16

Regulating Facial Recognition in Brazil

Legal and Policy Perspectives

Luca Belli, Walter Britto Gaspar, and Nicolo Zingales

16.1 INTRODUCTION

Facial recognition technology (FRT) has been in use by the Brazilian public administration for various purposes since at least 2011. It has seen an uptick in the 2018–2019 period, with noteworthy implementations in Rio de Janeiro and São Paulo, among others.[1] Nonetheless, there is no general legislation or sectoral regulation on the use of FRT – thus leaving unregulated both its general implementation and specific uses, such as for public security, public transportation systems, or identification.[2]

This chapter aims at identifying vulnerabilities and opportunities posed by the use of FRT in Brazil, focussing on the current legislative and regulatory landscape. Thus, it shall attempt to describe the evolving legislative framework and assess its adequacy to deal with the risks to fundamental rights posed by such technologies.

To do so, we assume the reader's prior knowledge of the basic functioning of facial recognition. This allows us to dive deeper into the literature concerning the adoption of FRT in Brazil (in Section 16.1), prior to reviewing the existing legislation (Section 16.2) relating to its deployment, especially in the context of law enforcement. A final section (Section 16.3) concludes with a brief analysis of this normative framework and puts forward a few suggestions on how to improve the national normative framework.

16.2 IMPLEMENTATIONS OF FRT IN BRAZIL

Information on the implementation of FRTs in Brazil is scattered. States, municipalities, and the federal government have all implemented projects utilising the

[1] Instituto Igarapé, 'Reconhecimento facial no Brasil' (2021), https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/; Jonas Valente, 'Tecnologias de reconhecimento facial são usadas em 37 cidades no país' (19 September 2019), *Agência Brasil*, https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/tecnologias-de-reconhecimento-facial-sao-usadas-em-37-cidades-no-pais.

[2] FRA, 'Facial recognition technology: Fundamental rights considerations in the context of law enforcement' (2019), European Union Agency for Fundamental Rights, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf; Lucas Introna and David Wood, 'Picturing algorithmic surveillance: The politics of facial recognition systems' (2004) 2 *Surveillance & Society* 177.

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

technology, frequently without prior notice or consultation with civil society, which has hampered transparency and accountability. FRT is frequently introduced in the context of 'Smart City' programmes aiming at enhancing urban safety, in the absence of specific regulation and with no guidance from the National Data Protection Authority (ANPD) on how data protection impact assessments must be performed.[3] Alongside this, there are private implementations of FRT, which are even less transparent since there is no disclosure obligation of any kind.

Among several attempts at mapping FRT implementations in Brazil. the most recent one is Venturini and Faray,[4] which, drawing on access to information requests, search engines, and interviews with key actors, identifies six projects where facial recognition was being implemented. One is the emotion recognition contract for advertisement display purposes between Via Quatro, a private operator managing one of the subway lines at the city of São Paulo, and AdMobilize, an artificial intelligence (AI) analytics company headquartered in the United States.[5] Given the lack of notice and information over this contract, Idec, a civil society organisation acting in consumer rights issues, obtained a blocking injunction pursuant to a civil public action to uphold the rights of the users of the São Paulo subway system, where it argued that there was no consent for the collection and use of biometric data, no information on the functioning of the technology, the data processing, and its purposes, or the possibility to exercise data subject rights. Another project involved the subway administrator, Companhia do Metropolitano de São Paulo,[6] with the aim of installing FRT cameras for subway security in stations.[7]

Two other projects involved surveillance of public spaces: one in the city of Campina Grande, in the state of Paraíba, and the other in Itacoatiara, in the state of Amazonas. The former involves FRT-enabled cameras running Facewatch installed

[3] Jess Reia and Luca Belli, 'Smart cities no Brasil: regulação, tecnologia e direitos' (2021), http://bibliotecadigital.fgv.br:80/dspace/handle/10438/31403; Luca Belli, 'BRICS countries to build digital sovereignty' in Luca Belli (ed.), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries* (Springer International Publishing, 2021), https://doi.org/10.1007/978-3-030-56405-6_7; Luca Belli, 'Como implementar a LGPD por meio da Avaliação de Impacto Sobre Privacidade e Ética de Dados (AIPED)' in Laura Schertel Mendes, Danilo Doneda, Ingo Wolfgang Sarlet, Otavio Luiz Rodrigues Jr. and Bruno Bioni (eds.), *Tratado de Proteção de Dados Pessoais* (Forense, 2021).

[4] Jamila Venturini and Vladimir Garay, 'Reconhecimento Facial Na América Latina: Tendências Na Implementação de Uma Tecnologia Perversa' (2021), Fundación Karisma, https://estudio.reconocimientofacial.info/.

