FACIAL RECOGNITION, LAW ENFORCEMENT AND THE IDENTITY-AUSTRALIAN MATCHING SERVICES ('IMS') BILL

RECONHECIMENTO FACIAL, APLICAÇÃO DA LEI E O PROJETO DE LEI IDENTITY-MACHING SERVICE (IMS) AUSTRALIANO

Shana Schlottfeldt[1]

Abstract: This paper focus on the use of facial recognition technology ('FRT') by Australian government for the purpose of law enforcement. The use of FRT to law enforcement presents several challenges (risks) for which there are no easy solutions, but that need to be recognized more broadly, such as the lack of accuracy, bias, impact on civil liberties (privacy), security risks. This research has a qualitative nature and was developed through bibliographic research. Part I describes how FRT works and its risks. Part II makes considerations on the employment of FRT in Australia to identity-matching. Part III talks about the Identity Matching Services ('IMS') Bill, introduced in 2018 to facilitate the sharing of identification information (including facial images) within the government; this legislation lapsed on the dissolution of parliament and, as will be discussed, at least how it is now, it should not be revived.

Keywords: Biometrics. Facial recognition. Identity matching. Human rights. Australia.

[1] Ph.D. in Informatics from University of Brasília. M.S. in Informatics from Universidad Carlos III de Madrid. LLB exchange student at Australian National University. LLB student at University of Brasília.

Resumo: Este artigo enfoca o uso da tecnologia de reconhecimento facial (FRT) pelo governo australiano para fins de aplicação da lei. O uso da FRT para aplicação da lei apresenta vários desafios (riscos) para os quais não há solução fácil, mas que precisam ser reconhecidos de forma mais ampla, e.g., falta de precisão, preconceito, impacto nas liberdades civis (privacidade) e riscos de segurança. Esta pesquisa possui natureza qualitativa e foi desenvolvida ao por meio de pesquisa bibliográfica. A Seção I descreve como a FRT funciona e seus riscos. A Seção II faz considerações sobre o emprego da FRT na Austrália para fins identificação. A Seção III fala sobre o Projeto de Lei "Identity Matching Services" (IMS), lançado em 2018 para facilitar o compartilhamento de informações de identificação (incluindo imagens faciais) dentro do governo; essa legislação caducou com a dissolução do parlamento e, como será discutido, pelo menos como está agora, não deve ser reapresentada.

Palavras-chave: Biometria. Reconhecimento facial. Identificação. Direitos humanos. Australia.

Submissão: 29/03/2020
Aceite: 27/06/2020

INTRODUCTION

The use of biometrics in law enforcement investigation and other applications has significantly increased in the last few years (LYON, 2008, p. 500). According to the International Standards Organisation, *biometric recognition* is the 'automated recognition of individuals based on their biological and behavioural characteristics', (e.g., fingerprint, DNA, eye retina and irises, voice, facial image, gait and keystroke patterns); and *automated recognition* 'implies that a machine-based system is used for the recognition, either for the full process or assisted by a human being'(ISO/IEC, 2017). In this sense, *facial recognition technology* ('FRT') is the automated process of one-to-many 'matching' faces to determine whether they represent the same individual, utilizing biometric scanning technologies and algorithms (BIOMETRICS GROUP, 2019, p.1; GARVIE, BEDOYA, FRANKLE, 2016, p. 116).

This paper focus on the use of FRT by government for the purpose of law enforcement. Part I describes how FRT works and its risks. Part II makes considerations on the employment of FRT in Australia to identity-matching. Part III talks about the Identity Matching Services ('IMS') Bill, introduced in 2018 to facilitate the sharing of identification information (including facial images) within the government; this legislation lapsed on the dissolution of parliament and, as will be discussed, at least how it is now, it should not be revived.

I HOW DOES FRT WORK AND WHAT ARE THE RISKS?

