Automated Facial Recognition in Law Enforcement: The Queen (*On Application of Edward Bridges) v The Chief Constable of South Wales Police*

BJ Gordon*

Online ISSN
1727-3781

P·E·R

**Pioneer in peer-reviewed,
open access online law publications**

Author

Barrie Gordon

Affiliation

University of South Africa

Email

bgordon@unisa.ac.za

Date Submission

22 September 2020

Date Revised

20 April 2021

Date Accepted

20 April 2021

Date published

30 June 2021

Editor Dr N Kilian

How to cite this article

Gordon BJ "Automated Facial Recognition in Law Enforcement: The Queen *(On Application of Edward Bridges) v The Chief Constable of South Wales Police*" *PER / PELJ* 2021(24) - DOI http://dx.doi.org/10.17159/1727-3781/2021/v24i0a8923

DOI
http://dx.doi.org/10.17159/1727-3781/2021/v24i0a8923

Abstract

The use of automated facial recognition in law enforcement is still a novel practice and as a result the legislative framework for this technology is ill-defined. The judgement of *The Queen (on application of Edward Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058 is the first case in the world that examines pertinent legal questions pertaining to this new technology. Automatic facial recognition may be used in law enforcement, but to prevent massive human rights violations, operators should perform their duties within a well-defined legal framework where discretion is kept to the minimum, and strict data-retention policies are followed. Furthermore, human oversight should always be part of an automated facial recognition system to ensure accuracy, fairness, and compliance with the law.

Keywords

Automated facial recognition; facial biometrics; *Bridges*; human rights violations; law enforcement; biometric data; *Protection of Personal Information Act*; POPI; privacy; data retention

……………………………………………………….

1 Introduction

Automated Facial Recognition as a new technology has the potential to change law enforcement worldwide. It has the ability to process facial biometrics in large crowds, and by doing so it becomes possible to identify individuals within those crowds. In a similar vein automated facial recognition has the potential to infringe on people's human rights *en masse,* and if this technology is not used within the strict boundaries of the law, it becomes outright dangerous.

An automated facial recognition system is: "[a] computer application capable of identifying or verifying a person from a digital image or a video frame from a video source."[1]

The most common way to use this new technology in law enforcement is to process facial biometric data from known offenders, i.e., to extract facial biometrics of people known to law enforcement from existing photos or video feeds. This information is then collated in a database which forms the basis of facial comparison. A second live video feed from the public is fed to the automated facial recognition software, which creates similar facial biometrics and compares them to the first database.[2] If a match is found, the software alerts the user to this fact, and the law enforcement officer may take the necessary steps to apprehend the identified person.[3]

As with any new technology, automatic facial recognition creates issues that the law will have to address. In the recent case of *The Queen (on application of Edward Bridges) v The Chief Constable of South Wales Police*[4] *(R-Bridges)* the United Kingdom Court of Appeal had to rule on a number of these issues. As this is the first case in the world dealing with automatic facial recognition,[5] the purpose of this contribution is to illustrate and collate the pertinent issues regarding automated facial recognition as found in this

[*] Barrie J Gordon. BA LLB LLM (RAU) LLD (Unisa). Senior Lecturer, Department of Criminal and Procedural Law, Unisa, South Africa. Email: bgordon@unisa.ac.za. ORCID ID https://orcid.org/0000-0003-0581-2377.

[1] De Sousa *Neuromarketing* 143. The author further gives the example that: "One of the ways to do this is by comparing selected facial features from the image and a facial database." This example is exactly what this study is about to discuss.

[2] Kamila *Handbook of Research on Emerging Perspectives* 218.

[3] Li *Handbook of Face Recognition* 624.

[4] *The Queen (on application of Edward Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058 (*R-Bridges*).

[5] At first glance this might appear to be a rather bold and sweeping statement, but the judgement itself mentions this fact. See *Edward Bridges v The Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) para 1.

case. Since all of these principles are centred in the law of the United Kingdom, this case note seeks to identify comparable principles in South African law and apply the lessons learned in the Bridges case to these principles and legislation.

In order to understand the matter thoroughly, the original divisional court case of *Edward Bridges v The Chief Constable of South Wales Police*[6] *(Bridges)* will be looked at first, and then the appeal in *R-Bridges* will be discussed.

2 *Edward Bridges v the Chief Constable of South Wales Police*

2.1 Background

During the course of 2017 the South Wales Police rolled out a pilot project to experiment with automated facial recognition in law enforcement.[7] The central issue before the court was to determine if the legislative framework was adequate when using automated facial recognition in the United Kingdom. The investigation looked at whether the use of automated facial recognition complied with privacy and data retention policies and legislation and the parameters within which it should be used, and to eliminate to the largest extent possible any arbitrary use of the technology.[8]

The court started by noting that law enforcement is not precluded from using new technologies such as automated facial recognition.[9] In *R(S) v Chief Constable of the South Yorkshire Police*[10] it was noted that:

> It is of paramount importance that the law enforcement agencies should take full advantage of the available techniques of modern technology and forensic science.[11]

New technologies, like DNA,[12] fingerprints[13] and now the use of automated facial recognition are invaluable to law enforcement, as they provide accurate tools to positively identify perpetrators of crime. Using new technologies in law enforcement is quite normal, as long as the law

[6] *Edward Bridges v The Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) (*Bridges*).
[7] *Bridges* para 8.
[8] *Bridges* para 1.
[9] *Bridges* para 5.
[10] *R (S) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196.
[11] *Bridges* paras 1-2.
[12] Makin *DNA and Property Crime Scene Investigation* 203.
[13] Hawthorne *Fingerprints* 16.

enforcement official stays within the parameters of the law when deploying the new technology.[14]

The use of automated facial recognition creates concerns about privacy and civil liberties, as the faces and features of large groups of people are digitally assessed and stored.[15]

The South Wales police started using an automated facial recognition technology known as "AFR Locate", which involved the deployment of surveillance cameras in public places, and then captured and processed those video feeds. The results were then compared to a watch list of known suspects and other people whom the South Wales Police wanted to locate, such as persons in need of protection, or possible witnesses in court cases.[16]

It is interesting to note that automated facial recognition does not merely monitor behaviour, but has the potential to also alter it. When a suspect is aware that he is being monitored, for example while attending a peaceful protest, his behaviour may be different from what it would have been if he was not being monitored.[17]

The use of automated facial recognition should therefore be contained within a very specific and defined framework.[18]

The framework for the use of automated facial recognition in the United Kingdom is the *Data Protection Act* 12 of 2018. In addition to this, the Surveillance Camera Commissioner has responsibilities under section 34 of the *Protection of Freedoms Act* 9 of 2012 which involve compliance with the Code of Compliance for surveillance cameras. As will be seen below, a number of laws of general application, like the *European Convention on Human Rights* and the *Equality Act* 15 of 2010, is also applicable.

