Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces

Thiago Guimarães Moraes¹ · Eduarda Costa Almeida¹ · José Renato Laranjeira de Pereira¹

Received: 27 July 2020 / Accepted: 10 September 2020 / Published online: 10 October 2020
© Springer Nature Switzerland AG 2020

Abstract

This article analyses the use of facial recognition technology (FRT) in (semi-)public spaces with a focus in the Brazilian context. Therefore, the operation of the FRT processing chain is addressed, as well as the juridical nature of the facial signature, focusing mainly in the Brazilian data protection framework. FRT has been used in everyday life for several purposes, such as security, digital ranking, targeted marketing and health protection. However, the indiscriminate use of FRT poses high risks to privacy and data protection. In this perspective, to avoid harms such as inaccuracy, normalisation of cyber-surveillance and lack of transparency, safeguards were identified to guarantee individual rights, such as soft law, oversight, international standards and regulatory sandboxes.

Keywords Facial recognition · Surveillance · Data protection · Safeguard · Sandbox

1 Introduction

Initially restricted to physical access control systems in chemical/radioactive laboratories, facial recognition technology (FRT) is being increasingly applied to identify individuals on *web* pages, photos, video recordings and in physical spaces. This has raised concern about the right to privacy of individuals being identified: who is surveilling? In what context? For which purposes? These questions are even more sensitive when facial recognition is used in (semi-)public spaces indiscriminately, without the establishment of a proper criteria to filter which personal data will be collected, and from whom.

Semi-public spaces are characterized by being freely accessible and having few usage restrictions. According to Peterson, these are places which, although belonging to private entities, are freely used in a shared way by different social groups [1]. Examples are shopping centres,

supermarkets and libraries. Their protection should take account of private security regulations, while *stricto sensu* public spaces are protected by the legitimate interest of public security.¹

Around the world, several cases involving the deployment of facial recognition systems have come to the attention of digital rights organizations and the general public. In the UK, the London Metropolitan Police—MET used two facial recognition cameras in one of the most crowded sites in London, the *King's Cross Central* [2]. The experiment lasted months, and the authorities had no concern to establish transparency and information mechanisms to passersby who had their data collected.

In the Brazilian context, facial recognition has already been used in carnival blocks in Rio de Janeiro and Salvador [3] and in a “smart/safe city” project in Campinas [4]. In June 2019, the Metropolitan Company of São Paulo opened a procurement for the implementation of FRT in three metro lines [5].

So far, the main purpose for the deployment of such technology in Brazil has been security [4], as facial recognition helps in the identification of individuals who have committed crimes or are about to commit it. Security is also a concern for shopping centres, supermarkets and other spaces, as

¹ In this article, we use the sentence “(semi-)public” to represent the two types of spaces, one of public nature and other of a private nature. Where it is necessary to distinguish between them, we use the term *sensu stricto* to identify the former.

✉ Eduarda Costa Almeida
eduarda@lapin.org.br

Thiago Guimarães Moraes
thiago@lapin.org.br

José Renato Laranjeira de Pereira
joser Renato@lapin.org.br

¹ Public Policy Division, LAPIN - Laboratory of Public Policy and Internet, Brasília, DF, Brazil

Fig. 1 Facial recognition steps
(Source: EFF, adapted)

they have an interest in protecting consumers and their own property [6]. However, we could question what is the great contribution of facial recognition for this purpose: would it not be sufficient to use traditional surveillance cameras, which have a much smaller impact in people's privacy and rely less on the autonomy for making decisions of these systems? Another concern is how these companies may be using the data processed for further purposes, such as the profiling of users to offer customized marketing services [7].

The use of facial recognition when applied for generic or obscure purposes is in direct contrast with the principles provided by the Brazilian data protection legislation, Law 13.709/2018, *Lei Geral de Proteção de Dados*—LGPD.² In the next sections, this work will investigate which risks involve the use of facial recognition in public spaces, and which technical and legal measures could be implemented to ensure the protection of individuals' personal data and privacy in Brazil. The focus will be on examples of the use of FRT for identification purposes, in opposition to facial detection applications of FRT where there is no identification, but solely categorization, such as the case of digital signages [8]. At some points, comparisons will be made with the European data protection framework, from which the Brazilian LGPD is heavily inspired. In particular, the European General Data Protection Regulation—GDPR and the Law Enforcement Directive are mentioned.

2 Facial recognition technologies and their use in (semi-)public spaces

To understand the privacy implications of facial recognition systems, we highlight some technical features to understand the *modus operandi* of this technology. We then discuss the different identification purposes of their use in public spaces, both by the State and by private parties.

2.1 Facial recognition processing chain

Facial recognition systems use computational algorithms (usually machine learning models) to select unique identifying details of a person's face. The first step is capturing the face from a photo or a video. More advanced technologies allow recognising faces in the crowd or even from someone's silhouette [7].

The second step is the reading of the face geometry by the facial recognition software. The main factors include the distance between the eyes and the distance from the forehead to the chin. The result is known as the 'individual signature' [9]. This signature, which is no more than a mathematical formula, is then compared to known faces in a database. Based on the similarity of the model captured and the data found, a match between the image captured by the surveillance camera and a given image in the faces database may be made. For better understanding, see Fig. 1.

In this sense, the following data processing operations can be highlighted in facial recognition systems [10]:

² For an English version of the LGPD, refer to https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.

- (a) acquisition of images (collection): process of capturing the face of an individual and converting into a digital image;
- (b) face detection: process for detecting the presence of a face in a digital image and marking the area;
- (c) normalisation: process to smooth variations in detected facial regions, such as converting image into a standard size or even rotating or aligning the colour distributions;
- (d) attribute extraction (features): process to isolate and produce repeatable readings, distinct from an individual's digital image. The set of attributes is defined as a template for comparisons with the face database—the facial signature;
- (e) storage: if this is the first time the face of the individual is captured, the image and/or reference model can be stored as a record for future comparisons;
- (f) comparison: the process of measuring the similarity between the sample and another model previously included in the system. This comparison can be made for (1) identification, (2) authentication/verification and/or (3) categorization.