FRT generally performs at least one of three things (LYNCH, 2018, p. 5-6):

- Identify an unknown person (e.g., from a surveillance camera footage).
- Confirm the identity of a known person (e.g., to unlock a smartphone).
- Look for multiple specific, previously-identified faces (e.g. wanted persons on a subway platform, shoppers in a store, card counters at a casino).

In order to identify an individual, the algorithm proceeds through the following steps (GARVIE, BEDOYA, FRANKLE, 2016, p. 9, 46; ADLER, SCHUCKERS, 2007, 1248-49; RICANEK, BOEHNEN, 2012, p. 95; LYNCH, 2018, p. 4-6; WOODWARD JR et al, 2003, p. 3-4):

- Face detection: find the person within the photo or video segment.
- Normalization: once detected, the face is scaled, rotated and aligned, in order to be easier for the algorithm to compare the images at the 'same position'.
- Extraction of features: attributes that can be numerically quantified (e.g., skin texture, eye distance, shape of chin) are identified. FRT records not the face itself, but the spatial geometry of distinguishing features of the face.
- Pair comparison: the algorithm check pairs of faces (the image is compared to other faces previously collected and stored in a repository) and returns a numerical score indicating their features similarity.

As can be apprehended, FRT is intrinsically probabilistic. Its output is not a binary answer, but a probability match score between the searched face and faces stored in a database. Generally, FRT will return those photos above a similarity threshold, ranked in likelihood order of correct identification (LYNCH, 2018, p. 6).

The use of FRT to law enforcement presents several challenges (risks) for which there are no easy solutions, but that need to be recognized more broadly. Following, we approach some of them.

A ACCURACY

FRT is less accurate than, for instance, fingerprinting, especially when used in real-time or on large databases (GARVIE, BEDOYA, FRANKLE, 2016, p. 3, 46). Several factors influence a match probability/accuracy, such as (BIOMETRICS GROUP, 2019, p. 2; HAMANN, SMITH, 2019):

- The quality of the images (lighting, background, resolution, angle, facial expression, etc.).
- The environmental conditions where the image is captured (lighting, camera position, etc.).
- The size of the watchlist (dataset).

- The thresholds of match.
- The changes face suffers over time (e.g., body weight, facial hair, hairstyle, and the effects of aging).
- A near real-time response or not.
- If there is human action after machine-generated biometric match, and if this person is trained. It has been shown to be beneficial that human double-check the results of FRT, but, without specialized training, in half of the time, human users make the wrong decision about a match (WHITE et al, 2015, p. 6).

Since FRT vary in its ability to identify people, it should report its rate of errors, i.e., the number of false positives (aka 'false accept rate') and false negatives (aka 'false reject rate'), which not always happens (LYNCH, 2018, p. 6).

B. BIAS

Worries with efficacy extend to ethical considerations (INTRONA, NISSEMBAUM, 2009, p. 72). Concerns about potential gender and racial bias within FRT have already been raised (BOULAMWINI, GEBRU, 2018, p. 2-3). Pairs of photos of the same person are presented to the FRT algorithm during training; over time, the algorithm learns 'to concentrate' on the most relevant features. If a training dataset is composed by more samples representing a certain group, the algorithm may learn to better identify members of that group (GARVIE, BEDOYA, FRANKLE, 2016, p. 9). This is behaviour similar to the 'other-race effect', a phenomenon in which people have difficulty telling apart individuals of a different race to their own (ANU, 2019; McKONE et al., p. 1). Studies have shown that FRT misidentified 'people of colour and ethnic minorities, young people, and women' at higher rates than 'whites, older people, and men' (BOULAMWINI, GEBRU, 2018, p. 2-3; BIOMETRICS GROUP, 2019, p. 2). The formers, trigger more false positive recognition, and this kind of inaccuracy has impact on the 'presumption of innocence' by placing on them, the onus to show that they are not who the FRT identifies (LYNCH, 2018, p. 10).