2.2 Facts

The claimant is a civil liberties campaigner named Edward Bridges. He contested the use of automated facial recognition by the South Wales Police

[14] *Bridges* para 2.

[15] *Bridges* para 7.

[16] *Bridges* para 7.

[17] Davies, Dawson and Innes 2020 https://theconversation.com/how-facial-recognition-technology-aids-police-107730.

[18] *Bridges* paras 2 and 7.

department.[19] The defendant is the Chief Constable of the South Wales Police.[20]

Mr Bridges claimed that his facial features were processed by the South Wales Police on two occasions. The first occurrence was on the 21st of December 2017 at Queen Street, which is a very busy shopping area in Cardiff, in the United Kingdom. The second occurrence was at a motor show on 27 March 2018.[21]

The automated facial recognition deployment on 21 December 2017 was performed from a marked police vehicle, although the claimant mentioned that he did not observe any markings on the van.[22] Police deployed the automated facial recognition on that day with the specific purpose of locating and detaining "Priority and Prolific Offenders". The strategy was to compile three watch lists: a "red" watch list with one person suspected of committing a serious crime; an "amber" watch list, comprising of 382 people with outstanding warrants; and a "purple" watch list comprising 536 suspects of committing various crimes within the jurisdiction of the South Wales Police department. During the day in question the automated facial recognition identified ten possible matches, of which two matches were incorrect. Of the remaining eight correct automated facial recognition matches, two arrests were made.[23]

The second use of automated facial recognition where the claimant was involved occurred at a motor show on 27 March 2018, also in Cardiff in Wales. During the previous year the show had been disrupted by a bomb scare, and police wanted to use automated facial recognition to identify known offenders of this type of crime.[24] Police again created three watch lists, just as before. Based on these lists, one positive identification was made, with no false positives.[25]

Mr Bridges was participating in a peaceful protest at the motor show. At this time Mr Bridges noticed the marked police vehicle, and it was only then that Mr Bridges became aware that automated facial recognition was being

[19] *Bridges* para 8.

[20] *Bridges* para 8.

[21] *Bridges* para 10.

[22] *Bridges* para 12. The claimant also acknowledged that he was within reach of the camera’s field of view, and therefore his facial particulars must have been processed on both occasions.

[23] *Bridges* para 11.

[24] *Bridges* para 13. The automated facial recognition system in use did, in fact, correctly identify one known suspect for making bomb-scares on the day.

[25] *Bridges* para 14.

used. He also stated that he was within a few metres of the police vehicle, and it is very probable that his facial features were scanned by the automated facial recognition system. Mr Bridges further stated that no police official was on the scene to explain or provide information on the use of automated facial recognition.[26]

At the trial it was not possible to confirm whether or not Mr Bridges was in fact a target of the automated facial recognition system.[27] The reason for this is that it is an automated process, and after the facial recognition had been performed, the system would immediately have deleted any biometric information which did not correspond to a known suspect on the watch list. The South Wales Police confirmed that Mr Bridges had not been on any of the watch lists on the two occasions in question, and if the automated facial recognition system had processed his facial features, all data pertaining to that would have been deleted immediately. As a result, it was impossible for the South Wales Police department to confirm if Mr Bridges' facial information was processed by the system, but as it is able to process multiple images per second, it is highly likely that Mr Bridges' facial features had been processed. The South Wales Police acknowledged that Mr Bridges' features would have been processed and that he was able to bring this matter to court.[28]

The claimant made the following claims:

(a) The use of automated facial recognition interfered with his rights under Article 8(1) of the *European Convention on Human Rights*. Furthermore, the use of automated facial recognition interfered with Article 8(2) of the *European Convention on Human Rights* in that it was neither "in accordance with the law" nor "necessary" or "proportionate".[29]

(b) The use of automated facial recognition was in breach of Articles 10 and 11 of the *European Convention on Human Rights* (Freedom of Expression and Freedom of Assembly). This ground was subsequently withdrawn, and the court did not make any judgement on it.[30]

[26] *Bridges* para 15.
[27] *Bridges* para 16.
[28] *Bridges* para 16.
[29] *Bridges* para 18.
[30] *Bridges* para 19 fn 3.

(c) The use of automated facial recognition was in contravention of section 35 of the current *Data Protection Act* 12 of 2018.[31] The claimant brought claims under the old *Data Protection Act* 29 of 1998 as well, since the old Act would have been applicable to the first incident on 21 December 2017, but the new *Data Protection Act* 12 of 2018 would have been applicable to the second incident, which occurred on 27 March 2018.[32] In addition, a claim was brought that the South Wales Police had infringed section 64(1) of the current *Data Protection Act* 12 of 1964 as it did not complete a data protection impact assessment prior to implementing the automated facial recognition system.[33]

(d) The use of the automated facial recognition system was in contravention of section 149(1) of the *Equality Act* 15 of 2010 in that the South Wales Police failed to take into consideration that it might be prejudicial towards minority ethnic groups.[34]

2.3 Automated Facial Recognition Technology

The court started off by stating that in order to determine whether or not this technology falls within the ambit of the enabling legislation, it was necessary to understand, in broad terms, how automated facial recognition technology worked, and how it was implemented.[35]

In its simplest form it is a technology that compares two facial images and determines whether they are images of the same person.[36] In the case of law enforcement, a photograph of a known suspect will be used to extract facial biometric data. This simply means that a mathematical map will be made by comparing facial features, such as the width of the eyes, the distance they are apart, the length and width of the nose and mouth, and their proportions to one another.[37] Other features like ears and cheekbones may also be used if they are available. By using all these pieces of

[31] *Bridges* para 18.

[32] The provisions under the new Act will be examined in this study, as they illustrate the issues at hand sufficiently.

[33] *Bridges* para 18.

[34] *Bridges* para 18.

[35] *Bridges* paras 7 and 23-25.

[36] *Bridges* para 23.