[5] Via Quatro informed in a press announcement that the technology would be implemented, without giving further details. Later news revealed that this was done through a partnership with LG and the pharmaceutical company Hyperapharma consisting in the projecting of their ads on digital screens of the subway equipped with cameras that would read and register the emotions in response to the ads.

[6] This was an 'empresa de economia mista' – a mixed controllership company in which the state is the controlling shareholder, but the company is legally structured as a private entity.

[7] Both Via Quatro and Cia. do Metropolitano de São Paulo's intent were halted by civil public actions moved by civil society organisations, the state's prosecutor office, and public defender's office. Via Quatro's implementation was grounded to a halt by judicial decree, but the case against Metropolitano de São Paulo is still ongoing (although an interim decision suspended the use of FRT).

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

during the city's São João festival, beginning in 2019. The cameras were still being utilised in 2022, when they aided in the arrest of twenty-five people during that year's festival and were expanded to two other cities in the same state (João Pessoa and Patos) via a command-and-control centre, totalling 1,600 cameras.[8] In Itacoatiara, a command centre was also created, with sixteen face recognition cameras for public security purposes.[9]

Finally, the authors highlight the use of FRT by the Federal Data Processing Service (SERPRO), a public company, to confirm the identity of driver's licence holders; and by SERPRO and the Social Service's information technology company (DATAPREV) to confirm identity and provide proof of living for social security beneficiaries.

A paper focussed on FRT application in public security and police work reports on the use of these technologies in the states of Bahia, Rio de Janeiro, Santa Catarina, and Paraíba from March to October 2019.[10] Although the specifics (contracting parties, public procurement format, etc.) are not disclosed, the article contains insightful information on the efficacy of such systems, which led to 151 arrests in total. Particularly, out of forty-two cases where information on race was available, 90.5 per cent of suspects were black and 9.5 per cent were white.[11] The research also analyses one specific case where FRT was applied for four days during the Carnival at Feira de Santana, a city in the state of Bahia, with an efficacy rate of less than 4 per cent.[12]

A more recent work by Nunes and colleagues goes into more detail about FRT in Rio de Janeiro.[13] The researchers scrutinise a pilot-project involving the deployment of FRT in Copacabana, during Carnival 2019, which was later expanded to two more areas of the city. The two-phase FRT programme for public security was managed by the State Military Police Office (SEPM) in a partnership with Oi, one of

[8] Governo de Paraíba, João Azevêdo Inaugura Centro Integrado de Comando e Controle e Sertão Ganha Equipamento Referência Para a Segurança Pública Do Nordeste. Governo Da Paraíba' (2022), https://paraiba.pb.gov.br/noticias/joao-azevedo-inaugura-centro-integrado-de-comando-e-controle-e-sertao-ganha-equipamento-referencia-para-a-seguranca-publica-do-nordeste; Portal Correio, 'Recon hecimento facial pemite a prisão de 25 procurados da Justiça no São João de Campina Grande' (11 July 2022), https://portalcorreio.com.br/reconhecimento-facial-pemite-a-prisao-de-25-procurados-da-justica-no-sao-joao-de-campina-grande/. It is not clear whether the 1,600 cameras in use in 2022 are a continuation of the 2019 implementation of Facewatch, since public announcements found on the state government's website merely mention the use of 'facial recognition', without specifying contractors and technology used.

[9] Portal de Amazônia, 'Itacoatiara Terá Centro Integrado de Câmeras Com Reconhecimento Facial e de Placas de Veículos' (6 April 2021), https://deamazonia.com.br/?q=278-conteudo-196736-itacoatiara-tera-centro-integrado-de-cameras-com-reconhecimento-facial-e-de-placas-de-veiculos.

[10] Pablo Nunes, 'Novas Ferramentas, Velhas Práticas: Reconhecimento Facial e Policiamento No Brasil' in Rede de Observatórios da Segurança & CESeC (eds.), *Retratos da Violência: Cinco meses de monitoramento, análises e descobertas* (Rede de Observatórios da Segurança/CESeC, 2019), pp. 67–70.

[11] Ibid., p. 69.

[12] Ibid., p. 68.

[13] Pablo Nunes, Mariah Rafaela Silva, and Samuel R. de Oliveira, 'Um Rio de câmeras com olhos seletivos: Uso do reconhecimento facial pela polícia fluminense' (2022), O Panoptico, https://opanoptico.com.br/Caso/um-rio-de-cameras-com-olhos-seletivos-uso-do-reconhecimento-facial-pela-policia-fluminense/.

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

the major telecommunications operators in Brazil. Firstly, thirty-four FRT-enabled cameras were installed in Copacabana during a ten-day period, and coordinated by four military policemen trained by Oi and Huawei.[14] This programme was extended for two more months in the same year in additional locations in the city, increasing the number of cameras to ninety-five.