C. IMPACT ON CIVIL LIBERTIES (PRIVACY)

Most of the technology used to track a person aim at belongings, e.g., cell phone, car, and computer. FRT takes tracking to a new level, they 'pursue' the person's body. The distinction is meaningful: you can dispose of your belongings, although your face… (GARVIE, BEDOYA, FRANKLE, 2016, p. 9). Furthermore, FRT can be more invasive than other forms of biometric identification (MANN, SMITH, 2017, p. 125): they can do the tracking remotely, in secrecy, and on a great amount of people (WOODWARD JR et al., 2003, p. 3-4).

Moreover, agencies are targeting to add 'crowd, closed circuit television ('CCTV'), driver's license photographs, social media' to their databases (MANN, SMITH, 2017, p. 121). In this case, anybody, even if not suspected of a crime, could end up in a database without their knowledge (RECTOR, KNEZEVICH, 2016; STONE, ZICKLER, DARRELL, 2010, p. 1408). This kind of surveillance threatens free speech and freedom of association (BIG BROTHER WATCH, 2018, p. 41), having a chilling effect on willingness to engage in public debate, to publicly disclose political views, to associate with others whose religion, values or political views may be considered different from the majority, generating what is called the 'spiral of silence' (STOYCHEFF, 2016, p. 297-299).

D. SECURITY RISKS

Like any other data, government data is also at risk of misuse and breach whether by:

- Insiders (e.g., in 2013, workers of the US National Security Agency ('NSA') were caught using surveillance records to spy on spouses, girlfriends, and boyfriends) (SELYUKH, 2013; GELLMAN, 2013).
- Outsiders (e.g., hackers. In June 2019, the UK Eurofins Forensics Services ('EFS') suffered a cyber-attack. EFS handles about 90% of England and Wales complex forensics toxicology work (over 70,000 criminal cases in the UK each year). A ransom to unlock the frozen accounts was established although it is not clear if EFS paid it) (HOUSE OF COMMONS SCIENCE AND TECHNOLOGY COMMITTEE, 2019, p. 9; SHAW, 2019).

Nonetheless, as mentioned, biometrics is unique to the person and cannot be easily changed, so, the consequences of a breach of face recognition could be more serious than other identifying data (LYNCH, 2018, p. 11).

E. CRIMINAL INVESTIGATION V LAW-ABIDING PEOPLE

Biometrics is being used in a way it has never done before. Historically, fingerprint and DNA databases have been made up of information from criminal arrests or investigations. By running face recognition searches, agencies have built a biometric network that primarily includes law-abiding people. This is unprecedented (GARVIE, BEDOYA, FRANKLE, 2016, p. 2).

II USE OF FRT IN AUSTRALIA

As can be seen, the use of FRT represents a point of tension between collective security and individual privacy (MANN, SMITH, 2017, p. 121; DIXON, 2019, p. 12).

Countries as the UK, US and Russia have integrated FRT with CCTV (known as 'Smart CCTV') and some Australian Jurisdiction, as Northern Territory and Queensland, as well. In New South Wales, FRT was introduced through an amendment to the regulations governing drivers' licenses (NEC, 2015; MANN, SMITH, 2017, p.123; PETRIE, 2018, p. 5; NSW, 2009).

Several advantages have been appointed in the use of FRT (NEC, 2015):

- The system allows fast search through a photography database and match against any image or CCTV footage, as well as photos taken from body-worn camera videos, drones and phone images.
- Compared to fingerprinting, face images can be captured from a distance without touching the person being identified.
- The technology is helping reduce investigation time by enabling investigators to quickly identify or rule out suspects soon after a crime has been committed.

• It could assist police to identify missing persons (including who suffer from dementia or other similar health issues).

The annual cost of identity crime (in which a perpetrator uses a fabricated, manipulated or stolen identity to facilitate the commission of a crime) in Australia is estimated in $2.65 billion (JORNA, SMITH, 2018, p. x). And FRT could help prevent it.

