Forensic Science International: Synergy 2 (2020) 86–89

Contents lists available at ScienceDirect

Forensic Science International: Synergy

journal homepage: https://www.journals.elsevier.com/forensic-science-international-synergy/

The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention

Kyriakos N. Kotsoglou*, Marion Oswald

School of Law, Northumbria University, Newcastle Upon Tyne, UK

ARTICLE INFO

Article history:
Received 22 November 2019
Received in revised form
6 January 2020
Accepted 7 January 2020
Available online 13 January 2020

Keywords:
Automated facial recognition
Algorithms
Policing
Decision-making
Reasonableness
Evidence
Individualisation

ABSTRACT

Criminal law's efficient and accurate administration depends to a considerable extent on the ability of decision-makers to identify unique individuals, circumstances and events as instances of abstract terms (such as events raising 'reasonable suspicion') laid out in the legal framework. Automated Facial Recognition has the potential to revolutionise the identification process, facilitate crime detection, and eliminate misidentification of suspects. This paper commences from the recent decision regarding the deployment of AFR by South Wales Police in order to discuss the lack of underpinning conceptual framework pertinent to a broader consideration of AFR in other contexts. We conclude that the judgment does not give the green light to other fact sensitive deployments of AFR. We consider two of these: a) use of AFR as a trigger for intervention short of arrest; b) use of AFR in an evidential context in criminal proceedings. AFR may on the face of it appear objective and sufficient, but this is belied by the probabilistic nature of the output, and the building of certain values into the tool, raising questions as to the justifiability of regarding the tool's output as an 'objective' ground for reasonable suspicion. The means by which the identification took place must be disclosed to the defence, if Article 6 right to a fair trial is to be upheld, together with information regarding disregarded 'matches' and error rates and uncertainties of the system itself. Furthermore, AFR raises the risk that scientific or algorithmic findings could usurp the role of the legitimate decision-maker, necessitating the development of a framework to protect the position of the human with decision-making prerogative.

1. Introduction

This paper commences from the recent decision regarding the deployment of AFR by South Wales Police in order to discuss the lack of underpinning conceptual framework pertinent to a broader consideration of AFR in other contexts (and is not therefore intended to be a case-note in the more traditional sense) (*II*). We will argue that the judgment does not give the green light to other fact sensitive deployments of AFR. We consider two of these: a) use of AFR as a trigger for intervention short of arrest (*III*); b) use of AFR in an evidential context in criminal proceedings (*IV*). AFR may, on the face of it, appear objective and sufficient, but this is belied by the probabilistic nature of the output, and the building of certain values into the tool, raising questions as to the justifiability of regarding the tool's output as an 'objective' ground for reasonable suspicion. We will thus highlight the decisional elements salient in the use of AFR and remind that algorithmic devices can only render data, not decisions (*V*).

Although modern computational power enables a far more comprehensive and time-efficient approach than before, the core idea underlying Automated Facia Recognition (AFR) goes back to Bertillon's (one of the fathers of forensic science) anthropometric methods as a means of identifying certain individuals or suspects. At its heart, forensics are about the (testimonial) claim of an expert that a forensic trace can be reduced in a scientifically reliable (replicable) way to a certain individual/object. For individualisation is widely regarded as the essence of forensic science [1]. Forensic experts (including decision support systems) are thus expected to authoritatively inform fact-finders and decision-makers on whether, say, the fingerprint at the crime scene *belongs* to that suspect or whether the person depicted on CCTV-footage *is* the wanted criminal – *to the exclusion of all others*. The problem hereby is not just the possible lack of sufficient empirical basis for a methodologically warranted claim (Source Attribution

* Corresponding author.
E-mail addresses: kyriakos.kotsoglou@northumbria.ac.uk (K.N. Kotsoglou), marion.oswald@northumbria.ac.uk (M. Oswald).

https://doi.org/10.1016/j.fsisyn.2020.01.002

Determination) - a number of blue-ribbon committees have openly questioned the scientific validity of forensic sciences - or that every method is prone to error; the problem is the practice of individualisation as such. The US-American case *Willie Allen Lynch v. State of Florida,* [2] where the AFR analyst reported that 'the analyst *makes a judgment* as to whether or not this *is* the individual and sends that information back to the detective that requested it' exemplifies this practice.