The database against which matches were checked was fed by information from the state's Civil Police Office (Sepol), the Department of Motor Vehicles (Detran), and the missing and wanted persons database. SEPM indicated that the data was encrypted, and information regarding persons identified via facial recognition was stored and made available to public security organs and criminal justice for purposes of planning, investigation, and enforcement, while false positives were immediately discarded by the system operator at the monitoring site.[15]

During the first phase, 2,993,692 facial images were captured, with 2,465 face correlations being established between those and the database records. This amounts to a 0.082 per cent match rate. There are no specific numbers for the second phase alone, but in total, from March to October 2019, sixty-three people were arrested, two missing persons were located, and five vehicles were recovered thanks to the use of FRT.[16]

Another study by Instituto Igarapé identifies forty-seven use cases of FRT in Brazilian cities from 2011 to 2019, spanning sixteen states out of the twenty-seven federal units composing the Brazilian federation.[17] Most instances (twenty-one) were related to public transportation – fraud prevention in free passes. These were followed by public security (thirteen cases), education (five cases), and border control (four cases).[18] Critically, the researchers report that 'many of the publicly announced cases focus mainly on the expected efficiency and implementation and less so on informing results'.[19] This is a perception shared by Nunes and colleagues when analysing the aforementioned case of Rio de Janeiro, pointing to a lack of metrics enabling performance reviews and stressing several instances where clarifications are needed to evaluate the projects' objectives and results.

Traditionally, Brazilian municipalities have adopted poor data governance practices, with sensitivity to personal data protection only kicking in after the applicability of sanctions in the General Data Protection Law (LGPD) in August 2021.[20] From

[14] Although Oi was the contracting party, the technology utilised was developed and provided by Huawei.

[15] Nunes, Silva, and Oliveira, 'Um Rio de cameras', p. 11.

[16] Instituto Igarapé, 'Videomonitoramento Webreport' (2020), https://igarape.org.br/videomonitoramento-webreport/; Nunes, Silva, and de Oliveira, 'Um Rio de cameras'.

[17] Instituto Igarapé, 'Reconhecimento facial no Brasil'.

[18] Ibid.

[19] Ibid.

[20] Luca Belli and Danilo Doneda, 'Municipal data governance: An analysis of Brazilian and European practices/Governança de Dados Municipal: Uma Análise Das Práticas Brasileiras e Européias' (2020) 12 *Revista de Direito da Cidade* 1588. For a non-official translation of the LGPD,

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

this perspective, a central concern regarding FRT use is the possible re-purposing of the personal data that has been collected, notably the sharing of such information with the government. For instance, in the case of FRT usage to prevent abuse of gratuity programmes in public transportation, it was revealed that the processed data may also be shared with the security forces 'when requested'.[21] Similar concerns apply when FRT is used to monitor student attendance, such as a case in the municipality of Itumbiara, in the state of Goiás. Questioned by researchers, the municipal education office made assurances that the data were stored in the same device it was captured on and a prior Data Protection Impact Assessment had been done, although the assessment was not shared publicly or with the researchers.[22]

Despite existing assurances from public bodies responsible for FRT implementation, the risk of surveillance creep remains significant – not only involving a possible transferring of biometric data to third parties, but also the receiving of such data from third parties. In July 2021, for instance, the governor of Bahia announced the expansion of a FRT project from Feira de Santana to seventy-six other cities in the state, for a total of 4,095 cameras, on a R$ 665 million partnership with a conglomerate formed by Oi and the security tech company Avantia. In making the announcement, the governor also revealed an ambition to have private security cameras connected to the system, allowing for 'banking agencies, shopping malls and condominiums […] to connect their cameras and deliver the movements and faces of passers-by to authorities'.[23]

16.3 CURRENT LEGISLATION, REGULATION, AND GOVERNANCE

There is currently no specific law regarding FRTs in Brazil, whether for public or private ends, and whether in security, transportation, or any other area. Furthermore, there is no specific law or regulation framing the usage of AI systems in Brazil, although legislative efforts are being made. There is, however, a set of laws that regulate specific areas of FRT and can be used to build the basis for a regulatory framework; they are briefly explained in this section.

see Luca Belli, Laila Lorenzon, Luã Fergus and Walter B. Gaspar, 'The Brazilian General Data Protection Law (LGPD) – Unofficial English version' (22 January 2020), CyberBRICS, https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/.

[21] Leonardo Zvarick, 'Reconhecimento Facial Bloqueia 331 Mil Bilhetes Únicos Em SP – 12/06/2019' (12 June 2019), São Paulo Agora, https://agora.folha.uol.com.br/sao-paulo/2019/06/reconhecimento-facial-bloqueia-331-mil-bilhetes-unicos-em-sp.shtml.