Regardless of the intended purpose, the processing steps followed by this type of technology are almost the same. As will be seen below, the use of FRTs for different purposes will require different safeguards for protecting individuals' rights. However, before discussing this topic, it is necessary to understand what is the nature of the facial signature data under the Brazilian and European data protection frameworks.

2.2 Legal nature of the facial signature data

Data processed by facial recognition systems should be recognised as personal data, as they allow us to extract information related to the identified or identifiable natural person.³ However, it is appropriate to consider whether such personal data should be considered sensitive.

According to the Article 29 Working Party, biometric data can be defined as 'unique and measurable biological properties even if the patterns used in practice to measure them technically involve a certain degree of probability' [11]. By its turn, Article 5, II, of the LGPD defines that where linked to a natural person, biometric data falls within the concept of sensitive data.

Facial recognition thus constitutes a biometric technique, as the biological characteristics observed for generating the facial signature, which is biometric data, contain sufficient details to allow for the unique identification of an individual

[10]. As long as this facial signature is used for identification purposes, processing of data by FRTs should be considered sensitive data. Their processing should thus fulfil one of the legal basis for sensitive data provided by Article 11 of the LGPD, which are much more restrictive than those of Article 7, which relates to "general" personal data. In the European context, a similar conclusion can be made, where FRT used for identification will fall under Article 9 of the GDPR [8].

As a counterpoint, it is important to understand that not every camera surveillance system will carry out sensitive data processing. If a video captures several persons but does not identify them uniquely, there is no sensitive data processing, and, therefore, falls under the rules of Article 7 of the LGPD, which is the equivalent of Article 6 of the GDPR [12]. One example of FRT that does not identify natural persons is digital signages, such as billboards that perform advertising based on the main characteristics of a group of passers-by in a given time [12].

Now that the question regarding the legal nature of signature data collected in facial recognition contexts has been stressed, the next session will discuss how identifying the purpose of the processing may be clouded when the difference between the use of FRT by public or private agents is not clear.

2.3 The purposes of using facial recognition in (semi-)public spaces

The analysis of the purposes for processing data collected by FRTs is relevant for identifying the legal basis for its use and the limits imposed by legislation. In this sense, this research analyses the following purposes for using facial recognition technologies in (semi-)public spaces: (1) public security; (2) digital identity; (3) private security; (4) targeted marketing; and (5) health protection, as occurred during the COVID-19 pandemic. In all these cases, we highlight at least one context where FRT is used for identification of the natural person, thus falling under the more restrictive rules of processing of sensitive data. Some of the use cases presented also go beyond what is currently implemented in Brazil, since there is always the risk that surveillance technologies used in one country may be eventually imported to another.

2.3.1 Public security

Article 144 of the Brazilian Constitution defines public security as the State's duty of maintenance of public order, people and patrimony [13]. To achieve this goal, the Brazilian Government has increased the use of cameras and technology tools with the aim of making security more efficient in *stricto sensu* public spaces. However, the use of FRTs

³ LGPD, Art 5, I.

for this purpose has not been effectively regulated in the country yet.

The installation of facial recognition cameras in the Rio de Janeiro's Carnival made it possible to identify and arrest four persons who had been subject to an arrest warrant issued by the police [3]. The captured images of the individuals had been compared and confronted with the existing police database to identify them in real time.

Despite the apparent success of the police operation, the lack of transparency of the deployed facial recognition system motivated the Brazilian Consumer Protection Institute—IDEC, a civil society organisation, to send a letter to the Secretary of the Military Police of Rio de Janeiro asking for clarification. According to IDEC, facial recognition could be a threat to the individual rights of citizens, due to the possibility of substantial data breaches [14]. In addition, the institution signalled that there is room for potential misuse of such data, which could, for example, be shared with other public entities or even private self-interested companies without the knowledge of the data subject [14].

It should be noted that, according to a report prepared by the *Rede de Observatórios de Segurança* (Safety Observatories Network), the use of facial recognition in Brazil for public security purposes reflects the strong racial bias of the country's criminal system: 90.5% of the persons arrested with the use of FRT were black-skinned individuals. These results are even more worrisome as historically, data transparency requirements on public security and crime are not respected in Brazil [15].

Furthermore, the legal basis for regulating the use of FRT for public security purposes is not yet specified in the LGPD, since Article 4 states that it does not apply to data processing for public security.⁴ Therefore, there are no reporting mechanisms to an accountable use of facial recognition, such as where and how these cameras are used and information on the collection and the storage of such data.

2.3.2 Scoring systems and digital identity

Another application for facial recognition technology is the creation of digital identity systems. The Chinese government is developing the 'Social Credit System' for evaluating

citizens according to their behaviour in public through the creation of digital profiles [16]. To obtain information on citizens' habits, the Chinese government uses data collected by facial recognition cameras installed in public spaces, and gives scores for the actions of each individual according to ethical and moral parameters which are deemed the most appropriate by the authorities.

The Social Credit System foresees ways to punish and reward such individuals based on their score. Penalty examples may be banning citizens on travelling, restricting their access to certain public services and even the addressing of moral punishments. Hence, the Chinese government concentrates the power of watching and evaluating people in their most intimate sphere.

A similar example occurs in India, which has a project to create a national identification system with the help of facial recognition [17]. The *Aadhaar*, as called, aims to integrate personal information such as biometric data, residence and work address, photos and other details accessed by means of a single card. Despite the argument that facial recognition technology has been applied for the maintenance of public safety, its use has actually led to a scenario of mass surveillance, mainly of minorities that are contrary to the government. The situation is exacerbated by the imprecise nature of data protection and privacy legislation in India [17].