[37] Lee-Morrison *Portraits of Automated Facial Recognition* 72.

information in combination with one another, a simple mathematical triangulated map of the face is constructed.[38]

The facial map is stored in a database, and when the system is deployed in public, the software will process faces from a video feed and compare them to the facial maps stored in the database.

The process can be structured as follows:[39]

(a) Processing known images: Existing facial images are processed to construct a mathematical, triangulated map of the face. This is simply expressed as a group of numerical values. The processed information is stored in a database, which will form the basis of comparison to new data.

(b) Facial images obtained from video feed: An ordinary CCTV camera feed is used to acquire real-time facial information. This can be done either in a formal setting, where a subject has to pose for the photo to be taken, or informally, where facial information is extracted from people passing by the camera. The current matter involves the latter.

(c) Face Detection: An image or video feed may contain a number of faces in a single shot. Individual facial information is isolated in this process. This would be similar to taking a picture of a single, unique face.

(d) Feature extraction: This process involves mathematical processing of the face by identifying facial features such as the eyes, nose, mouth, and ears, and calculating the size of each and the distance between them. This process creates the biometric feature that will be used to compare with the biometric data on file (database).

(e) Face comparison: The biometric feature created from the live video feed is compared with the one on file.

(f) Matching: The automated facial recognition software creates a "similarity score" between two matching faces. The higher the score, the more probable it is that the person from the live video feed is indeed the suspect. The software also provides the user with an option

[38] De Marsico *Face Recognition* 23 explains how this triangulated map is constructed: "The faces are parameterized as triangulated meshes. In this context, registered means that every face is in the same parameterization, i.e., shares the same triangulation, and that — semantically all corresponding points, such as the corners of the eye, are at the same having the same number of vertices".

[39] *Bridges* para 24.

> to adjust the similarity score: the lower the adjustment, the more false positives will be generated; conversely, if the similarity score is adjusted higher, false positives will be minimised, but true matches might also be mismatched, making the system less useful.

As automated facial recognition is a new technology, the South Wales Police was careful to use it under very specific conditions. For example, a specific purpose was identified with each deployment, and watch lists for that specific deployment were created.[40] In the deployment of 27 March at the motor show, the purpose was to identify suspects known to commit bomb scares, and the watch list was developed with the purpose of identifying such persons. In this particular case the system performed according to its design, as it did, in fact, identify a known bomb scare suspect on that day, and the organiser of the motor show was informed immediately.[41]

Watch lists used by the South Wales Police comprised between 400-800 suspects at a deployment, and the software's maximum is 2000 images.[42]

The automated facial recognition software has a very important safety feature to prevent false positives. When a positive match is made, the software will immediately open a screen to display the two matched photos side-by-side. This is done to enable the police official using the software to make a positive identification and to instruct other police officials nearby to act, if necessary. The court made special mention that this is a justified and important safeguard of the public's rights.[43]

The South Wales Police confirmed that the automated facial recognition system dealt with very large numbers of scans. The software has the capacity to scan 50 facial images per second. Automated facial recognition software was deployed on 50 occasions between 2017 and 2018, and the South Wales Police estimated that around 500 000 faces may have been scanned during this period.[44] However, in the vast majority of cases the system did not make any positive identification, and the captured facial data were immediately deleted. Only when a positive match was made would the system alert the operator to compare the matched image with the live video

[40] *Bridges* para 29.
[41] *Bridges* para 101.
[42] *Bridges* para 31.
[43] *Bridges* para 33.
[44] *Bridges* para 36.

feed. It was then up to the police official to decide to take the necessary action.[45]

2.4 Data retention

In every case where a captured image resulted in a negative match, the image was deleted immediately and automatically. Police officials did not have access to any of these images and the identity of the person was not obtained. The "raw" CCTV video feed was retained for 31 days and positive matches were kept for a period not exceeding 24 hours. These retention periods were mandated by the South Wales Police Standard Operating Procedures and Data Protection Impact Assessments.[46]

2.5 Finding

The divisional High Court meticulously dealt with each claim in turn.

2.5.1 Claim 1: The Convention on Rights Claim

Article 8(1) of the *European Convention on Human Rights* provides that:

> Everyone has the right to respect for his private and family life, his home and his correspondence.

This provision stretches further than the privacy of an individual's home, as illustrated by *S and Marper v United Kingdom,*[47] which specifically mentions that a state may not use modern scientific techniques at any cost, but that it should rather be balanced to conform to the principles contained in Article 8 of the *European Convention on Human Rights*.[48]

[45] *Bridges* para 36.

[46] The court states: "AFR Locate does not retain the facial biometrics or image of persons whose faces are scanned. They are immediately and automatically deleted. That data is not available to the system operator or any other police officer. The CCTV feed is retained for 31 days in accordance with the standard CCTV retention period. Data associated with a match is retained within AFR Locate for up to 24 hours. In the event of no match, the data is immediately deleted." *Bridges* para 37.

[47] *S and Marper v United Kingdom* [2009] 48 EHRR 50.

[48] The court observes on 112 that: "[t]he protection afforded by Art. 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. … The Court considers that any state claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard."

The divisional court accepted the reasoning in the above mentioned case, and confirmed that the reach of Article 8(1) is quite broad.[49] However, in *R (Wood) v Commissioner of Police of the Metropolis*,[50] the court submitted that the "bare act of taking pictures"[51] cannot be regarded as a contravention of Article 8(1). If law enforcement performs "expected and unsurprising" actions, then its conduct is lawful and Article 8(1) is not infringed upon.[52]

The next question was whether automated facial recognition should be regarded as a bare act of taking pictures. No, said the court unequivocally, as "AFR Locate goes much further than taking a photograph."[53] In this context the case of *PG and JH v United Kingdom*[54] is more appropriate, where the *European Court of Human Rights* states that:

> There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectation as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, *once any systematic or permanent record comes into existence of such material from the public domain* ...[55]

The court then concluded that the use of biometric data was well beyond the "expected and unsurprising".[56]

Thus, if personal data are stored, this points to a potential infringement of Article 8(1). The court mentioned that this is true, even if data are stored for a brief moment, as in the case with the automated facial recognition technology. The court then stated unequivocally:

> We are fortified in our conclusion that the use of automated facial recognition technology engages Article 8 ... .[57]

[49] *Bridges* paras 47-49.