[22] Bárbara Simão, Blenda Santos, Carolina Reis, Eduarda Costa, Elora Fernandes, Enrico Roberto, Felipe Rocha and Rafaela de Alcântara, 'Cidades Inteligentes e Dados Pessoais: Recomendações e boas práticas' (2022), Internet Lab, ARTICLE 19, LAPIN, p. 47.

[23] Cíntia Falcão, 'A Bahia está virando um laboratório de reconhecimento facial' (2021), *The Intercept Brasil*, https://theintercept.com/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/.

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

16.3.1 *General Data Protection Law (LGPD)*

A first important port of call is the LGPD. Four key elements for FRT purposes are:

(1) its characterisation of biometric data, such as facial images, as 'sensitive personal data' (Art. 5°, II), which means that its processing can be grounded only on a more limited range of legal bases (Art. 11°);
(2) the overarching principles of data processing, which set the fundamental elements of all personal data processing, including those involved in FRT (Art. 6°);
(3) the right to revision regarding automated decision-making based on personal data that affect the data subject's interests (Art. 20 and Art. 20.§1); and
(4) the limited scope of the LGPD when it comes to security, prevention, and repression of criminal activities, and the obligation to perform data protection impact assessment in such cases (Art. 4.§3.).

The first point refers to the fact that, being categorised as sensitive, the codified data of every individual's facial print, used in face recognition to identify matches, must be based on explicit and informed consent of the data subject or else be 'indispensable' to achieve one of seven legal bases as set in Article 11. One can imagine some of these alternative legal bases being in principle suitable to justify FRT for public interest purposes. For instance, 'prevention of fraud' can justify one-to-one authentication of an individual who needs to access a secure electronic system (an example being biometric authentication for one's own bank account). Moreover, 'compliance with legal or regulatory obligations' allows data controllers to conduct FRT operations when this is imposed as a legal or regulatory obligation; and 'execution of public policies' allows the shared use of information between public entities or between public and private entities, upon prior authorisation, for the execution by the public administration of public policies.

This latter provision is a peculiarity of the Brazilian framework, allowing the sharing of datasets between government departments, executive agencies, and private entities who have been involved in the execution of public policies. However, this can only be done under terms and conditions that have been previously defined in legislation or equivalent legal sources (ordinances, resolutions, regulations, etc.), which provide a mechanism to ensure transparency and accountability of such processing.

The third relevant aspect of the LGPD concerns its principles, which construct concrete obligations for the data controllers and processors. Good faith (duty to maintain an honest and trustworthy conduct in the data processing relationship) opens the set of principles contained in Article 6 of the law,[24] followed by principles similar to those found in other data protection frameworks – for example, purpose

[24] Good faith (*boa fé*) is divided in Brazilian legal doctrine into subjective and objective manifestations. In the case of its use in Art. 6 of LGPD, as well as in Art. 422 of the Brazilian Civil Code, it is meant in its objective form, that is, a duty to behave according to the legitimate expectations of one another in a legal relationship. Bioni (2019) comments on this point connecting the objective good faith

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

limitation, data minimisation, security. Of particular interest for FRT are the principles of non-discrimination and responsibility and accountability, in conjunction with the transparency principle. Since LGPD principles must inform and shape the whole design and implementation of data processing, this means that controllers must be able to demonstrate that specific measures have been taken to mitigate risks, such as biased and unfair processing, and have been communicated in a clear and intelligible manner.

Owing to the invasive nature of FRT, the correct implementation of the LGPD principles requires the performance of periodic data protection impact assessments. This is particularly relevant when FRT is deployed for security purposes by public organs and law enforcement agencies, as only auditable technologies can be legitimately used by the state bodies without undermining constitutional guarantees. Unfortunately, this is far from being the case. Furthermore, a sound implementation of the transparency principle is key in the case of FRT. This not only demands an analysis and audit of FRT's impact, but also requires that the information resulting from such analysis be transparently communicated in an accessible language.

The second key element of the LGPD that is relevant for FRT concerns automated decision-making. According to LGPD, these decisions should be structured in a way that allows for revision,[25] which, logically, also demands that the data subject be informed they are subjected to automated decision-making.[26] A hard question would be what form of communication of that information is suitable for giving notice: would this require a 'just-in-time' notification, or would consent to a generic statement in a controller's privacy policy be sufficient?

Lastly, it is important to mention that the LGPD creates a rather large exception within the data protection framework regarding any data protection processing aimed exclusively at fostering public security, national defence, the safety of the country, or crime investigation and repression (Art. 4). While this exception currently leaves the door open to a wide range of illegitimate uses from state organs, the LGPD also foresees that these exceptions 'shall be governed by a specific law, which shall contain proportional measures as strictly required to serve the public interest, subject to due process of law, general principles of protection and the rights of the data subjects set forth in this Law' (Art. 4 §1). Furthermore, paragraph 3 of the same LGPD article also provides a key element for the purposes of FRT regulation, specifying that the ANPD will issue technical opinions or recommendations regulating the exceptions

contained in LGPD to the concept of contextual privacy, based on the trust between parties in a data processing relationship that the information shared will not be used in manners that contradict the original context of its sharing. See B. R. Bioni, 'Proteção de dados pessoais : a função e os limites do consentimento' (Forense, 2019), http://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/5973.