2. Automated Facial Recognition in a world first

(Criminal) law's efficient and accurate administration depends to a considerable extent on the ability of decision-makers to identify unique individuals, circumstances and events as instances of abstract terms (such as events raising 'reasonable suspicion') laid out in the legal framework. Artificial Intelligence (AI) systems aspiring to assist or even automate decision-making processes are – for obvious reasons – attractive for every legal order aiming for coherent management of the infinite number of cases emerging in an increasingly technological world. One of these powerful technologies, AFR, has the potential to revolutionise the identification process, facilitate crime detection, and eliminate misidentification of suspects.

Recently, the High Court of Justice (England and Wales) was called upon to determine whether the current legal regime in the UK was 'adequate to ensure the appropriate and non-arbitrary use of AFR in a free and civilized society' [3]. Its judgment was reportedly the first in the world to consider AFR, with the grounds of challenge contending breach of Article 8 (1) and (2) ECHR (primarily that use of AFR was not 'in accordance with law'); breach of data protection law, and failure to comply with the public sector equality duty (which we do not discuss).

AFR, as the court described, is technology aimed at assessing whether two facial images depict the same person. It does this by extracting biometric data from a digital image, and then comparing that data against biometric data from images in a database, say a 'watch-list'. If a sufficient amount of biometric data appears to be similar, then a 'match' is declared between the face on the footage and the face on the watch-list. A 'similarity score' is generated, with a higher number indicating a greater likelihood of a positive match. A human decision is required as to where to fix the threshold at which the software will indicate a match. Fixing this threshold too high or too low risks high false positive or false negative rates respectively. The case concerned the use of AFR by South Wales Police, in a pilot project called 'AFR Locate' which involved deployment of surveillance cameras to capture digital images of members of the public which were then compared with watch-lists compiled for the purposes of the pilot. If the algorithmic process renders a match between a face captured on video and an image on the watchlist, the court noted, then the system operator, i.e. a human being (police officer), has to intervene and make his or her assessment by reviewing the 'match'.

While the court agreed that use of AFR interfered with the claimant's article 8 rights, it determined that the police's common law powers were 'amply sufficient' for the use of AFR Locate. The court's view was that use of AFR Locate was not an intrusive act, in the sense of physical entry onto property, contact or force, and therefore fell within the common law duty to prevent and detect crime, and corresponding common law power to take steps to prevent and detect crime. The court dismissed the claim that the generic legal framework (consisting of the common law, data protection and human rights legislation, codes of practice issued under legislation and the police's own local policies) was insufficient: 'The fact that a technology is new does not mean that it is outside the scope of existing regulation, or that it is always necessary to create a bespoke legal framework for it.'

Regarding the substantive article 8 claims, the court held that use of AFR Locate by South Wales Police was not disproportionate by reference to *Bank Mellat* principles [4]: these were trials conducted for a limited time over a limited footprint; it sought individuals who were justifiably of interest to the police; nobody was wrongly arrested. The court drew attention to the purposes behind the deployment – public safety and detection of crime – and that 'CCTV alone could not have achieved these aims.' This view of proportionality, dismissing the claimant's argument that use of AFR should be limited to the prevention or detection of 'serious' crime, seems likely to have been influenced by the court's view of the intrusiveness of the technology as 'no more intrusive than the use of CCTV on the streets'. This view appears open to challenge, particularly bearing in mind that the court's own analysis of the interference with the claimant's Article 8 rights drew attention to the AFR-derived biometric data and (rather contradictorily) that AFR 'goes much further than the simple taking of a photograph.' Furthermore, the test as to whether the interference was necessary requires a 'pressing social need', an interference proportionate to the aim pursued, and relevant and sufficient justification [5]. As Fussey and Murray point out, 'a measure may be necessary in a democratic society in relation to certain purposes but not for others. In the context of LFR, a number of factors are therefore relevant when considering necessity. These include the nature of the deployments, the interconnectivity of different facial recognition systems, any analysis performed, and the formulation of watchlists.' [6] It is arguable that, although the court considered the high level purposes behind the deployment, it paid insufficient attention to the specific activities and policing purposes underlying particular uses, and to the consequences of these, essential to a consideration of whether an interference is proportionate to the aim pursued.