In Brazil, while there is no evidence that similar initiatives exist, some eyebrows were raised with the creation of a national database, the "Cadastro Base do Cidadão" (CBC), which aims to create an index converging all citizen's data held by the government on a single place. CBC was enacted by Presidential Decree nº 10.046/2019, which also establishes rules for the free flow of data among government agencies. Although the government claims that its sole reason is to bring more efficiency to public administration, it's still unclear what efficiency will mean in practice, since there might be room for its integration with FRT and scoring systems such as the abovementioned, considering that the Decree has specific provisions related to biometric data storage.

2.3.3 Private security

Private security in the Brazilian legal system is regulated by Law No 7.102/73 [18], which provides for the conduct of security officers and is aimed at preserving the integrity of goods, public or private establishments and persons, as well as carrying out the safe transport of values and loads.⁵

⁵ Law 7.102/73, Art. 10. Activities carried out by way of provision of services shall be considered to be private security for the purpose of:

(I) the financial monitoring of financial institutions and other public or private establishments and the security of persons;

(II) carry out the transport of securities or ensure the carriage of any other type of cargo.

⁴ Article 4. This Law does not apply to the processing of personal data:

III—Carried out for the sole purpose of:

(a) public security;
(b) national defence;
(c) State security;

§ 1 The processing of personal data provided for in Item III shall be governed by specific legislation, which shall provide for proportionate and strictly necessary measures to meet the public interest, observed due process, the general principles of protection and the rights of the data subject provided for in this Law.

As the purpose of this paper is to analyse the use of FRTs in (semi-)public spaces, we focus on discussing the use of such systems by private security agents operating both in public establishments where access is not unrestricted and uncontrolled, such as public offices and Courts of Justice, as well as in private spaces where access is almost unrestricted, such as in shopping centres.

As these (semi-)public spaces are kept and accompanied by wardens, the purpose of surveillance is not public, but private security, and therefore the LGPD applies. In those scenarios, the legal person who hires private agents to provide security services performs the function of data controller,⁶ since it defines the security policy of the establishment and is hence the one responsible for establishing the purposes and means of the processing of personal data.

As long as FRTs are applied for private security purposes, the LGPD applies, and, hence, the processing of personal data will only be possible if the legal hypotheses of this law are fulfilled, as described in Article 11. In this sense, the possibilities for dealing with sensitive data are rather limited: if there is no consent of the holder or if any of the cases set out in Article 11, II, applies,⁷ the use of facial recognition for private security shall not be legitimate. The processing of sensitive data also impedes data controllers to rely on the legitimate interest basis (Article 7, IX, of the LGPD), since this legal ground is not existent under Article 11.

In a real-world situation, obtaining the consent of individuals filmed by FRTs is infeasible. As explained by the European Data Protection Supervisor—EDPS, a person who has been filmed cannot choose whether or not to have their

data collected, even less when she needs access to semi-public spaces monitored by facial recognition surveillance [19]. It is, therefore, difficult for the controller to rely on consent, which must be free, informed and unambiguous (Article 5, XII, of the LGPD).

2.3.4 Targeted marketing

Processing of facial recognition data may also serve advertising purposes such as the promotion of targeted marketing or ways of enhancing publicly available advertisements by analysing consumer behaviour and profiling.

In Brazil, services such as those mentioned would be broken down in at least two points of conflict under the LGPD. The first, in a similar manner to the security situation, would be the applicable legal basis. Since legitimate interest is not a criterion for processing sensitive data according to Article 11, LGPD, the controller should necessarily ensure that consent is given in a specific and prominent manner. Unless the customer is able to interact directly with the camera to confirm explicitly that it has an interest in being recognised, consent will not be valid, and very hardly any of the other legal basis will apply to the context.

The second point of tension is brought by Article 20 of the LGPD, which provides for a set of rights to data subjects that are targets of automated decision-making where consumption profiles are created based on their physical and emotional characteristics. There are at least two rights that need to be guaranteed here: (1) the right to obtain clear and appropriate information about the criteria and procedures used for the automated decision and (2) the right to request a review of decisions taken solely on the basis of automated processing affecting their interests.

Recently, Cia Hering, a Brazilian clothes retail company, was sued by the Brazilian Institute for Consumer Defense (IDEC) for applying FRTs to capture consumers' reactions when looking at exposed items, and it was sentenced to pay a R\$ 58.7 thousand fine for the conduct [20]. The conduct of the company has consisted of an indiscriminate collection of sensitive data without the consent of consumers and without demonstrating the purposes of such processing or storage. Such use of cameras for non-informed purposes is known as function creep, and impacts on the rights to privacy, data protection and image rights [21].

2.3.5 Public health protection

Once the FRT infrastructure is installed, the technology can easily be used in different contexts. This was the case at the beginning of 2020, with the health crisis of COVID-19, where some governments started to monitor compliance with quarantines through facial recognition.

⁶ LGPD, Art. 5, VI—Controller: natural or legal person, whether governed by public or private law, to whom decisions relating to the processing of personal data are responsible; (free translation).

⁷ Article 11. Sensitive personal data may only be processed in the following cases: [...]

(II) without the holder's consent, in cases where it is indispensable for:

(a) compliance with legal or regulatory obligations by the controller;
(b) sharing of data necessary for the execution by the public administration of public policies provided for by laws or regulations;
(c) carrying out research by means of searching by means of ensuring, where possible, anonymisation of sensitive personal data;
(d) regular exercise of rights, including contract and judicial, administrative and arbitral proceedings, the latter pursuant to Law No 9.307 of 23 September 1996 (Arbitration Act);
(e) protection of the life or physical age of the holder or of a third party;
(f) health protection, which is carried out exclusively by healthcare professionals, health services or health authorities; or
(g) ensuring the prevention of fraud and the security of the holder, the procedures for identifying and authenticating records in electronic systems, retaining the rights referred to in Article 9 of this Law and except in the case of fundamental rights and freedoms of the data subject which require the protection of personal data. (free translation).