[25] Not necessarily human revision, although one could argue an automated revision of automated decisions constitutes another instance of possible 'revision' under the law.

[26] This is an accessory obligation – since one cannot assert one's right if one is unaware of the fact that there is a situation that gives rise to that right. It can also be derived from the general transparency principle.

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

mentioned earlier and shall request a data protection impact assessment to the persons in charge of data processing for such purposes. Hence, we may assume that whenever FRT is used for safety and security reasons it is necessary to undertake a data protection impact assessment. Moreover, the ANPD has general competence to regulate how data protection impact assessments should be conducted (Art. 55-J, XIII).

16.3.2 *Additional Legislation*

In addition to LGPD, some other normative references are relevant to FRT. First of all, the Brazilian Constitution contains provisions on intimacy (Art. 5, X), secrecy of communications (Art. 5, XII), habeas data (Art. 5, LXXII), and personal data protection (Art. 5, LXXIX).

Secondly, the Brazilian Consumer Code applies to business-to-consumer relations, potentially impacting the viability of FRT deployments in consumer-facing applications, products, and services. For instance, it contains provisions on databases, anticipating many of the rights that would be afforded to data subjects by the LGPD in general (the Code precedes LGPD by more than two decades). Importantly, it establishes strict liability in consumer relations (Art. 12 and Art. 14); an obligation to maintain correct and updated data; and the right of the consumer to be informed of a new registry of their personal data (Art. 43).

Another relevant provision is Federal Decree no. 10.046/2019, which establishes guidelines for the sharing of data among the Federal Public Administration. This norm allowed the unification of fifty-one existing databases and created two new ones (including biometric and biographic data), and was criticised for laying out insufficient safeguards of compliance with the LGPD.[27] Two actions challenging the constitutionality of the Decree were filed before the Constitutional Court in 2021, due to its alleged clash with fundamental rights to privacy and data protection. In a unanimous decision, the court interpreted the Decree in conformity with the Constitution, clarifying data sharing must be conditioned to:

(1) the pursuit of legitimate, specific, and explicit purposes;
(2) the compatibility with the stated purposes;
(3) compliance with the LGPD's public sector norms;
(4) its transparency and publicity, including the control mechanisms for access to the database, insertion of new data, and the security measures enabling the imposition of liability on the relevant public servant in case of abuse;
(5) its respect for the norms established in specific legislation and case-law in the operations of data sharing and intelligence;

[27] Estela Aranha, 'Elaboração de parecer sobre a legalidade dos Decretos nº 10.046/2019 e 10.047/2019 em face das normas que disciplinam os direitos fundamentais à proteção de dados e à privacidade no ordenamento jurídico brasileiro' (12 February 2020), OABRJ, www.oabrj.org.br/noticias/comissao-protecao-dados-privacidade-lanca-parecer-sobre-decretos-federais-criam-grande.

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

(6) the existence of norms of civil responsibility of the state in case of illegality; and
(7) the existence of norms of responsibility for administrative impropriety of any agent acting on behalf of the state in case of intentional violation of the duty of publicity established by Article 23 of the LGPD.[28]

At the same time, the ruling found unconstitutional the part of the Decree concerning the composition of the Central Committee for Data Governance (the entity that may formulate the concrete norms and standards for data sharing under the Decree). The court gave the government sixty days to open its composition to effective participation of other democratic institutions, with minimum guarantees against undue influence on its members. In other words, the ruling consecrated the importance of both transparency and multi-stakeholder participation in the formulation of policies regarding government use of data.

Finally, Ordinance no. 793/2019 of the Ministry of Justice and Public Security is directly concerned with the use of FRT for public security purposes. This norm establishes financial incentives for security-oriented actions aimed at implementing the National Public Security and Social Defence Policy. FRT is explicitly mentioned in Article 4, §1, III, b,[29] which allows the application of funds from the National Public Security Fund (which reached more than 1 billion reais in 2021 and almost 2 billion reais in 2022) in the implementation of technologies such as video monitoring systems with facial recognition solutions, optical character recognition, and AI.[30] Although the intent to increase such applications is expressed, no safeguards in terms of transparency and accountability are described.

16.4 DISCUSSION: IS THE EXISTING FRAMEWORK ADEQUATE?

To assess if the existing (or proposed) legal framework regarding AI and FRT in Brazil is adequate for the protection of fundamental rights, it is first necessary to understand the risks associated with the application of these technologies. A brief discussion of these risks is presented here. Based on such an understanding, we then draw some necessary conclusions.