In respect of data protection, the court agreed with the claimant that processing of his image by AFR Locate individualised him from others, therefore constituting processing of his personal data and so the data protection principles applied. Based on the proportionality determination however, the processing was held to be lawful and fair. The court also agreed that AFR Locate involved sensitive processing of the biometric data of members of the public; again, based on the proportionality assessment, the 'strictly necessary' and 'substantial public interest' requirements were held to be satisfied.

To those who might regard this decision as giving the green light to more general use of AFR by the police, the court gave a note of caution: 'there is a limit what can sensibly be said in respect of possible future use of AFR Locate. Questions of proportionality are generally fact sensitive.' It is to this fact sensitive nature of particular deployments of AFR that we now turn. The South Wales police decision involved a trial of the technology, said by the police to be primarily for the purposes of the detecting and arrest of offenders, and so it did not pay particular attention to specific decision-making contexts in which AFR could be deployed and the need for robust frameworks to underpin such contexts. We consider two of these: a) use of AFR as a trigger for intervention short of arrest; b) use of AFR in an evidential context in criminal proceedings.

3. Use of AFR as a trigger for intervention short of arrest

Modern legal orders – including the Fourth Amendment in the USA and the Police and Criminal Evidence Act 1984 (PACE) and its accompanying Codes of Practice in England and Wales – are to a large extent reliant upon context-sensitive notions such as *reasonableness*. Police must demonstrate 'reasonable grounds for believing' and 'reasonable grounds for suspecting' on a number of occasions, and, in making this judgement, the officer will be

exercising professional discretion. It is a basic principle in the law of England and Wales that ordinary words such as 'reasonable' or 'sure', in the many contexts in which they appear, are to be left undefined, so as to enable decision-makers to draw upon their own experience of ordinary life [7].

It is increasingly likely that we will soon see in England and Wales police interventions, such as stop-and-search or arrest, based (partially, or contra legem: exclusively) upon live or after-the-event AFR matching. As regards stop-and-search powers under section 1 of PACE, PACE Code A emphasises the requirement for an *objective* basis for that suspicion based on facts, information and/or intelligence, and that personal factors can never support reasonable suspicion, unless information or intelligence provides a personal description [8]. In relation to arrest, section 24 of PACE also requires 'reasonable' grounds for the suspicion that the individual is about to commit, or has committed, an offence (although the South Wales Police pilot appeared to be operating in this context, this aspect was not discussed in the judgment).

AFR may on the face of it appear objective or even sufficient for further action, but this is belied by the probabilistic (i.e. general) nature of the output; the fact that manufacturers of AFR technology can set the default-threshold value for False Alarm Rates at will; or the fact that the end user is by design allowed to 'change the threshold value to whatever they choose'. These rates represent the building in of certain values into the tool, for example the avoidance of false negatives, resulting therefore in an increase in false positives. Would the officer be justified in regarding the tool's output as 'objective' in such circumstances?

The human in the loop — 'the fact that human eye is used to ensure that an intervention is justified' — was regarded by the court in the South Wales police case as an important safeguard. The potential for unnuanced statistical or computer-generated scores to be highly influential on human decision-makers is well-known [9], thus raising the risk that discretion could be fettered unlawfully [10]. How valid is that safeguard in circumstances when an officer on the ground is presented with a finding from AFR and requested to act on it, especially where decisions around the values built into the tool (and therefore the uncertainties) are made elsewhere? [11].

4. Use of AFR in an evidential context in criminal proceedings

Evidence is the admissible information with which disputed facts in a legal setting including the criminal process are proven. However, evidence, especially scientific/algorithmic evidence, does not equate to (adequate) proof in its own right and legal issues including questions about ordinary words cannot be answered by making recourse *solely* to inference and empirical observations. The prosecution must use all the evidence in combination to prove the case to the required standard of proof (being 'sure' in England and Wales) [12]. Outputs from AFR, as in the US case of *Lynch* referred to above, could lead to the arrest and prosecution of a particular individual to the exclusion of others who may have been flagged or matched by the system with less certainty. What is more, there is no guarantee that the abovementioned industrial settings (values) shall reflect the institutional architecture of the criminal process including the overriding objectives of the latter, i.e. acquitting the innocent, convicting the guilty, especially the acceptable rate of errors/trade-off between these objectives. The renowned Blackstone-ratio and the dictum in *In* Re *Winship*, stressing the 'fundamental value […] of our society that it is far worse to convict an innocent man than to let a guilty man go free' [13], illustrate this point. In other words, in order to answer any practical question (arrest/not-arrest, conviction/acquittal etc), we need more than the available data we have (e.g. AFR output). The choice of any course of action will reflect value judgments made by human beings [14].