The most alarming case is probably of China, where FRT systems are able to detect people's temperature even in a crowd and identify citizens who are not wearing face masks to send them notifications [22]. However, use is not limited to this country, and reports point out that Russia also used FRT to monitor quarantine compliance in Moscow [23].

Using FRT during a health crisis raises concerns first because it allows for biometric data to be crossed with an individual's health information, aggregating a large amount of sensitive data in one single database. Furthermore, one should ask whether these means are necessary and proportional to combat a health crisis. In this sense, several organizations, such as the OECD [24] and the European Commission [25], have already warned about caution when implementing technologies for massive data collection in epidemic contexts. Among the many issues they have highlighted is the absence of specific guidance on using FRTs for this context, the lack of fully informed and explicit consent, and algorithmic bias.

In the Brazilian case, although the LGPD provides for the legal basis of processing data for health protection (arts. 7, VIII and 11, II, f), its use must be exclusive to health professionals, health services or sanitary authorities. Thus, the purpose of monitoring quarantines would only be compatible with this legal hypothesis in case this control is performed exclusively by the indicated professionals.

3 The risks of use of facial recognition technologies

While facial recognition technologies can foster multiple benefits to society for enhancing marketing operations and increasing efficiency of surveillance systems for public and private security, it is important that operators of such tools are aware of the risks involved in their use. Some of the main risks related to the implementation of FRT are (1) lack of legal basis; (2) inaccuracy; (3) normalisation of cyber-surveillance; and (4) lack of transparency.

3.1 Lack of legal basis

One of the biggest issues of employing a FRT is the lack of a proper legal basis that justifies the use of such an invasive technology. Considering that the first step for processing personal data is verifying which legal basis should apply for a given purpose, we should thus first look at how to frame intended purposes of use of FRTs with their respective legal basis.

Public authorities will usually rely on legal obligations or public interest to justify personal data processing. However, processing for criminal-related purposes such as public security requires specific legislation in Brazil, since the LGPD

is not applicable in the context of this activity. In this sense, enacting legislation about the theme is of utmost importance in the country, as it has been made in the European Union with Directive 2016/680.⁸ Therefore, all the performance tests that have been running on Carnivals and other public security contexts in Brazil have been done without proper safeguards. Nevertheless, it should be noted that Article 4, § 1º, provides that any form of personal data processing, irrespective of its purpose, should respect the data protection principles established by Article 6, LGPD.

With regard to scoring systems and digital identity, at the moment there is also no specific legislation that regulates how FRT could be used in these contexts, and it would probably not fall into any of the LGPD's legal basis. Finally, while the LGPD has a specific legal basis (Article 7, VIII and Article 11, II, f) for allowing personal data processing for healthcare purposes exclusively by health professionals, the law provisions have not been respected during the pandemic since professionals from other areas have also been processing such data.

Regarding private controllers, the common legal basis would be consent or legitimate interest. On the one hand, consent is very unlikely to be fulfilled since it is very difficult (or rather impossible) to make every single person who has been filmed on a semi-public place to freely choose whether or not they allow to have their data collected. For example, in a retail store, it will be very improbable that the FRT will be able to differentiate consumers that have consented to target advertisements from those who have not. On the other hand, if the biometric data are linked to a natural person (what happens very often when using FRT), it will be considered sensitive data, and legitimate interest will not be a valid legal ground.

Furthermore, even if it did not fall under the sensitive data category, a private party would have issues with balancing legitimate interest and the rights and freedom of individuals. For example, in a retail store, a consumer may understand the importance of cameras for private security, but using FRT for further identification clearly exceeds their reasonable expectations [26].

Therefore, the lack of legal basis in Brazil is a concrete risk to FRT used in different contexts, be it by public authorities—such as public security—or private companies, such as private security or targeted marketing, since there is not a robust regulation that dictates how facial recognition should be used. Without proper legal safeguards, the use of FRT may violate fundamental rights and freedoms, rendering the use of the technology illegitimate in these circumstances.

⁸ Further details of this Directive are mentioned in section IV.C.

3.2 Inaccuracy

Another risk that deserves particular attention relates to the accuracy of authentication and identification systems using facial recognition technologies. As such systems are designed in a binary form, mistakes may be reflected in false positives and false negatives.

False positives would occur when a facial template (see Section IIA) is incorrectly related to an image contained in the technology database. In cases involving public security, a target may be erroneously identified as a criminal in the police database. This is what happened in a case whereby a facial recognition system applied by the military police in Rio de Janeiro misidentified a woman as a police fugitive and arrested her for mistake [27]. Conversely, false negatives occur when the system does not link a captured facial template with its corresponding image in a database, thus failing to identify the target [28].

As a match is taken on the basis of a probability (e.g. the system defines a *sample*⁹ as having 95% chance to correspond to a base), it is inevitable that there is a *trade-off* between false positive and false negatives: the higher the match probability, the less false positives will likely exist, while the number of false negatives will increase.

That being said, improvements in the quality of the data collected and in the decision-making systems can ensure a reduction of false negatives for the same fixed positive value (e.g. 1% or 0.1%) [28]. In the context of public security, false positives are much more detrimental to targets (potential victims of discrimination) since they can be mistakenly identified as criminals by the police and consequently be arrested. Therefore, the setting of a reasonable value for this accuracy threshold becomes a matter of public policy.

While accuracy may be an issue in any context, it is particularly sensitive when FRT is used for security and digital identity purposes. First, in a security context, inaccuracy means the possibility of charging someone responsible for an act or crime that the person did not commit. This is even more serious in view of the possibility of punishment, such as imprisonment. In addition, the use of FRT on digital identities can also connect a person with an activity or behaviour that she did not perform, thus creating a digital profile with incorrect information about her.

3.3 Normalisation of cyber-surveillance

Technological monitoring takes place in society not only by public authorities, but also by private corporations and even

by individuals, such as in the case of cyber-watchdogs [27]. This multifaceted phenomenon has led to the development of post-conflict surveillance theories, which bring further shape to the original theories of Bentham and Eddy [29]. One of the risks linked to the reality we live today, where data extracted from the physical world flows constantly across the digital world are that massive surveillance makes us insensitive to its perverse effects [30].