16.4.1 *The Probable Risks of FRT Deployment in Brazil*

One of the most cited and known risks is the discriminatory consequences that these technologies may have. Particularly, systems trained based on discriminatory

[28] Gilmar Mendes, Voto Conjunto ADI 6649 e ADPF 695.

[29] Portaria no. 793/19, de 24 outubro de 2019, Imprensa Nacional de 25 outubro (Brazil), www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575).

[30] Portal da Transparência, 'Fundo Nacional de Segurança Pública' (n.d.), www.portaltransparencia.gov.br/orgaos/30911?ano=2022.

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

datasets will likely tend to reproduce the biases and discriminatory tendencies inferred from the data. Systems developed by under-representative teams may suffer from more subtle dysfunctionalities – resulting from issues such as limited selection criteria set by developers, the conceptualisation of the elements that will constitute inputs and outputs of the system, and a myopic view of the results in terms of their discriminatory impacts. Poorly designed systems and datasets might result in systems that disproportionately target these populations, and consequently, new disproportionate data being generated and fed into the system.

Possa highlights how, in a country where black individuals made up 66.7 per cent of the national prisoner population in 2019 and where in 2015 the Supreme Court declared the general state of the carceral system as an 'unconstitutional situation', adopting public security technologies that harm the presumption of innocence and present biases toward structurally discriminated peoples only reinforces that unconstitutionality.[31]

All these issues result in systems that are inept at dealing with certain aspects of the social phenomena they are built to address – in the case of FRT, systems are unable to recognise non-Caucasian, non-male faces, resulting in undue targeting of these groups, as many studies and cases have previously shown.[32] This seems also to be the case with some of the previously discussed implementations of FRT in Brazil, as anecdotal evidence suggests.[33]

Those problems are compounded by AI systems' opacity, which impairs accountability and public oversight.[34] This is further complicated by the information asymmetry between private actors who source these technologies and the public using them, or the public institutions that contract AI services. As stated by Mazzucato

[31] Alisson Possa, 'O reconhecimento facial como instrumento de reforço do estado de coisas inconstitucionais no Brasil' (2021) 1 *IDP Law Review* 134.

[32] João Victor Archegas and Christian Perrone, 'Don't snoop on me' (16 December 2021), Verfassungsblog: On Matters Constitutional, https://intr2dok.vifa-recht.de/receive/mir_mods_00011576; Moriah Daugherty, Katie Evans, Edward J. George, Sabrina McCubbin, Harrison Rudolph, Ilana Ullman, Sara Ainsworth, David Houck, Megan Iorio, Matthew Kahn, Eric Olson, Jaime Petenko and Kelly Singleton, 'The perpetual line-up: Unregulated police face recognition in America' (18 October 2016), Georgetown Law Center on Privacy and Technology, www.perpetuallineup.org; Karen Hao and Jonathan Stray, 'Can you make AI fairer than a judge? Play our courtroom algorithm game' (17 October 2019), *MIT Technology Review*, www.technologyreview.com/2019/10/17/75285/ai-fairer-than-judge-criminal-risk-assessment-algorithm/; Will Douglas Heaven, 'Predictive policing algorithms are racist. They need to be dismantled' (17 July 2020), *MIT Technology Review*, www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/; Jennifer Lynch, 'Face off: Law enforcement use of face recognition technology' (May 2019), Electronic Frontier Foundation, www.eff.org/files/2019/05/28/face-off-report.pdf

[33] Carolina Reis, Eduarda Costa Almeida, Fernando Fellows Dourado and Felipe Rocha da Silva, 'Vigilância automatizada: uso de reconhecimento facial pela Administração Pública no Brasil' (7 July 2021), LAPIN, p. 51, https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/. Nunes, 'Novas Ferramentas'.

[34] Frank Pasquale, 'Secret algorithms threaten the rule of law' (1 June 2017), *MIT Technology Review*, www.technologyreview.com/2017/06/01/151447/secret-algorithms-threaten-the-rule-of-law/.