[50] *R (Wood) v Commissioner of Police of the Metropolis* [2010] 1 WLR 123.

[51] *Bridges* paras 36-37.

[52] *Bridges* para 44.

[53] *Bridges* para 54.

[54] *PG and JH v United Kingdom* [2001] ECHR 546 (25 September 2001).

[55] *Bridges* para 57. My emphasis added.

[56] *Bridges* para 55.

[57] *Bridges* para 59 where the court states "The mere storing of biometric data is enough to trigger Article 8".

The court came to the conclusion that the use of AFR Locate infringed upon Article 8(1) of the *European Convention on Human Rights*.[58]

The court now moved to the claim that the use by South Wales Police of automated facial recognition was "not in accordance with the law". This claim was based on Article 8(2) of the *European Convention on Human Rights,* which states that no infringement of Article 8(1) may be permitted unless it is "in accordance with the law". The claimant argued that the South Wales Police could not legally deploy AFR Locate, since the legal framework enabling it was insufficient. In essence the claimant viewed the South Wales Police's use of automated facial recognition as *ultra vires.*[59]

The court was of the opinion that the only way that the South Wales Police could have acted *ultra vires* was if the automated facial recognition technology was an "intrusive method" of obtaining evidence.[60] The court looked at other intrusive methods of obtaining evidence, like fingerprints and searching a person's private property, and came to the conclusion that facial biometrics was nothing like this, as it is not intrusive at all. Automated facial recognition is no more intrusive than an ordinary CCTV camera, and taking a photograph of the face is all that is needed, which is not intrusive at all.[61] Consequently the court held that the South Wales Police did not act *ultra vires.*[62]

The court then turned to the second leg of this claim, namely whether a sufficient legal framework existed for automated facial recognition to be used.[63] The court mentioned that if new technology is used in law enforcement, this does not mean that it is automatically outside the scope of the law.[64] In this particular case the technology conformed to existing legislation, namely the *Data Protection Act* 29 of 1998 as well as the *Data Protection Act* 12 of 2018.[65] It also fell within the ambit of the Code of Practice on the Management of Police Information,[66] on the processing of personal data. Another piece of applicable legislation is the Surveillance Camera Code, which is issued in terms of the *Protection of Freedoms Act* 9 of 2012. This deals specifically with the use of surveillance cameras and

[58] *Bridges* para 62.
[59] *Bridges* para 68.
[60] *Bridges* para 74.
[61] *Bridges* para 75.
[62] *Bridges* para 78.
[63] *Bridges* para 79.
[64] *Bridges* para 84.
[65] *Bridges* para 85; S 34(3) of the *Data Protection Act* of 2018.
[66] Which is regulated by the s 39A(7) of the *Police Act* of 1996; *Bridges* para 88.

contains twelve guiding principles when CCTV cameras are used.[67] All these principles apply in equal measure to automated facial recognition.

In addition to the legislative framework, the South Wales Police have their own set of policies that regulate their conduct. The court identified at least three such policies governing the use of automated facial recognition, namely the South Wales Police Department's own Standard Operating Procedures, the SWP Deployment Reports and the SWP Policy on Sensitive Processing.[68] Bearing all of this in mind, the court came to the conclusion that a satisfactory legal framework existed for automated facial recognition to be deployed.[69] As a result, the claim on this ground was rejected.

2.5.2 Claim 2: The Data Protection Claims

The claimant brought data protection claims under the old *Data Protection Act* 29 of 1998 as well as the *Data Protection Act* 12 of 2018. The reason for this was that the *Data Protection Act* 29 of 1998 had been in force at the time the first incident took place, while the *Data Protection Act* 12 of 2018 was in effect when the second incident took place. For our purposes we will focus on the latter Act only, as the principles involved are materially similar.

The claimant asserted that the South Wales Police's use of automated facial recognition resulted in "sensitive processing" of the public at large. Section 35(8) of the *Data Protection Act* 12 of 2018 stipulates that sensitive processing occurs when racial or ethnic features are captured, if political opinions or religious beliefs are processed, or if trade union membership is revealed. Sensitive processing triggers stricter conduct from police and may be performed in two cases only, namely where the subject consents to it, or where it is strictly necessary for law enforcement purposes.[70]

The South Wales Police argued that they process biometric data on persons on their watch lists only, and not on the public at large.[71] The court rejected this notion and held that automated facial recognition processes biometric data for people on the watch list as well as those of the public at large.[72]

[67] *Bridges* para 90.

[68] *Bridges* para 92.

[69] *Bridges* para 108.

[70] S 35 of the *Data Protection Act* of 2018 also stipulates that when sensitive data are processed, the "controller" should have an appropriate policy document in place.

[71] *Bridges* para 129.

[72] *Bridges* paras 131-132.

The reason for this is that the system individualises facial features, an act which falls within the category of "identifying".[73]

Seeing that sensitive biometric data are processed, the *Data Protection Act* 12 of 2018 states further in section 64 that an impact assessment is needed when processing such sensitive data. The purpose of this is clearly to limit the intrusion on the public's right to privacy. The South Wales Police did in fact have such an impact assessment in place which limits in clear language the police's actions.[74] As the police's primary focus was limited to persons on the police's watch list, the larger public's rights were not unreasonably infringed, since the impact assessment implemented adequate safeguards to protect those rights by prescribing a specific length of time that the records might be kept.[75] As adequate safeguards were in place to protect the public's rights, Mr Bridges' claim on this ground failed.[76]

2.5.3 Claim 3: The Public Sector Equality Claims

Bridges' public sector equality claims stemmed from section 149(1) of the *Equality Act* 15 of 2010, which aims to eliminate discrimination, advance equality among people and foster good relations between "persons who share a relevant protected characteristic and persons who do not share it".[77] The issue at hand is that automated facial recognition technology is apparently inherently discriminatory as it leads to a higher rate of false positives in females and people of colour. Mr Bridges claimed that the South Wales Police Impact Assessment did not take this issue into consideration, and as a result it contravened section 149(1) of the *Equality Act* 15 of 2010.[78]

The court did not accept this contention. The only piece of evidence supplied by the claimant was an expert witness' opinion that automated facial recognition algorithms perform better on demographics they were trained on, i.e., if the algorithm was trained on "white North European"[79] male faces, it would generally perform better with that demographic group. The expert never specifically said that other automated facial recognition

[73] In *Bridges* para 132 the court states: "Although SWP's overall purpose is to identify the persons on the watch list, in order to achieve that overall purpose, the biometric information of members of the public must also be processed so that each is also uniquely identified, i.e., in order to achieve a comparison."
[74] *Bridges* para 148.
[75] *Bridges* para 148.
[76] *Bridges* para 148.
[77] S 149(1) of the *Equality Act* of 2010.
[78] *Bridges* paras 151-152.
[79] *R-Bridges* para 189.

algorithms necessarily fare worse on other demographics. As a result, the South Wales Police could not have known or foreseen that the software might operate contrary to anticipations. According to the court there was still no evidence that the software was inherently discriminatory.[80] As a result the claimant's Public Sector Equality claims were dismissed.