This feeling of normalisation of the use of surveillance technology seems to mainly affect individuals born between 1982 and 2000, the ‘Millennium’ generation, who grew up already integrated to digital technologies [31]. A research conducted by the Pew Research Centre, in November 2019, reveals that youngsters ranging from 18 to 29 years old feel more in control of the technologies they use and are less interested in keeping abreast of news about privacy and data protection [32]. Another study showed that youngsters believe that the reduction of privacy is part of contemporary life and that providing personal information is necessary to participate in the digital world [33].

The fact that multiple digital services are based on the constant exposure to monitoring cameras in conjunction with rampant data collection means that individuals are unable to object to the mass processing of their personal data. The issue is even more complex in countries like Brazil, where urban violence is a daily problem and public (and private) security is perceived as a measure to be prioritised. State efforts to make their security systems more efficient are such that large grants are offered for the development of technologies for this purpose [34].

The possibility of creating a society that is indifferent to cyber-surveillance is a relevant risk that should be taken into account in the use of FRT. If this happens, citizens’ expectation of privacy threshold will lower down, and the idea of being under constant surveillance, either by public agents or private entities, will become an accepted routine. This is a process which is already happening: the application on FRT to promote security, scoring systems or targeted marketing has the potential to gradually make individuals believe that ubiquitous surveillance should be part of their everyday’s lives.

3.4 Lack of transparency

The aim of conducting predictive analyses of individuals’ actions is often limited by statistical handicaps of artificial intelligence programmes, of which facial recognition is a sub-category [35]. These systems are fed by large databases to search for correlations between stored images and those captured with special cameras. However, the matches are based on specific patterns to make predictions that do not take account of the contexts in which individuals whose data are collected perform their actions [36]. The inability

⁹ A *match* occurs when the artificial intelligence system is compatible between an image captured by the camera and another image contained in a given data bank.

Table 1 Risks of FRT processing purposes in Brazil

Risks	Purposes				
	Public security	Social scoring and digital identity	Private security	Targeted marketing	Public health
Lack of legal basis	X	X	X	X	X
Inaccuracy	X	X	X		
Normalisation of cyber-surveillance	X	X	X	X	
Lack of transparency	X	X		X	X

to contextualise could lead to arbitrary decisions based on pre-existing discriminatory social patterns, for example to categorise individuals who would allegedly have the most chance of presenting deviant behaviour.

In this regard, situations such as the false positive occurrences during Carnival in Brazil lead to the questioning of how to improve transparency in facial recognition systems, a key principle for the exercise of data protection rights such as rectification (the correction of errors in databases) and erasure of personal data. Without adequate supervision of such applications, standards used for the profiling of individuals and recognition of suspects are not revealed, which hinders accountability for possible abuses and discriminatory practices [36].

Knowledge of how data are processed and how profiles are developed is essential for individuals to be able to scrutinise the actions taken by public and private actors when applying facial recognition technologies. The lack of transparency only increases the error points, as the channels of operators' responsibility for possible abuses in the monitoring of individuals are almost non-existent when there is no knowledge of how data are processed. Knowing which data feed public and private security systems is an important factor in determining the levels of error for these applications [37]. In public security settings, police often base their decisions on data which they are not sure how it has been collected or categorised.

In this regard, the United States' National Institute of Standards and Technology—NIST highlighted face recognition systems' failures in identifying individuals from specific racial/ethnic groups. In a report published in December 2019, the institute pointed out how these systems constantly identified black-skinned people with less precision than it was the case with white-skinned individuals. These systems were also more accurate in identifying men than women, which indicates how certain groups were misrepresented in the databases from which the technology was fed [38].

To this end, to ensure the proper use of those facial recognition systems, the development of transparency mechanisms is crucial to prevent unjustified intrusion in privacy and data protection, as well as the sanction of agents abusing personal data. Therefore, the lack of transparency can

harm fundamental rights when used to achieve public security, digital identity, marketing and public health purposes, whereas the data subject may not be aware of how her data is being processed. This includes information about the purposes of processing, the possibility of sharing the data with others entities and the period of time during which her information will be used.

With that being said, a parallel between different uses of FRT and the risks they pose should be resumed as under Table 1. Although they focus on the Brazilian context, some risks could similarly exist under other jurisdictions. Furthermore, while the identified risks could apply to any of the purposes, the table highlights where they seem to be most critical.

4 Measures to ensure data protection in venues applying facial recognition systems

The use of facial recognition makes it necessary to implement safeguards to ensure the protection of personal data collected in public or private spaces through the mere transit of individuals. The measures addressed in this study are (1) soft law mechanisms; (2) oversight; (3) use of technical standards; (4) public security data protection settings; and (5) implementation of regulatory sandboxes.

4.1 Soft law

Legislative norms are often insufficient to regulate the minutiae and complexities surrounding the application of rules and principles in the practice of regulated sectors. Soft law mechanisms have thus been developed to comprise the publication of guidelines and recommendations of non-binding effects to guide regulated agents [39]. Soft law tools are particularly useful for the regulation of fast-moving technology because they are more flexible and dynamic than legislation and they are often also applied by courts [39].

In the European context, the European Data Protection Board (EDPB) indicates issues to be observed in the storage of biometric templates such as those collected for

Fig. 2 Monitoring camera warning panel. How they are usually in Brazil (left) and how it would be an ideal model, inspired by the recommendations of the EDPB and adapted to the context of LGPD (right)

authentication purposes in high-security environments, such as airports or laboratories. In such situations, the controller must ensure that she does not hold the sensitive data of individuals in her database. The template should preferably be stored in a device (e.g. a token) to which only the data subject has access, a measure which reduces data breach risks and ensures that the data subject has control over her biometric data [12].