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

and colleagues: 'The proprietary nature of most AI applications means the public lacks insight as well as the ability to design proper oversight. Advancing technical capabilities without matching adjustments to governance, institutional and organisational models is leading to failure in effectively evaluating the risks of AI and managing its opportunities.'[35]

On top of all this, there are issues particular to the Brazilian context. As systematically demonstrated by Reis and others, and reflected in anecdotal evidence from various other authors previously referenced, most of the FRT being implemented by the Public Administration in the country come from foreign sources, especially China, Israel, the United States, and the United Kingdom. In many instances, contracting was based on aggressive negotiation tactics directed at conquering market dominance and locking-in the contracting administrations.[36] This trend is particularly marked in Latin American countries.[37]

This raises concerns around the strategic value of technologies and the underlying personal data being collected – especially considering that data sharing terms with these private companies are not always publicly transparent.[38] One other concern is the ability of the state to incentivise the emergence of national AI and FRT capabilities, directing their development into interests aligned with national societal goals or 'missions',[39] and strengthening the national innovation system.[40]

Much has been said in public debate about the harms of algorithmic bias and the need to combat or fix it. Powles and Nissenbaum comment on how focussing on solving bias is a reflection of society's deference to technologists even in the fields of ethics, law, and the media, and how focus should not be shifted from discussions such as which systems really deserve to be built; which problems most need to be tackled; who is best placed to build them, and who decides?[41] Souza and Zanatta

[35] Mariana Mazzucato, Marietje Schaake, Seb Krier and Josh Entsminger, 'Governing artificial intelligence in the public interest' (28 July 2022), UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2022–12), www.ucl.ac.uk/bartlett/public-purpose/wp2022-12.

[36] Reis et al., 'Vigilância automatizada'.

[37] Gaspar Pisanu and Verónica Arroyo, 'Surveillance tech in Latin America: Made abroad, deployed at home' (9 August 2021), Access Now, www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home/.

[38] Nunes, Silva, and de Oliveira, 'Um Rio de câmeras'; Reis et al., 'Vigilância automatizada'; Reia and Belli, 'Smart cities no Brasil'.

[39] Mazzucato et al., 'Governing artificial intelligence'; Mariana Mazzucato and Josh Ryan-Collins, 'Putting value creation back into "public value": From market-fixing to market-shaping' (2022)25(4) *Journal of Economic Policy Reform* 345–360.

[40] Glauco Arbix, Mario Sergio Salerno, Guilherme Amaral, and Leonardo Melo Lins, 'Avanços, equívocos e instabilidade das políticas de inovação no Brasil' (2017) 36 *Novos estudos CEBRAP* 9; Chris Freeman, 'The economics of technical change' (1994) 18 *Cambridge Journal of Economics* 463; Chris Freeman, 'The "national system of innovation" in historical perspective' (1995) 19 *Cambridge Journal of Economics* 5.

[41] Julia Powles and Helen Nissenbaum, 'The seductive diversion of "solving" bias in artificial intelligence' (7 December 2018), *OneZero*, https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53.

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

add to this debate,[42] connecting the application of FRT to a broader neo-liberal tendency for the decentralisation of state functions to technology firms, and the associated push from the market in the context of 'surveillance capitalism'.[43] This 'techno-solutionism' serves as a smokescreen over the deeper-seated issues of structural racism and the surveillance state,[44] forcing public debate into the question of *how* to make FRT fair and efficient instead of *if* it is truly needed and proportional to the desired ends. An adequate regulatory framework should deal with these issues.

16.4.2 *Moving from the Existing to the Ideal FRT Framework for Brazil*

Based on the analysis conducted in the previous sections, we can argue that the current and proposed framework for FRT regulation adopts a rather lenient approach to the ex-ante regulation of risk – by leaving a measure of discretion to the control of high-risk applications by the public administration. Such choice may be detrimental in terms of compliance with the LGPD principles, especially considering the ANPD has demonstrated a remarkably timid stance regarding overseeing the implementation of LGPD by public bodies and law enforcement agencies – *de facto* leaving the correct implementation of the existing framework to the good faith and good will of the bodies that deploy FRT.

Moreover, the existing framework does not foresee a differentiated approach that customises specific obligations and safeguards based on the purposes for which FRT is implemented. As we have emphasised, the purpose for which FRT is deployed – for instance identification in the context of crime prosecution versus authentication – has a considerable impact not only on the legislation that will be applied, but also on the obligations of the data controller and the guarantees of the data subject. The complexity of this situation might be exacerbated further by the jurisdictional uncertainty over what administrative level is competent to regulate the use of FRT. Indeed, the regulation of security issues is a state issue, but data protection is an issue of exclusively federal competence.

In addition, we argue that more information needs to be pro-actively made available by public administrators and public service concessionaires on the intended FRT implementations, adopting an accountability-first stance and a transparency-by-design approach. As we have emphasised, information should be communicated in a clear and intelligible manner and should at least specify: when, where, and why FRT is used; what databases are used to train the FRT systems; what data is collected; what measures are taken to guarantee information security; with which

[42] M. Souza and R. Zanatta, 'The problem of automated facial recognition technologies in Brazil: Social countermovements and the new frontiers of fundamental rights' (2021) 1 *Latin American Human Rights Studies*, https://revistas.ufg.br/lahrs/article/view/69423.

[43] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Kindle) (Profile Books, 2019).