FRT has long been used for immigration control and the issuing of visas. The Migration Act 1958 authorizes the collection of biometric data, including face images, from people (whether citizens or non-citizens) entering or leaving Australia; moreover, visa applicants located in certain countries are asked to supply biometric information (generally their fingerprints and facial image) during the application process (PETRIE, 2018, p.5).

FRT is used by airport SmartGates to check a traveller's identity by matching a live image captured at the SmartGate with the person ePassport photo, without needing to present the passport (O'SULLIVAN, 2018).

In 2015, the Commonwealth government announced that a National Facial Biometric Matching Capability ('NFBMC') was expected to function in 2016, enabling agencies to share facial information for the purpose of FRT (ATTORNEY-GENERAL'S DEPARTMENT, 2015). NFBMC has not been settle yet, but it is worth noting that it is being established through administrative processes in a way that 'does not require expanded police powers or the introduction of specific Commonwealth legislation', i.e., outside of a legislative framework, which weakens external scrutiny (MANN, SMITH, 2017, p. 127-128).

In 2016, under the Australian Criminal Intelligence Commission effort to integrate all police information systems, including biometric databases held by Australian police (state, territory and federal), NEC was contracted to implement the Biometric Identification Services (BIS) (AUSTENDER, 2016). The BIS was expected to form part of the NFBMC. Nevertheless, the project was discontinued in June 2018 due to a 'cost spiral' and a 'systemic pattern of delay', confirmed by the Australian National Audit Office ('ANAO') (AUSTRALIAN CRIMINAL INTELIGENCE COMMISSION, 2018; HENDRY, 2018; AUSTRALIAN NATIONAL AUDIT OFFICE, 2019). Now, NEC is suing the government for their losses (SHARWOOD, 2019).

As often is the case, there is a lag between technological improvements and regulation, especially FRT (MANN, SMITH, 2017, p. 121-122). In the USA, for instance (GARVIE, BEDOYA, FRANKLE, 2016, p. 35):

- 17 states regulated geolocation tracking.
- 13 states regulated the use of drones by the police.
- 9 states regulated police use of automated license plate readers.
- But not a single state has passed a law about the use of FRT.

In Australia, with the lack of a 'constitutional bill of rights or a cause of action for serious invasion of privacy, there are limited protections in relation to biometric information' (MANN; SMITH, 2017, p. 121-122). Although the Australian case *R v Tang* allowed facial mapping expert evidence (under the condition that the expert does not make positive identifications), there is no precedent for the use of FRT for positive identifications in criminal cases in Australia (R v TANG, 2006, §§ 681, 697 [57], 712 [135], 713-14 [143]-[146]). Australian authorities 'have begun amending legislation to enable driver licence photograph databases to be shared with federal agencies' (SMITH; MANN; URBAS, 2018, p. 54). Under these amendments, photos may be released for investigation of 'terrorism offence', 'threat of a terrorist act' and 'terrorist act', or even a 'relevant criminal activity' (MANN; SMITH, 2017, p. 126). The global 'war on terror' and concerns about security have been leading to legislative and executive measures that can be seen, sometimes, as a disproportionately intrusive erosion of civil liberties (COPER, 2007, p. 4). As consequence, the adoption of FRT is happening without serious supervision, without accuracy testing in the field, and without the 'enactment of legal protections to prevent internal and external misuse' (LYNCH, 2018, p. 1). Add to this, concerns related to information provided for a specific use being accessible for another purpose for which consent was neither solicited nor obtained (NICHOLLS, 2015).

III THE IDENTITY-MATCHING SERVICES BILL

In February 2018, the Commonwealth Government introduced the Identity-matching Services Bill 2018 ('IMS Bill') to establish a framework for sharing identification information – including facial images held in government databases (e.g., driver license, passport, and visa photographs) – between the federal, state and territory government agencies (and even some private organisations) for the purposes of identity-matching (PETRIE, 2018, p. 3-5). The IMS Bill (DEPARTMENT OF HOME AFFAIR, 2019):

- Authorises the Department of Home Affairs to collect, use and disclose identity-matching information.
- Specifies identity-matching services (e.g., the Face Verification Service and the Face Identification Service).
- States the necessity of a legal basis for collecting and disclosing personal information, although do not establish this legal basis.
- Creates an offence for entrusted persons to record or disclose protected information in connection with the services and define circumstances where disclosure will be authorized.

