusion of problematic data could heavily skew the algorithmic outcomes." Peter K. Yu, *The Algorithmic Divide and Equality in the Age of Artificial Intelligence*, 72 FLA. L. REV. 331, 373 (2020).

[246] Ho & Xiang, *supra* note 244, at 153.

[247] As to the differences between countering discrimination in training and at deployment of artificial intelligence, see *id.* at 141–42, 152.

[248] Yu, *supra* note 245, at 356–57.

[249] South Wales Police, *Freedom of Information Request 163/18,* 3 (Apr. 16, 2018) (on file with the author).

personal information, during that week the software returned 173 true positive alerts and 2,297 false positive alerts,[250] with a false positive ratio of 92%.[251]

Finally, the Court of Appeal gave a realistic consideration of the role of the human supervisors in charge of checking the match between the watch-list and the cameras before taking action. While the Court acknowledged the importance of such protocol to avoid misidentifications, it also gave weight to the impact that algorithms actually have on human decision makers.[252] In fact, there is evidence that human override of an AI outcome is likely to happen only "when the result from the algorithm is not in line with [the human's] stereotypes."[253] The combination of human biases with human overconfidence in AFR can therefore perpetuate and reinforce clichés and prejudices instead of preventing them.

The Court of Appeal's judgment focused also on the possibility that excessively discretionary police powers weaponize the AFR's potential to target specific persons.[254] Unfettered powers to deploy AFR tools can become insidious, facially neutral ways for the police to chase certain individuals. Only adequate protocols, which lay out how the watch-lists are made and where the technology is deployed, and which courts can review, are able to keep these dangers under check. Warning the public that AFR is operating in a certain area does not waive police forces from such obligations. As the Court of Appeal noted, despite the actions taken by the police to inform the public that an AFR system was operating, many could not be made aware of it.[255]

Bridges did not encourage general bans on AFR tools. Neither EU law nor the ECHR's privacy protection rules out the deployment of AFR, after all.[256] Such rights, in fact, "are not absolute rights, but must be considered in relation to their function in society."[257] As long as their limitations "are provided for by law, respect the essence of those rights, and, in accordance with the principle of proportionality, are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedom or others,"[258] they are permitted. This is also the approach of the draft bill of the Artificial Intelligence Act that the European Commission

---

[250] *Id.*

[251] Burgess, *supra* note 228. *See also* Chris Duckett, *Facial Recognition System Had 7 Percent Hit Rate at 2017 Championship*, ZDNET (May 7, 2018), https://www.zdnet.com/article/facial-recognition-system-had-7-percent-hit-rate-at-2017-champions-league-final/ [https://perma.cc/6SBK-YH4L].

[252] *See Bridges II*, EWCA (Civ) 1058 ¶ 185. The phrasing is borrowed by Madalina Busuioc. *See* Busuioc, *supra* note 15, at 8.

[253] GETTING THE FUTURE RIGHT, *supra* note 243, at 64.

[254] *See Bridges II*, EWCA (Civ) 1058 ¶¶ 91, 94.

[255] *Id.* ¶ 20.

[256] *See* GETTING THE FUTURE RIGHT, *supra* note 243, at 11; Guide to the Case-Law of the European Court of Human Rights: Data protection, Eur. Ct. H.R., ¶ 61 (Apr. 30, 2021).

[257] Case C-291/12, Michael Schwarz v. Stadt Bochum, ECLI:EU:C:2013:670, ¶ 33 (Oct. 17, 2013).

[258] *Id.* ¶¶ 33–34 (within the context of taking an individual's fingerprints).

has put forward: while it rules out the usage of AFR technologies for law enforcement in general, it does carve out some limited exception that may deserve its usage.[259]

Bridges did put some limitations on what police can do with AFR-based technologies. First, it preserved the EU's general rule that individuals should "*not* be subject to a decision based solely on automated decision-making."[260] Second, it required that AFR deployments follow precise protocols as to whom to include in the watch-lists and where to utilize such tools.[261] Third, it gave thorough consideration to the risks of discrimination, requiring police forces to do what is feasible to avoid biases and allowing the inspection of the code also at the expense of intellectual property's protection.[262]

Finally, by finding the police powers to deploy AFR too broad and discretionary, *Bridges* resonated with the calls for "[a]n adequate regulatory framework" as "an essential element to direct AI towards the good and welfare of individuals and society," and showcased the insufficiency of the existing regulatory instruments that are in place even within public bodies.[263] As novel technologies routinely require that policymakers develop new regulatory frameworks,[264] *Bridges* adamantly stated that new, adequate regulations are an imperative if such technologies are deployed by public bodies.[265]

The draft bill of the Artificial Intelligence Act now under consideration of EU bodies seems to heed *Bridges*'s calls more than the European lukewarm concern for the deployment of AFR.[266] Peoples within the EU do not seem to display "public movements" of a "scale and passion"[267] that can be compared to the popular wave against massive deployments of intrusive technologies that is mounting in the United States, effectively forcing legislative bodies to ensure that such tools comply with basic legal and ethical values.[268] As terrorist attacks and later the pandemic have greatly affected their social and individual lives, Europeans are more inclined to give credit to AFR. The Artificial Intelligence Act, however, does display a heightened sense of concern that AFR may disrupt the social cohesion and the enjoyment of fundamental rights such as the freedom to assembly. Time will tell what prevails in the EU between the fears of terrorism and the pandemic or of AFR technologies.

---

[259] *Proposal for Harmonised Rules on AI*, *supra* note 13, at 43–44.

[260] Busuioc, *supra* note 15, at 4.

[261] *Bridges II*, EWCA (Civ) 1058 ¶¶ 38, 152, 154.

[262] *See* Keenan, *supra* note 1, at 10.

[263] Francesca Lagioia & Giovanni Sartor, *Artificial Intelligence in the Big Data Era: Risks and Opportunities*, *in* LEGAL CHALLENGES OF BIG DATA 280, 305 (Joe Cannataci, Valeria Falce, & Oreste Pollicino eds., 2020).

[264] Araz Teihag et al., *Assessing the Regulatory Challenges of Emerging Disruptive Technologies*, REGUL. & GOVERNANCE 1, 1–2 (2021).

[265] *See Bridges II*, EWCA (Civ) 1058 ¶¶ 85–90, 94–96.

[266] *Proposal for Harmonised Rules on AI*, *supra* note 13, at 1, 3.

[267] Huq, *supra* note 16, at 1953.

[268] *See* Huq, *supra* note 16, at 1953.