Mr Bridges took the matter to the England and Wales Court of Appeal.

3 *The Queen (on application of Edward Bridges) v The Chief Constable of South Wales Police*

The appeal relied on five grounds:

Ground 1: The court *a quo* erred in concluding that interfering with the appellant's rights under Article 8(1) of the *European Convention on Human Rights* by the South Wales Police was lawful.[81]

Ground 2: The court *a quo* failed to consider how the automated facial recognition technology caused a cumulative interference with Article 8 rights.[82]

Ground 3: The court *a quo* erred in holding that the South Wales Police's Data Protection Impact Assessment complied with section 64 of the *Data Protection Act* 12 of 2018, specifically with regard to the processing of facial features of people *not* on the police's watch lists.[83]

Ground 4: The court *a quo* erred by not reaching a conclusion as to whether the South Wales Police had an "appropriate policy document" in place. The appellant contended that in order to conclude that the first data principle of section 35 of the *Data Protection Act* 12 of 2018 has been complied with, a determination on the validity of the "appropriate policy document" had first to be made.[84]

Ground 5: The court *a quo* erred in holding that the South Wales Police's Equality Impact Assessment complied with its Public Sector Equality Duty, as set out in Section 149 of the *Equality Act* 15 of 2010.

[80] *Bridges* para 153.
[81] *R-Bridges* para 53.
[82] *R-Bridges* para 53.
[83] *R-Bridges* para 53.
[84] *R-Bridges* para 53.

3.1 Ground 1: Lawful Interference under Article 8 of the European Convention on Human Rights

Regarding the technology in the present case, the court accepted that it was "more than" simply taking photographs.[85] The court mentioned specifically that automated facial recognition technology was new,[86] that it involved processing large numbers of images of members of the public,[87] that the vast majority of the images processed would not be important to the police,[88] that it was indeed "sensitive",[89] and that the data were processed in an automated way.[90]

Having taken into consideration all these factors, the court concluded that the legal framework as it stood was insufficient as it provided too much discretion for individual police officers. The court said, more specifically, that it was "not clear who can be placed on the watch list nor is it clear that there are any criteria for determining where automatic facial recognition can be deployed."[91]

Furthermore, the court contended that a crucial feature of automated facial recognition deployment was:

> [t]hat the data of anyone where there is no match with a person on the watch list is automatically deleted without any human observation at all and that this takes place almost instantaneously. We would hope that that feature of the current scheme would not simply be set out in a policy document by way of description but that it would be made clear that such automatic and almost instantaneous deletion is required for there to be an adequate legal framework for the use of AFR Locate.[92]

The court made a very important point, and it should be emphasised again: it is a requirement for the lawful deployment of automated facial recognition technology that processed images of the public at large should be deleted automatically, and immediately after it is evident that the facial data do not match those on the watch list. The facial data of the masses should therefore not be viewable by or accessible to any member of the police department at a later stage.

[85] *R-Bridges* para 85.

[86] *R-Bridges* para 86.

[87] *R-Bridges* para 87.

[88] *R-Bridges* para 87.

[89] *R-Bridges* para 88.

[90] *R-Bridges* para 89.

[91] *R-Bridges* para 91.

[92] *R-Bridges* para 93.

The court held that the current framework within which automated facial recognition was deployed was not sufficient and was therefore not lawful. In paragraph 94 the court stated:

> We are satisfied, however, that the current policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary quality of law.[93]

Turning back to the question on who could be placed on the automated facial recognition watch list, the court looked at the South Wales Police's own Standard Operating Procedures. These procedures simply mentioned that a pre-populated watch list may be compiled, but did not specifically mention how the watch list would be compiled, or the criteria for who would be included in the watch list.[94] The entries in the watch list were limited to 2000, but this was simply due to a contractual limitation between the South Wales Police and the automated facial recognition service provider.[95]

After examining the South Wales Police's Standard Operating Procedures, the court concluded that the procedures did not adequately limit the scope of who should be placed on the watch list.[96]

The court then briefly addressed the question of where AFR Locate might be deployed.[97] From the facts it became evident that the South Wales' Standard Operating Procedures did not make any mention of this, and the court concluded that this issue was deficient in the Procedures manual. This was to be corrected.

After taking all these issues into consideration, the court held that the appeal on this ground should succeed, since the legislative framework for using automated facial recognition technology was not sufficient.[98]

3.2 Ground 2: Proportionality

The court of appeal stressed that the issue of proportionality was whether the court *a quo* erred in its finding, and was not a finding of proportionality de novo. The court *a quo* noted that automated facial recognition had a negligible effect on the applicant's rights, as the facial data were deleted instantly after the computer had made the assessment that the appellant's

[93] *R-Bridges* para 94.

[94] *R-Bridges* paras 56, 80, and in particular 121.

[95] *Bridges* para 31.

[96] *R-Bridges* para 129.

[97] *R-Bridges* para 130.

[98] *R-Bridges* para 130.

features did not meet those on the watch list. The court of appeal came to a similar conclusion, and added that an:

> [i]mpact that has very little weight cannot become weightier simply because other people were also affected. It is not a question of simple multiplication.[99]

Consequently, this ground of appeal was rejected.

3.3 Ground 3: Data Protection Impact Assessment

The South Wales Police compiled a Data Protection Impact Assessment, as required by section 64(3)(b) of the *Data Protection Act* 12 of 1998. This Assessment was compiled under the impression that Article 8 of the *European Convention on Human Rights* was not infringed, however, and as it was infringed (as held in Ground 1 above), the Data Protection Impact Assessment, as it stood, was deficient. Consequently, this ground was upheld on appeal.