In April 2019, the Bill lapsed on the dissolution of parliament (PARLIAMENT OF AUSTRALIA, 2019). Legislation is an important option for addressing FRT matter, but the IMS Bill presents key issues that should be addressed before considering revive it, including (PETRIE, 2018, p. 17-28):

- Concerns that the broad scope of the Bill 'may enable substantial infringements on privacy rights, allowing disclosure of personal information for an extremely wide range of purposes'.
- The Bill 'provides inadequate protection against misuse of ... information', and it 'does not include key safeguards contained in the [Intergovernmental Agreement on Identity Matching Services] IGA (COUNCIL OF AUSTRALIAN GOVERNMENTS, 2017), such as access criteria and limitations on the amount of information released by the identity-matching systems'.
- Private sector access is another concern (it is questioned if it is appropriate).

The literature proposes certain recommendations that should be considered when proposing a bill that deals with FRT, and which the IMS Bill should take into account (GARVIE, BEDOYA, FRANKLE, 2016, p. 35, 62; LYNCH, 2018, p. 24-27; BIG BROTHER WATCH, 2018, p. 41):

- Impose limits on law enforcement face recognition.
- Limit the collection of data to the minimum necessary to achieve

the government's stated purpose.

- Define clear rules on the legal process required for collection.
- Limit the amount and type of data stored and retained.
- Limit retention period.
- Define simple and clear methods for an individual to request biometric removal from the system.
- Limit the association of biometric data in a single database (otherwise, it would increase the potential harm in case of data breach).
- 'Define clear rules for use and sharing (biometrics collected for one purpose should not be used for another)'.
- Enact robust security procedures.
- Define clear notice requirements (due to the fact that face prints can be collected without a person's knowledge).
- Define and standardize audit trails and accountability throughout the system.
- Ensure independent oversight.

IV. CONCLUSION

There are many benefits in the use of FRT, but also associated issues and controversy. On the one hand, FRT is helping achieve a rapid and efficient law enforcement response. On the other hand, FRT impacts peoples' privacy in many ways and will spark even more discussion about privacy boundaries. The use of FRT in Australia is growing, but it lacks a clear legal framework outlining FRT deployment to support law enforcement practices. As the technology improves, FRT role will continue to expand. In this scenario, it is important to try to reach a harmony between the right to privacy (private) and the need for information (public).

V. BIBLIOGRAFY

ADLER, A.; SCHUCKERS, M. E. Comparing Human and Automatic Face Recognition Performance. *IEEE Trans Syst Man Cybern B Cybern*, v. 37, n. 5, 1248-1260. 2007.

ANU. Early Exposure Key to Recognising 'Other-race' Faces. Australian National University (ANU), Newsroom, 13 September 2019. Disponível em: <https://www.anu.edu.au/news/all-news/early-exposure-key-to-recognising-%E2%80%98other-race%E2%80%99-faces>. Acesso em: 20 set. 2019.

ATTORNEY-GENERAL'S DEPARTMENT (Cth). *National Facial Biometric Matching Capability - Privacy Impact Assessment*: Interoperability Hub. August 2015.

AUSTENDER. *Contract Notice View - CN3343259*: Biometric Identification Services. Australian Government's Procurement Information System web page, 23 May 2016. Disponível em: <https://www.tenders.gov.au/Cn/Show/9156D484-FC31-5306-F65D-62AC112F52AE>. Acesso em 20 nov. 2019.

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION. *Biometric Identification Services Project to Close.* Australian Criminal Intelligence Commission web page, 15 June 2018. Disponível em: <https://www.acic.gov.au/media-centre/media-releases-and-statements/biometric-identification-services-project-close>. Acesso em: 20 nov. 2019.