In the procedural context, we would argue that the means by which the identification took place must be disclosed to the defence, if Article 6 right to a fair trial is to be upheld, together with information regarding disregarded 'matches' and error rates and uncertainties of the system itself. Only then would the defence have the ability to effectively cross-examine the system via the expert witness, in the same way as they would cross-examine an eyewitness. The Strasbourg Court (Grand Chamber) regarded the ability to *understand* the verdict as 'a vital safeguard against arbitrariness' [15]. True, the Grand Chamber made clear that decision-makers have no *duty* to give reasons for decisions in order to comply with Art 6 of the Convention [16]. But to reiterate this, misses its target. *Giving* reasons for decisions is one thing. *Having* reasons for a decision is quite another.

5. Decision-making authority

Criminal courts have drawn attention many times in the past to the risk that scientific or algorithmic findings could usurp the role of the decision-maker in the legal proceedings. As Justice Scalia (SCOTUS) put it pithily: Statistical evidence 'is worlds away from 'significant proof'' [17]. Given that individualisation, i.e. the decision that 'the biometric data belong to *this person* to the exclusion of all others' requires more than the data we can obtain from an AFR system, the question now is, *who* will make that decision. Legal orders have their own established routines for resolving factual disputes, a normatively structured decision-making process under uncertainty. A legal order does not only determine what types of behaviour are worthy of censuring and punishment; for it is more than a *static* set of substantive rules. A legal order regulates itself by conferring legal authority to certain individuals to make decisions, for instance to stop and search or to ascribe criminal liability.

In the province of law, only decisions issued by the *competent* authority are valid. Any other opinion as to the existence of an ultimate issue (such as the identity of the depicted person) is inadmissible; expert witnesses let alone algorithms are not authorised to make decisions. Given that simple real-life situations including face recognition (or cognition in general) are analytically intractable, we need a 'human eye' to decide whether an algorithmically generated match can be declared valid.

The court in the South Wales Police case stated that it was neither 'necessary not practical' for legislation to define precisely the circumstances in which AFR may be used. We would argue however for an urgent discussion into what (kind of) decisional framework or safeguards should be put in place for use of AFR as evidence or trigger for police intervention. Treating *decisions* about unique historical events as if they are indistinguishable from *scientific/algorithmic findings* does not bring real-life let alone legal problems to heel. It simply adds to the uncertainty. By focusing exclusively on epistemic considerations, we neglect structural features of any legal order which lay out *who* decides *what* under *which* circumstances by following a certain procedure.

Technological developments including AFR show no signs of abating and it is therefore of paramount importance to realise that practical contexts in general and policing or the criminal process in particular are normatively structured decision-making processes under *uncertainty* [18]. The complexity of the world —and the simple fact that the very effort to catalogue the combinatorial possibilities of all pertinent elements would strain even a supercomputer— [19] means that decision-making is computationally intractable. Each decision including facial recognition is premised on a 'leap of faith' rather than valid empirical data [20]. Discussion of the type and level of risks involved, i.e. the acceptable trade-off between different types of erroneous outcomes will also mean that the abovementioned 'leap' does not descend to an anything-

goes activity, and should be translated into clear codes of practice for specific decision-making contexts, subject to stringent oversight and regulation. We cannot allow police officers, the judge or the jury to be reduced to the long arm of the algorithm. The former have the decision-making prerogative whilst making judgments under uncertainty [21]. Their decisions may not ultimately be final; but only *they* can make these decisions.

Declaration of competing interest

We have no conflict of interest to declare.

Acknowledgments

The authors would like to thank the anonymous reviewer for useful comments and suggestions.