3.4 Ground 4: Compliance with Section 42 of the Data Protection Act

This ground was based on a technical point of law which did not deal with the deployment of automated facial recognition *per se.* Section 42 of the *Data Protection Act* 12 of 2018 set out the requirements of a "policy document" that had to be in place when any "personal data" were processed by law enforcement officers. The court simply held that the appeal on this ground should fail, seeing that the *Data Protection Act* 12 of 2018 was not in force when the two so-called "infringing" occurrences took place.[100]

3.5 Ground 5: Public Sector Equality Duty

This duty dealt with the elimination of discrimination based on certain factors, such as race, religion and sexual preference as stipulated by section 149(1) of the *Equality Act* 15 of 2010. Facial recognition software may supposedly be biased towards people from "black, Asian and other minority ethnic ... backgrounds, and also in the case of women."[101] Apparently automated facial recognition software is "trained" on "white

[99] *R-Bridges* para 143.

[100] *R-Bridges* paras 155-162.

[101] *R-Bridges* para 164.

North European"[102] males, and as a result it may produce more false positives with non-white facial biometrics.[103]

The court referred to a number of cases where it had been illustrated how important and non-delegable the Public Sector Equality Duty is.[104] Law enforcement officers should therefore do their utmost to discharge this duty.[105] Having said that, the court was of the opinion that the South Wales Police had not discharged this duty adequately, as they had not investigated the possibility of bias on the part of the software, but had taken its workings on face value.[106] As a result, the appellant's claim on this ground was upheld.[107]

In conclusion the court of appeal held that the appropriate remedy was declaratory in nature, as agreed by the parties.[108] The gist of the order was threefold:

(a) The use of automated facial recognition was not in accordance with the law for the purposes of Article 8(2) of the *European Convention on Human Rights*;[109]

(b) The respondent's Data Protection Impact Assessment did not comply with section 64(3)(b) of the *Data Protection Act* 12 of 1998;[110] and

(c) The respondent had not discharged his Public Sector Equality Duty, as stipulated by section 149 of the *Equality Act* 15 of 2010.[111]

4 Automated Facial Recognition and the law

From the discussion up to this point it is evident that both the court *a quo* and the court of appeal dealt with automated facial recognition in the very specific context of legislation in the United Kingdom. It would therefore be

[102] *R-Bridges* para 189.

[103] *R-Bridges* para 193. The court was clear in noting that it is not alleged that the particular "AFR Locate" software is necessarily biased, but rather that the South Wales Police did not take such a possibility into consideration when deploying the automatic facial recognition software. *R-Bridges* para 165.

[104] *R (Brown) v Secretary of State for Work and Pensions* [2008] EWHC 3158 (Admin); [2009] PTSR 1506; *R (Hurley & Moore) v Secretary of State for Business, Innovation and Skills* [2012] EWHC 201 (Admin); [2012] HRLR 13.

[105] *R-Bridges* para 176.

[106] *R-Bridges* para 201.

[107] *R-Bridges* para 202.

[108] *R-Bridges* para 210.

[109] *R-Bridges* para 210.

[110] *R-Bridges* para 210.

[111] *R-Bridges* para 210.

prudent at this point to extract the most relevant general principles in the judgements to determine the way in which South African law may benefit from them.

(a) Automated facial recognition is a new technology with the potential to be very intrusive on people's human rights;[112]

(b) Although automated facial recognition may infringe upon people's rights, it does not preclude law enforcement from using it;[113]

(c) For automated facial recognition to be used in law enforcement, it has to be deployed within a very specific legal framework;[114]

(d) Automatic facial recognition information should not be collected unless there is a specific need to do so;[115]

(e) Automatic facial recognition information should not be kept for longer than is necessary;[116]

(f) A limitation of further processing of biometric data should be introduced in the legal framework. This would limit possible violations of human rights by law enforcement personnel;[117]

(g) Human verification of biometric matches is extremely important, and should be a specific requirement when automated facial recognition is used in law enforcement;[118]

(h) The principles laid down in this judgement specifically deal with overt law enforcement. It is argued that an even more restrictive legal framework should exist to regulate the covert use of automated facial recognition.[119]

4.1 South African law

Although automatic facial recognition is a very new technology, our law is already able to deal with a number of its pertinent issues, albeit in a limited fashion. Automatic facial recognition is a *species* of the larger issue of

[112] *R-Bridges* para 58.
[113] *Bridges* para 5.
[114] *R-Bridges* para 3.
[115] *R-Bridges* paras 148-149.
[116] *R-Bridges* paras 4, 20 and 22.
[117] *R-Bridges* para 4.
[118] *R-Bridges* paras 32 and 115.
[119] *R-Bridges* para 126.

"biometrics", and this has been addressed in at least[120] one piece of legislation, namely the *Protection of Personal Information Act* 4 of 2013 (POPI Act).

4.1.1 The Protection of Personal Information Act

Section 1 of the POPI Act defines "biometrics" as:

> [a] technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.[121]

This is a much better definition than that of "biometrics" contained in the *Births and Deaths Registration Act* 51 of 1992. In the latter Act "biometrics" is defined as:

> [p]hotographs, fingerprints (including palm prints), hand measurements, signature verification or retinal patterns that may be used to verify the identity of individuals.[122]

A cursory reading of the two definitions will immediately show why the former definition is preferred over the latter one. In the POPI Act an added generic phrase acts as a "catch all" to include situations which the legislature did not foresee at the time. The latter definition does not include such a "catch all" phrase, and consequently it does not make provision for the situation under discussion, namely automatic facial recognition. Notice how the phrase "a technique of personal identification that is based on physical, physiological or behavioural characterisation" incorporates automatic facial recognition. Consequently, the provisions of the POPI Act are applicable to our discussion of automatic facial recognition, even though the generic term of "biometrics" is used.

Section 26(a) of the POPI Act creates a general prohibition on collecting biometric information.[123] In this same section a prohibition on collecting information based on race, sex or ethnic origin is also created,[124] which is quite convenient for the remainder of the discussion. The court of appeal in *R-Bridges* talked at length about race, sex, and ethnic origin within the context of automated facial recognition, and as the POPI Act does the same,

[120] There are a number of Acts addressing biometrics, such as s 9(1A) of the *Births and Deaths Registration Act* 51 of 1992; S 22(a) of the *Tax Administration Act* 28 of 2011 and s 1 of the *Promotion of Access to Information Act* 2 of 2000. These pieces of legislation are, however, not relevant to this study.