AUSTRALIAN NATIONAL AUDIT OFFICE. *Report No 24 of 2018–2019.* The Australian Criminal Intelligence Commission's Administration of the Biometric Identification Services Project, 21 January 2019.

BIG BROTHER WATCH. *Face Off*: the Lawless Growth of Facial Recognition in UK Policing. London: Big Brother Watch, May 2018.

BIOMETRICS GROUP. *Ethical Issues Arising from the Police use of Live Facial Recognition Technology*. Biometrics and Forensics Ethics Group Facial Recognition Working Group ('Biometrics Group'). Interim report, February 2019.

BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Machine Learning Research, v. 81, n. 1, 1-15, 2018.

COPER, M. *Three Good Things and Three Not-So-Good Things about the Australian Legal System*. International Association of Law Schools Conference, Learning from Each Other: Enriching the Law School Curriculum in an Interrelated World. Kenneth Wang School of Law, Soochow University, Suzhou, China, 17-19 October 2007.

COUNCIL OF AUSTRALIAN GOVERNMENTS. Intergovernamental Agreement on Identity Matching Services. October 2017. Disponível em: <https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf>. Acesso em: 20 nov. 2019.

DEPARTMENT OF HOME AFFAIR. *Face Matching Services*. Fact Sheet, 2017. Disponível em: <https://www.homeaffairs.gov.au/criminal-justice/files/face-matching-services-fact-sheet.pdf>. Acesso em: 20 nov. 2019.

DIXON, R. Functionalism and Australian Constitutional Values in DIXON, R. (ed), *Australian Constitutional Values*. Oxford: Hart Publishing, 2018.

GARVIE. C; BEDOYA, A. M.; FRANKLE, J. *The Perpetual Line-up*: Unregulated Police Face Recognition in America. Washington: Law Center Center on Privacy & Technology, Georgetown University, 2016.

GELLMAN, B. NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds. *The Washington Post*, 15 August 2013. Disponível em: <https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html>. Acesso em: 20 nov. 2019.

HAMANN, K.; SMITH, R. Facial Recognition Technology: Where Will it Take Us?. American Bar Association Criminal Justice Magazine, Spring 2019. Disponível em: <https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/>. Acesso em: 20 nov. 2019.

HENDRY, J. NEC Loses National Biometrics Database Project. *IT News*, 15 June 2018. Disponível em: <https://www.itnews.com.au/news/nec-loses-national-biometrics-database-project-494059>. Acesso em: 20 nov. 2019.

HOUSE OF COMMONS SCIENCE AND TECHNOLOGY COMMITTEE. *The work of the Biometrics Commissioner and the Forensic Science Regulator*. Report of Session, 17 July 2019.

INTRONA, L. D.; NISSENBAUM, H. *Facial Recognition Technology*: a Survey of Policy and Implementation Issues. New York: The Center for Catastrophe Preparedness & Response, New York University, 2009.

ISO/IEC. ISO 2382-37: Information technology - Vocabulary - Biometrics. 2017.

JORNA, P.; SMITH, R. G. *Identity crime and misuse in Australia 2017.* AIC Statistical Report 10, 31 December 2018.

LYNCH, J. *Face Off*: Law Enforcement Use of Face Recognition Technology. San Francisco: Electronic Frontier Foundation, 2018.

LYON, D. Biometrics, Identification and Surveillance. *Bioethics*, v. 22, n. 9, 499-508. 2008.

MANN, M.; SMITH, M. Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight. *UNSW Law Journal*, v. 40, n. 1, p. 121-145, 2017.

McKONE, E.; WAN, L. PIDCOCK, M.; CROOKES, K.; REYNOLDS, K.; DAWEL, A.; KIDD, E.; FIORENTINI, C. A Critical Period for Faces: Other-race Face Recognition is Improved by Childhood but not Adult Social Contact. Nature, Scientific Reports, v. 12820, n. 9, 1-13, Sep. 2019.