References

[1] P.L. Kirk, The ontogeny of criminalistics, J. Crim. Law Criminal. Police Sci 54 (1963) 235–238, https://doi.org/10.2307/1141173.
[2] Available online, https://cases.justia.com/florida/first-district-court-of-appeal/2018-16-3290.pdf?ts=1545938765 – Emphasis added. last accessed: 18 Nov 2019.
[3] R (Bridges) v Chief Constable of the South Wales Police [2019] EWHC 2341 (Admin).
[4] Bank Mellat v HM Treasury [2013] UKSC 39.
[5] Catt v UK, ECtHR, App. No. 43514/14, 24 Jan 2019, para 109.
[6] P. Fussey, D. Murray, Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, July 2019, p. 44.
[7] R v Golds [2016] UKSC 61, at [37].
[8] PACE 1984, Code of Practice A, para 2.2.
[9] D.J. Cooke, C. Michie, Violence risk assessment: from prediction to understanding–or from what? To why? in: C. Logan, L. Johnstone (Eds.), Managing Clinical Risk Routledge, London, 2013, pp. 22–44.
[10] M. Oswald, Algorithmic-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power, The growing ubiquity of algorithms in society: implications, impacts and innovations' issue of, Phil. Trans. R. Soc. A 376 (2018) 2128.
[11] On the necessity of a 'human in the loop' see D. A. Stoney, What made us ever think we could individualize using statistics? In: 31 J. Forensic Sci. Soc.. (1991), pp. 197–199; M.J.Saks and J.J. Koehler, The Coming Paradigm Shift in Forensic Identification, in: 309 Science (2005), pp. 892 – 895; J.J. Koehler, Error and Exaggeration in the Presentation of DNA Evidence at Trial, in: 34 Jurimetrics (1993-1994), pp. 21–39; M.J. Saks and J.J. Koehler, The Individualization Fallacy in Forensic Science Evidence, in: 61 Vanderbilt Law Review (2008), pp. 199–219.
[12] See The Crown Court Compendium (England and Wales), Part 1, para 5.1.
[13] In re Winship, 397 U.S. 358 (1970) (Harlan J., concurring) at 372.
[14] See also E. Sober, Evidence and Evolution. The Logic behind the Science, University Press, Cambridge, 2012, p. 7.
[15] Taxquet v. Belgium (GC), App. No. 926/05, (Eur. Ct. H.R., Nov. 16, 2010), para 90. Robert C. Power, Reasonable and Other Doubts: The Problem of Jury Instructions, 67 Tennessee Law Review (1999), pp. 45–123 (115) makes a similar pressure point: "There is a severe flaw in the black box approach, at least in criminal cases. If defendants only were entitled to a jury trial, then perhaps this would be acceptable [...] However, criminal defendants also have rights to the reasonable doubt standard".
[16] Taxquet (GC), para 90: "[t]he Convention does not require jurors to give reasons for their decision".
[17] Wal-Mart Stores, Inc. v. Dukes et al., 564 U.S. 338 (2011), Opinion (Scalia), p. 14.
[18] Paul Roberts, Renegotiating forensic cultures: between law, science and criminal justice, Stud. Hist. Philos. Sci. C Stud. Hist. Philos. Biol. Biomed. Sci. 44 (2013) 47–59, 53.
[19] Christopher Cherniak, Computational complexity and the universal acceptance of logic, J. Philos. 81 (1984) 739–758, https://doi.org/10.1007/s10506-019-09248-x (753); K.N. Kotsoglou, Proof Beyond a Context-Relevant Doubt. A Structural Analysis of the Standard of Proof in Criminal Adjudication. In: Di Bello, M., Verheij, B. (eds.) Evidence & decision making in the law: theoretical, computational and empirical approaches. Artif Intell Law (2019).
[20] Stoney, supra note 11, p. 198 Simon A. Cole, Individualization is dead, long live individualization! Reforms of reporting practices for fingerprint analysis in the United States, Law Probab. Risk 13 (2014) 117–150. M.J.Saks and J.J. Koehler, The Coming Paradigm Shift in Forensic Identification, in: 309 Science (2005), pp. 892–895.
[21] For a discussion of this term in relation to scientific evidence, see e.g A. Biedermann, K.N. Kotsoglou, Decisional dimensions in expert witness testimony – a structural analysis, Front. Psychol. 9 (2018), https://doi.org/10.3389/fpsyg.2018.02073. Article 2073.