To protect privacy and personal data, the handbook recommends technical and administrative measures which include data protection by design and by default. According to the guide, data safety should be able to provide confidentiality (data is accessible only to selected individuals), integrity (by preventing manipulation or loss of data) and availability (data should be available when required) [12]. In addition, an access control mechanism should be implemented, ensuring that only authorised persons access the data and the information system.

When cameras are used as a technical security measure, the data controller should (1) indicate the purpose and scope of the use of a camera system; (2) limit the video monitoring system over a specified period of time and space; (3) provide transparency by warning individuals about the existence of cameras in the environment; and (4) establish who has access to the recordings and for which reason. Information on the existence of surveillance cameras must be carried out in two layers. The first shall be a warning plate, which is visible and intelligible, and capable of providing a meaningful view of the purpose of the processing. For the second layer, a full information document should be available at a location with easy access such as an information point or a reception [12].

In Brazil, some spaces warn individuals that they are being filmed with a smiling image, suggesting that there is nothing to worry about the operation. Besides the

normalising effect of the warning sign, it also does not inform properly whose data is being collected and for what purposes. Inspired by recommendations of the EDPB Guide, we propose a model that would contain every information that should be present in an ideal warning sign (see Fig. 2). All of them comply with Article 18 of the LGPD, which provides for data subjects' rights.

Soft law may prove itself helpful in assisting data controllers to identify what legal basis is suitable for their intended purposes on the use of FRTs. Moreover, it would be an effective tool for defining acceptable accuracy thresholds for false positives or false negatives according to different contexts, something which would set parameters for data controllers in implementing safer solutions for face recognition. Guidelines may also establish what are the contexts in which FRT may be deployed, to combat the normalisation of cyber-surveillance in both public and private spaces. Finally, soft law may define transparency practices to be followed by controllers for informing data subjects about the use of FRTs.

EDPB's Guideline 03/2019 on video surveillance is a good example of how regulators should address this theme. The publication sheds light on how to specify the purposes and defining the legal basis for the data processing, namely for legitimate interest and consent. It also guides controllers on what should cameras record, the places they should be installed as well as transparency and information obligations [12].

4.2 Oversight

Oversight is one of the most important tools to ensure law enforcement and best practices among data controllers and processors. Five elements are crucial for a well-structured supervisory mechanism for video surveillance purposes: (1) existence of an independent supervisory authority; (2)

existence of legal authorisation for surveillance activities (i.e. the activity be authorised by law); (3) monitoring of the use of surveillance technology; (4) conducting surveillance reports; and (5) the existence of effective remedies in response to the surveillance operation.¹⁰

The existence of an independent supervisory authority for data protection ensures effective application of the law without the influence of political or economic interests [40]. By aggregating these features, the data protection authority is capable of effectively enforcing fundamental rights through regulatory channelling options in the supervised sector [41]. In addition, activities likely to allow for surveillance should be priorly authorised by the DPA, except in emergency situations such as imminent danger, in which case oversight may take place after data processing.

Surveillance will be lawful if it falls into the scope of one of the legal bases of Article 7 of the LGPD (or Article 11, if sensitive data is processed). Otherwise, it should be ensured that the transaction is authorised by specific legislation or other supervisory mechanisms (such as the Judiciary). Unfortunately, the absence of special law for dealing with public security cases in Brazil leaves a loophole for abuse by public authorities in the data processing of individuals.

In view of the above, an independent authority would be a key player for supervising the accuracy of face recognition systems, as well as establishing in which cases should FRT be used and how controllers should be transparent with data subjects.

In the Brazilian context, the National Data Protection Authority (ANPD) will have a key role in monitoring such data processing operations, which includes providing guidance and issuing sanctions for the technology's misuse. Unfortunately, up to the conclusion of this research, the supervisory authority had not yet been composed, which brings a lot of concerns to the future of the Brazilian data protection framework [42].

4.3 Standardisation

One of the most widely used self-regulatory mechanisms is the adoption of technical standards established by scientific and technical communities. Entities such as the International Organization for Standardization (ISO) and the Institute of Electrical and Electronics Engineers (IEEE) are known for their well-established standards, widely adopted by organisations. Complying with ISO's or IEEE's norms is a certificate

that a company adopts good practices, and is beneficial for both private entities and society [43].

Recently, the International Organisation for Standardisation (ISO) has launched a pattern for the development of Privacy Information Management Systems (PIMS), the ISO 27701 series, which complements the best-known ISO 27001, focusing on information security management systems (ISMS). ISO 27701 works with the concept of *Personally Identified Information* (PII), which is parallel to the definition of personal data in data protection settings such as LGPD and GDPR. Other concepts such as data subject, controller and data processor also have their counterparts under the ISO's standard.

Corporations expect that the adoption of technical standards such as ISO 27701 may be recognised by DPAs as proof of data protection compliance. In theory, this might be possible in Brazil, as the LGPD provides in Article 35 for the possibility of establishing certification schemes for the demonstration of conformity to regulation, a theme yet to be addressed by ANPD. A similar provision exists in Article 42 of the GDPR.

Such adoption may also represent adherence to the principle of Privacy by Design, provided by both LGPD and GDPR under articles 46 and 25, respectively, which establish that controllers shall implement appropriate technical and organisational measures to protect the rights of data subjects.

While there are no specific privacy standards for facial recognition technologies, it is expected that models such as ISO 27701 could limit eventual abuses by controllers and data processors, especially when establishing accuracy thresholds and tools for enhancing the transparency of these systems. However, the adoption of standards alone would hardly solve all problems, mainly because surveillance issues often take place for public security purposes, leaving aside the sphere of private interest and becoming a complex issue involving political interests.

4.4 Public security data protection legislation

Although general data protection laws, such as the LGPD and the GDPR do not apply to data processing for public security, this does not mean that this regulatory gap is irrelevant. On the contrary, it makes even more clear that there are rules which have yet to be discussed to regulate the subject.