NEC. NEC *Facial Recognition Helps NT Police Solve Cold Cases and Increase Public Safety in Australia.* NEC Web page, 1 September 2015. Disponível em: <https://www.nec.com/en/press/201509/global_20150901_02.html>. Acesso em: 20 nov. 2019.

NICHOLLS, S. Crime Commission Granted Access to Photographs of NSW Citizens to Aid Terrorism Fight. *The Sidney Morning Herald*, 18 October 2015. Disponível em: <https://www.smh.com.au/national/nsw/asio-crime-commission-granted-access-to-photographs-of-nsw-citizens-to-aid-terrorism-fight-20151018-gkbxa6.html>. Acesso em: 20 nov. 2019.

NWS. *Road Transport (Driver Licensing) Amendment (Facial Recognition Technology) Regulation 2009 under the Road Transport (Driver Licensing) Act 1998.*

O'SULLIVAN, M. *Your Face Will Be Your Passport*: Sydney Airport to Trial Biometrics. Sidney Morning Herald, February 2018. Disponível em: <https://www.smh.com.au/business/companies/your-face-will-be-your-passport-sydney-airport-to-trial-biometrics-20180221-p4z14p.html>. Acesso em: 22 nov. 2019.

PARLIAMENT OF AUSTRALIA. *Identity-matching Services Bill 2018 Information.* ParlInfo Search v1.30.0 web page. Disponível em: <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/billhome/r6031%22>. Acesso em: 2 set. 2019.

PETRIE, C. *Identity-matching Services Bill 2018 and Australian Passports Amendment.* Identity-matching Services. Bill 2018. Bills Digest No 110, 2017–18, 22 May 2018.

R v Tang (2006) 65 NSWLR 681.
RECTOR, K.; KNEZEVICH, A. Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates. *The Baltimore Sun*, 18 October 2016. Disponível em: <https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html>. Acesso em: 20 nov. 2019.
RICANEK, K.; BOEHNEN, C. Facial Analytics: From Big Data to Law Enforcement. *Computer*, v. 45, n.9, 95-97. 2012.
SELYUKH, A. NSA Staff Used Spy Tools on Spouses, Ex-lovers: Watchdog. *Reuters*, 28 September 2013. Disponível em: <https://www.reuters.com/article/us-usa-surveil-lance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927>. Acesso em: 20 nov. 2019.
SHARWOOD, S. NEC Sues Feds over Binned Biometric Identification Services Project. *IT News*, 19 July 2019. Disponível em: <https://www.itnews.com.au/news/nec-sues-feds-over-binned-biometric-identification-services-project-528468>. Acesso em: 20 nov. 2019.
SHAW, D. *Eurofins Scientific*: Forensic services firm paid ransom after cyber-attack. *BBC News*, 5 July 2019. Disponível em: <https://www.bbc.co.uk/news/uk-48881959>. Acesso em: 22 nov. 2019.
SMITH, M.; MANN, M.; URBAS, G. Facial Recognition in *Biometrics, Crime and Security*. Oxon: Routledge, 2018.
STONE, Z.; ZICKLER, T.; DARRELL, T. Toward Large-Scale Face Recognition Using Social Network Context. *Proceedings of the IEEE*, v. 98, n. 8, 1408-1415, 2010.
STOYCHEFF, E. Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. JOURNALISM & MASS COMMUNICATION QUARTERLY, v. 93, n. 2, 296-311, 8 March 2016.
WHITE, D.; DUNN, J. D.; SCHIMD, A. C.; KEMP, R. I. Error Rates in Users of Automatic Face Recognition Software. *PLoS ONE*, v. 10, n. 10, 1-14, 2015.
WOODWARD JR, J. D.; HORN, C.; GATUNE, J.; THOMAS, A. *Biometrics*: a Look at Facial Recognition. (Documented Briefing). Santa Monica: RAND Public Safety an Justice, 2003.