[44] Evgeny Morozov, *Big Tech: A Ascensão Dos Dados e a Morte Da Política* (Ubu Editora, 2019).

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

entities data are shared, if any; and what indicators will allow to evaluate the performance of the FRT deployment, such as how many investigations and criminal proceedings are carried out and how many crimes are solved based on the use of the FRT system under discussion.

Lastly, it seems necessary that the ANPD enact regulations and publish technical guidelines on specific aspects of the data processing pipeline, which are essential to make sure FRT systems are used in compliance with LGPD. In fact, as long as critical elements such as data anonymisation, algorithmic accountability and auditing, data protection impact assessments, and data security measures remain undefined, (FRT) compliance with LGPD will continue to be extraordinarily challenging.

In Brazil, the main legal reference concerning the use of FRT, owing to their intrinsic use of personal data, is the LGPD, which is enforced and detailed by the ANPD. There are, however, other concerned institutions that should be included in the discussion. One such is the Governance Committee of the Brazilian Artificial Intelligence Strategy, a multi-stakeholder body created in April 2021 and tasked with translating the strategy – which has been criticised for being overly general and more akin to a letter of intent than to an actual strategy – into concrete objectives and actions.[45] ANPD, however, only started participating in the Committee at its fourth meeting, in December 2021, and no specific progress on these matters has yet been announced.[46]

16.5 CONCLUSIONS

All in all, there are still substantial gaps in the regulation of AI and, consequently, FRT in Brazil, although a strong basis of principles is in place and there are important laws working to provide the necessary basis for the judicial protection of fundamental rights – as demonstrated by the Via Quatro case. A deeper issue with the implementation of these technologies is its scattered character – popping up in news announcements as sure techno-solutions to issues such as efficiency and public security. As discussed, this scattered nature is equally observed in the legislative

[45] Walter Gaspar and Yasmin Curzi de Mendonca, 'Artificial intelligence in Brazil still lacks a strategy' (2021), Report by the Center for Technology and Society at FGV Law School, https://cyberbrics.info/wp-content/uploads/2021/05/EBIA-en-2.pdf; Ronaldo Lemos, 'Estratégia de IA Brasileira é Patética' (2021), Folha de São Paulo, www1.folha.uol.com.br/colunas/ronaldolemos/2021/04/estrategia-de-ia-brasileira-e-patetica.shtml; Eduardo Magrani, 'Estratégia Brasileira de Inteligência Artificial: Comentários Sobre a Portaria 4.617/2021 Do MCTI' (2021), https://secureservercdn.net/192.169.220.85/dxc.177.myftpupload.com/wp-content/uploads/2021/12/OPINION-Brasil-PORT-.pdf?time=1643260747; Francisco Saboya, 'Existe Mesmo Uma Estratégia Brasileira de Inteligência Artificial?' (13 April 2021), *Canal MyNews*, https://canalmynews.com.br/francisco-saboya/existe-mesmo-uma-estrategia-brasileira-de-inteligencia-artificial/.

[46] MCTI, 'Inteligência Artificial Estratégia – Repositório. Ministério Da Ciência, Tecnologia e Inovações – Gov.Br' (n.d.), www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial-estrategia-repositorio.

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press

scenario, with federal, state, and municipal norms and proposed bills creating a cacophony that ultimately impairs advancement of a strong position on the role that these technologies should play in society.

In this context, one major institution that might play an important role is the ANPD, which was given ample ground to not only control, but also guide data processing activities in Brazil. ANPD must embrace its role as a technical agency aimed at providing market and public implementations of innovative data-based technologies with the guidelines necessary to build technological solutions that respect fundamental rights and the means to innovate within those limitations.

Another institutional actor that could play a bigger role in the future is the Governance Committee created to implement the National Artificial Intelligence Strategy. This multi-stakeholder body is seated within the Ministry for Science, Technology, and Innovation, a crucial actor in promoting the full enjoyment of the benefits that may arise from science and innovation, especially in promoting economic and social development. However, this must be guided by a strategic vision that recognises the position that Brazil occupies in the process of recovering its industrial basis and catching-up with advanced economies.

Overall, the debate on FRT in Brazil has been marked by two movements that appear contrary to each other. On the one hand, reliance on FRT as a solution to immediate issues brings about hastened implementations that do not provide the necessary degree of transparency, accountability, proportionality analysis, and sensitivity to the fundamental rights to privacy and data protection. On the other hand, as mentioned in the opening of Section 16.2, civil society has reacted with increasing degrees of rejection of these technologies, reaching a generalised sentiment for the ban of FRT in the surveillance of public spaces. In the midst of these movements, existing and proposed norms seem to tackle some of the problematic aspects of FRT use, but fall short of giving a systematic and unified answer.

https://doi.org/10.1017/9781009321211.019 Published online by Cambridge University Press