[121] S 1 of the *Protection of Personal Information Act* 4 of 2013.

[122] S 1 of the *Births and Deaths Registration Act* 51 of 1992.

[123] Also see Botha 2018 *TSF* 42 and Pienaar 2014 *SAJHR* 523 fn 144.

[124] Roos 2020 *CILSA* 12 and Staunton *et al* 2019 *SAMJ* 469.

it is a good sign that the South African legislature was on the right track when creating this section.

The prohibition on collecting information created in section 26 is subject to the provisions created in section 27, which creates an array of situations where collecting biometrics would be permissible. The first is where the data subject consents to the collection of biometric information.[125] In the context of automated facial recognition this provision may come into play, but it might be a difficult matter for law enforcement to prove that subjects have given consent. The case of *R-Bridges* illustrates this point very well, where the appellant specifically mentioned that he was not aware of the automated facial recognition surveillance until he was well within the range of the cameras. Whether this situation would constitute valid consent is doubtful.

Section 27(1)(b) would probably be of more value if automated facial recognition should be deployed in South Africa. Biometric information may be collected without the subject's consent if it "is necessary for the establishment, exercise or defence of a right or obligation in law." Enforcing South African laws falls clearly within this category, which means that this provision could easily be used to justify the use of automated facial recognition by law enforcement. Using automated facial recognition is thus clearly permitted in this subsection, but the boundaries within which it should be used should be extracted elsewhere.

Before this is done, section 33(1) of the POPI Act should be discussed, as it links directly to section 27(1)(b) above. Section 33(1) specifically authorises "bodies charged by law with applying criminal law" to collect biometric information. This is obviously applicable to all law enforcement officers, and the section even goes beyond this to include "responsible parties who have obtained that information in accordance with the law". This would probably refer to third parties, and in the context of this discussion it would include any non-law enforcement officer who might be involved in operating the automated facial recognition system. More specifically it seems that this provision goes beyond those found in *R-Bridges*. In that case the South Wales Police officers were the only ones permitted to use the automated facial recognition system. In the context of section 33(1) of the POPI Act it would seem that the South African police might even be permitted to employ third-party, knowledgeable personnel to perform

[125] S 27(1)(a) of the POPI Act.

automated facial recognition on their behalf.[126] If this is the case, then this section is indeed a source of great concern.

The Bridges court of appeal case illustrates how important it is to have an adequate legislative framework within which automated facial recognition should be regulated and deployed. The POPI Act does provide for the development of such a framework in sections 13, 14, 15 and 60.

The first provision in this group, section 13, starts off on an excellent note by stating that personal information must be collected for a specific purpose. This is perfectly in line with what the district court and the court of Appeals decided in *R-Bridges*. Such a stipulation limits the discretion of specific police officers and protects the rights and freedoms of the public.

In a similar vein, section 14(1) stipulates that records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed. Again, this is in line with what the South Wales Police did when they implemented automated facial recognition. If automated facial recognition should be used in South Africa and these provisions are adhered to, then this would mean that if the collected facial data do not match those on the watch list, then they should be deleted, as the purpose of the data collection has been realised.

Up to this point it seems that the principles outlined above create an adequate initial framework to safeguard citizens' rights if automated facial recognition should be deployed in South Africa. Unfortunately, this is not the case. Section 14(1) creates four exceptions where biometric data may be retained for longer periods of time. Two exceptions are pertinent to this study, namely:

[126] In practical terms this might be very easy to achieve. Fibre optical internet has been widely deployed in South Africa since 2019. A system of fibre-enabled CCTV cameras (commonly known as Vumacam) has also been deployed in conjunction with this system, and as automated facial recognition can be sourced from any common CCTV stream, the South African Police may easily contract this third-party service provider to deploy automated facial recognition on their behalf. If sufficient processes are not in place, this could easily be a major concern for the infringement of the human rights of ordinary South Africans; See Vumacam 2020 www.vumacam.co.za. The Johannesburg Road Agency (JRA) was already embroiled in a court case about the issuing of wayleaves, which permits Vuma to deploy the CCTV camera network. Apparently the JRA was concerned that the Vumacam system might be used to infringe upon the public's human rights; See TechCentral 2020 https://techcentral.co.za/vumacam-wins-spy-camera-court-case-against-city/100653/.

(a) retention of the records is required or authorised by law, and

(b) the records are reasonably required for "lawful purposes related to its functions or activities".

In essence these two provisions create a loophole for law enforcement to exercise wide discretion when deploying automated facial recognition. What "lawful purposes related to its functions or activities" might entail is an open question, since the Act itself does not shed any light on this phrase. It is quite foreseeable that automated facial recognition biometrics collected from the public might be retained and included in a larger database, just as fingerprints are collected and collated at government departments.[127] It could easily be argued that such a collection of automated facial recognition is related to the work of the police to enforce law and order. If this were to be the case, then a main requirement for the deployment of automated facial recognition, as stipulated in both the Bridges decisions, falls away, namely that one of the bedrock principles requires the immediate deletion of records if they do not match those on the watch list.

In all fairness, section 15 of the POPI Act does include a limitation on the further processing of biometric data. Unfortunately, this section is equally fraught with vague statements, such as section 15(c)(i), which specifically allows for the further processing of data "to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences." From the Bridges court of appeal case, it is abundantly clear that providing a wide discretion to law enforcement is not the correct approach. Instead there should be well-defined rules that specify the exact parameters within which law enforcement should operate. In essence section 15(c)(i) follows the exact opposite approach to that of the Bridges decision by widening the discretion of collectors of biometric data rather than narrowing it.