In the European case, this is done by Directive 2016/680, which entered into force and full effectiveness on the same dates as the GDPR. The regulation addresses the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, as well as the free movement of such data. The Directive is in many ways similar to the general regulation, such as when

¹⁰ These safeguards were based on the case-law in the context of surveillance of the European Court of Justice and the European Court of Human Rights. See more in MORAES, T. G.S. Spark of Light in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures. 2019. Master Thesis in the Law and Technology LLM Program, Tilburg (NL)—Jun/2019.

defining its principles. However, the peculiarities of activities concerning public security require more flexibility in certain legal obligations [25]. For example, the principle of transparency is not established, and certain restrictions are laid down for the principles of minimisation and purpose limitation.

In Brazil, an experts' committee has been set to draft a law proposal on the use of personal data for the purpose of criminal investigations [44]. The committee consists of a body of fifteen lawyers with different expertise and from different public and private entities. Nevertheless, considering the potential threats of FRT when applied to public security, a moratorium of the technology would probably be a safe option to avoid abuses with its use until the data protection legislation for public security purposes is approved. Such a measure has already been taken by the US city of San Francisco [45].

The specialised and multi-sector composition of the committee promises good prospects for the preliminary draft to be drawn up. While legislation should pursue technological neutrality by avoiding to cover a specific technology, it is inevitable that the principles and obligations to be set out in the proposal are used as a basis for the regulation of facial recognition technology.

4.5 Adoption of alternative regulatory methodologies: regulatory sandboxes

Given the difficulty of aligning the use of FRTs with data protection, a plausible solution is the adoption of testing environments to regulate it. An experimental model which may be adopted for this purpose is a regulatory sandbox.

A sandbox is a regulatory tool by which a regulatory authority creates a controlled normative environment where innovators can test innovative products, services or business models without having to follow all the legal norms that cover their activity. In that environment, regulators work alongside developers to assess what risks and benefits may rise from innovation to better regulate it. The requirements for a solution to be accepted for a sandbox vary from each regulator. In general, the product, service or business model is required to be innovative, beneficial to the consumer, ready to work and that there is a prior analysis of the risks involved [46].

The UK's Information Commissioner's Office—ICO, was the first body to set up a sandbox for assessing data protection issues [47]. One of the projects assessed by the ICO in the public security field has been an initiative of the *Violence Reduction Unit* (VRU), an entity of the Greater London Authority. The VRU has developed a system by which it intends to process health, social security and criminal activity data in an integrated and collaborative way to reduce

urban violence in London. The processing of such data is currently monitored by the ICO, which analyses potential impacts on privacy and data protection of individuals [45].

By creating a space of confidence in which the regulator and the regulated can engage directly, sandboxes allow changes in technology development to be made in a more agile and safe manner. In addition, they can reduce companies' legal advisory costs to comply with the patchwork of the regulatory systems of different countries, which, according to the OECD, amounts nearly 780 billion dollars per year worldwide [48]. A sandbox for FRT would probably be a great tool to better understand the risks of these systems and properly address issues such as their accuracy, as well as enhance transparency [49].

Brazil has already initiated discussions for the implementation of its first sandboxes. The Central Bank [50] and the Securities Commission [51] have already launched public consultations on the topic, whereby stakeholders may formally express their views on the topic.

A sandbox for FRTs should be monitored by the ANPD. In this sense, some steps should be followed for the smooth running of the programme. Firstly, the authority should ensure that it is equipped with enough personnel to keep pace with the development of the technology and to pay due attention to its creators' demands.

In addition, it is up to the regulator to adapt its organizational culture to allow more competitiveness and encourage innovation while ensuring privacy and data subjects' protection [52]. Otherwise, developers will be trapped in the regulators' conservatism and will not have incentives to join sandboxes whose authorities do not allow for adequate flexibility for the development of new technologies.

The relation between risks and measures to address them should thus be resumed as under Table 2. Once again, the measures herein addressed are focused on the Brazilian framework, but could be applied in other jurisdictions as well.

5 Conclusion

Due to the large amount of sensitive data processed by facial recognition systems, the principles and guarantees of data protection should be applied to these technologies with further care. The lack of regulation for the use of this technology raises concerns when it is applied for public security purposes and for digital profiling. By allowing indiscriminate and massive collection of personal data, the exercise of rights such as privacy and freedom of expression is put in check, threatening to put anyone under the vigilant eyes of the state.

On the other hand, in semi-public areas, the use of facial recognition for private security and targeted marketing

Table 2 Measures for addressing risks in FRTs

Measures	Risks			
	Lack of legal basis	Inaccuracy	Normalisation of cyber-surveillance	Lack of transparency
Soft Law	X	X	X	X
Oversight	X	X	X	X
Standardisation		X		X
Public security data protection framework	X			
Regulatory sandboxes		X		X

campaigns is also alarming not only for increasing the level of surveillance of individuals but also for the ability to create profiles and influence consumers' choices. Therefore, the processing of biometric data for identification in such contexts should comply with the narrow criteria of Article 11 of the LGPD, such as the need for the data subject's explicit consent or compliance with legal or regulatory obligations.

To mitigate those risks, initiatives such as those described in this paper should be considered: adoption of *soft law* mechanisms, implementation of adequate oversight, compliance to technical standards, regulatory sandboxes and, especially in Brazil, the development of a data protection legislation for public security purposes. Such tools may be useful to ensure a safer development of facial recognition technologies by developing normative methods to ensure compliance with data protection principles, such as minimisation of collected data, transparency, non-discrimination and free access. This is the only way to ensure more control of the data by its subject.

The development of such legal and regulatory mechanisms takes time. Therefore, until safeguard conditions for the data subject are guaranteed, the Brazilian State should consider the possibility of stipulating a moratorium on the use of such technology in public and semi-public spaces, as has been decided by the government of the US city of San Francisco.