From the discussion up to this point it is abundantly clear that the legislative framework within which a technology like automated facial recognition could be deployed in South Africa is far from ideal. Fortunately, this situation might

[127] The unfortunate practice of collating biometric information from unsuspecting members of the public is vividly illustrated by the Australian drivers' licensing system. Since 2009 facial biometric information has been captured from drivers' licence photographs. Since then, police have supplemented this information by police-body-worn cameras and surveillance drones. In 2015 the *Road Transport Legislation Amendment Act* ushered in a new era by allowing all this information to be shared across different government departments such as the Australian Security Intelligence Organisation. See Mann 2017 *UNSWLJ* 125-126.

be remedied if section 60 of the POPI Act is correctly applied. It provides for the issuing of Codes of Conduct which might regulate the collection of biometric information[128] in specific situations. In *R-Bridges* it was shown how the legislative framework is contained in "hard law", like the *Data Protection Act* 29 of 1998 and *Data Protection Act* 12 of 2018, or the *Protection of Freedoms Act* 9 of 2012, but that it is also included in "soft law" like the South Wales Police's Standard Operating Procedures, or the Surveillance Camera Code of Practice. In equal vein it would be quite possible, and very desirable, that section 60 of the POPI Act could be used to delineate the parameters of automated facial recognition. The two Bridges' court cases have provided an excellent outline of the principles applicable to the use of automated facial recognition, and creating a Code of Conduct for use in automated facial recognition is certainly the way forward for the South African Regulator.

5 Conclusion

The two cases of *Bridges* and *R-Bridges* are excellent benchmarks for providing many useful principles for the lawful use of automated facial recognition in law enforcement. It explains that this new technology may be used to assist law enforcement in performing its duties, and also outlines the pitfalls that the use of automated facial recognition may present in practice. It seems that the overarching issue with automated facial recognition in law enforcement is that an enabling but also limiting legal framework should be established to adequately regulate this technology, which has the potential to massively infringe on the human rights of the public.

A general prohibition on collecting biometric information is a sound principle, but it is understandable that such a prohibition should not be absolute. One of the bedrock principles of collected automated facial recognition biometrics is that they should be kept for the shortest possible time, and if possible, deleted immediately if they do not match the data in the watch list. Furthermore, specific parameters should be laid down to specify when this kind of surveillance should be used, and who will be included in the watch list.

[128] Technically this section, as well as the entire Act, deals with the collection of personal information, but as this study deals with automatic facial recognition in particular, the comments are focussed on biometrics, which will include automatic facial recognition as well.

This study has shown that the stub of an enabling legal framework for the use of automated facial recognition is present in South African legislation, and that it is contained in a number of provisions in the POPI Act. However, while the enabling legal framework for automated facial recognition is far from ideal, it could be remedied if the Regulator were to create a Code of Conduct fashioned on the well-defined principles enunciated in this study.

Bibliography

Literature

Botha 2018 *TSF*
Botha J "Medical Records and POPI" 2018 *TSF* 40-42

De Marsico *Face Recognition*
De Marsico M (ed) *Face Recognition in Adverse Conditions* (IGI Global Hershey 2014)

De Sousa *Neuromarketing*
De Sousa J *et al Neuromarketing and Big Data Analytics for Strategic Consumer Engagement* (IGI Global Hershey 2017)

Hawthorne *Fingerprints*
Hawthorne M *Fingerprints: Analysis and Understanding* (CRC Press Boca Raton 2009)

Kamila *Handbook of Research on Emerging Perspectives*
Kamila N *Handbook of Research on Emerging Perspectives in Intelligent Pattern Recognition, Analysis, and Image Processing* (IGI Global Hershey 2015)

Lee-Morrison *Portraits of Automated Facial Recognition*
Lee-Morrison L *Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face* (Transcript Bielefeld 2020)

Li *Handbook of Face Recognition*
Li S *et al Handbook of Face Recognition* (Springer London 2011)

Makin *DNA and Property Crime Scene Investigation*
Makin D *DNA and Property Crime Scene Investigation: Forensic Evidence and Law Enforcement* (Anderson Amsterdam 2014)

Mann 2017 *UNSWLJ*
Mann M *et al* "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight" 2017 *UNSWLJ* 121-145

Pienaar 2014 *SAJHR*
Pienaar L "Access to the Medical Records of a Child: Legislative Review Required" 2014 *SAJHR* 508-525

Roos 2020 *CILSA*
Roos A "The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'" 2020 *CILSA* 1-37

Staunton *et al* 2019 *SAMJ*
Staunton C *et al* "Safeguarding the Future of Genomic Research in South Africa: Broad Consent and the Protection of Personal Information Act No 4 of 2013" 2019 *SAMJ* 468-470

Case law

Edward Bridges v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin)

PG and JH v United Kingdom [2001] ECHR 546 (25 September 2001)

R (Brown) v Secretary of State for Work and Pensions [2008] EWHC 3158 (Admin); [2009] PTSR 1506

R (Hurley & Moore) v Secretary of State for Business, Innovation and Skills [2012] EWHC 201 (Admin); [2012] HRLR 13

R (S) v Chief Constable of the South Yorkshire Police [2004] 1 WLR 2196

R (Wood) v Commissioner of Police of the Metropolis [2010] 1 WLR 123

S and Marper v United Kingdom [2009] 48 EHRR 50

The Queen (on application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058

Legislation

Australia

Road Transport Legislation Amendment Act, 2015

South Africa

Births and Deaths Registration Act 51 of 1992

Tax Administration Act 28 of 2011

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

United Kingdom

Data Protection Act 29 of 1998

Data Protection Act 12 of 2018

Equality Act 15 of 2010

Police Act 16 of 1996

Protection of Freedoms Act 9 of 2012

International instruments

European Convention on Human Rights (1950)

Internet sources

Davies, Dawson and Innes 2020 https://theconversation.com/how-facial-recognition-technology-aids-police-107730
Davies B, Dawson A and Innes M 2020 *How Facial Recognition Technology Aids Police* https://theconversation.com/how-facial-recognition-technology-aids-police-107730 accessed 31 August 2020

TechCentral 2020 https://techcentral.co.za/vumacam-wins-spy-camera-court-case-against-city/100653/
TechCentral 2020 *Vumacam Wins 'Spy Camera' Case Against City* https://techcentral.co.za/vumacam-wins-spy-camera-court-case-against-city/100653/ accessed 31 August 2020

Vumacam 2020 https://www.vumacam.co.za/
Vumacam 2020 *Vumacam* https://www.vumacam.co.za/ accessed 31 August 2020

List of Abbreviations

AFR	Automated Facial Recognition
CCTV	Closed Circuit Television
CILSA	Comparative and International Law Journal of Southern Africa
DNA	Deoxyribonucleic Acid
POPI Act	Protection of Personal Information Act 4 of 2013
SAJHR	South African Journal on Human Rights
AMJ	South African Medical Journal
SWP	South Wales Police
TSF	The Specialist Forum
UNSWLJ	University of New South Wales Law Journal