In view of the high amount of sensitive data collected by FRTs, care must be taken to ensure that they are regulated in such a way as to ensure mechanisms to prevent abuse by entities applying these systems. Until then, the suspension of its use for a certain period of time ensures a deadline for discussing the implementation of adequate regulatory instruments, as well as the development of regulatory sandboxes and soft laws to ensure that it is properly developed. In this sense, some time is needed for regulators to propose proportionate safeguards that FRT operators should apply, not only to guarantee the ethical development of these technologies but also to make those who abuse them accountable.

Funding Not applicable.

Compliance with ethical standards

Conflict of interest All author(s) declare that they have no conflicts of interest.

References

- Peterson, M.: Living with difference in hyper-diverse areas: how important are encounters in semi-public spaces? <https://www.tandfonline.com/doi/full/10.1080/14649365.2016.1210667> (2016). Accessed 20 Jan 2020
- Sabbagh, D.: Facial recognition row: police gave King's Cross owner images of seven people' The Guardian. <https://www.theguardian.com/technology/2019/oct/04/facial-recognition-row-police-gave-kings-cross-owner-images-seven-people> (2019). Accessed 20 Jan 2020
- Lisboa, V.: Câmeras de reconhecimento facial levam a 4 prisões no carnaval do Rio' Agência Brasil. <http://agenciabrasil.ebc.com.br/geral/noticia/2019-03/cameras-de-reconhecimento-facial-levam-4-prisoas-no-carnaval-do-rio> (2019). Accessed 20 Jan 2020
- Lobato, L., et al.: Videomonitoramento: mais câmeras, mais segurança? <https://igarape.org.br/videomonitoramento-webreport/> (2020). Accessed 22 Jun 2020
- Metrô: Metrô compra sistema de monitoramento eletrônico com reconhecimento facial. <http://www.metro.sp.gov.br/noticias/28-06-2019-metro-compra-sistema-de-monitoramento-eletronico-com-reconhecimento-facial.fss> (2019). Accessed 20 Jan 2020
- Chivers, T.: Facial recognition... coming to a supermarket near you' The Guardian. <https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties> (2019). Accessed 20 Jan 2020
- Mann, M., Smith, M.: Automated facial recognition technology: recent developments and approaches to oversight. *UNSW Law J.* **40**(1), 121 (2017)
- Güven, K.: Facial recognition technology: lawfulness of processing under the GDPR in employment, digital signage and retail context. (Master Thesis, Tilburg University 2019) (2019)
- Garvais, J.: How facial recognition works? <https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html> (2018). Accessed 20 Jan 2020
- Article 29 Data Protection Working Party—Art29WP: Opinion 02/2012 on facial recognition in online and mobile services. <https://ec.europa.eu/justice/article-29/documentation/opinion-recom>

- mendation/files/2012/wp192_en.pdf (2012a). Accessed 22 Sept 2020
11. Article 29 Data Protection Working Party—Art29WP: Opinion 03/2012 on developments in biometric technologies. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (2012b). Accessed 22 Sept 2020
 12. EDPB: Guidelines 3/2019 on processing of personal data through video devices. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf (2020). Accessed 20 Jan 2020
 13. Brazil: Constitution of the Federative Republic of Brazil of 1988. http://www.planalto.gov.br/ccivil_03/Constituicao/ (1988). Accessed 20 Jan 2020
 14. Instituto Brasileiro de Defesa do Consumidor—IDEC: Carta Idec nº 30/2019/Coex. https://idec.org.br/sites/default/files/carta_idec_coex.pdf (2019). Accessed 20 Feb 2020
 15. Paiva, A., et al.: Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. <http://observatoriosegurancacom.br/wp-content/uploads/2019/11/1relatoriorede.pdf> (2019). Accessed 20 Jan 2020
 16. Ma, A.: China has started ranking citizens with a creepy “social credit” system—here’s what you can do wrong, and the embarrassing, demeaning ways they can punish you’ Business Insider. <https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4> (2018). Accessed 20 Jan 2020
 17. Lakshmanan, R.: India is going ahead with its facial recognition program despite privacy concerns The Next Web. <https://thenextweb.com/security/2019/11/11/india-goes-ahead-with-its-facial-recognition-program-despite-privacy-concerns/> (2019). Accessed 20 Jan 2020
 18. Brazil, Law 7.102, of 20 June 1973: http://www.planalto.gov.br/ccivil_03/LEIS/L7102.htm (2019). Accessed 22 Jun 2020
 19. Wiewiórowski, W.: Facial recognition: a solution in search of a problem? <https://edps.europa.eu/node/5551> (2019). Accessed 20 Jan 2020
 20. Instituto Brasileiro de Defesa do Consumidor: Após denúncia do Idec, Hering é condenada por uso de reconhecimento facial. <https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por-uso-de-reconhecimento-facial> (2019). Accessed 4 Sep 2020
 21. Dekkers, D.: Privacy or security?—Function Creep’ kills your privacy’ Digidentity. <https://www.digidentity.eu/en/article/Function-creep-kills-your-privacy/> (2016). Accessed 20 Jan 2020
 22. Kuo, L.: The new normal: China’s excessive coronavirus public monitoring could be here to stay’ The Guardian. <https://www.theguardian.com/world/2020/mar/09/the-new-normal-china-s-excessive-coronavirus-public-monitoring-could-be-here-to-stay> (2020). Accessed 20 Jan 2020
 23. Tétrault-Farber: Moscow deploys facial recognition technology for coronavirus quarantine’ Thomson Reuters. <https://uk.reuters.com/article/us-china-health-moscow-technology/moscow-deploys-facial-recognition-technology-for-coronavirus-quarantine-idUKKBN20F1RZ> (2020)
 24. OECD: Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics. <https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics/> (2020). Accessed 20 Jun 2020
 25. European Commission: Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. <https://eur-lex.europa.eu/eli/reco/2020/518/oj> (2020). Accessed 20 Jun 2020
 26. Wright, E.: The future of facial recognition is not fully known: developing privacy and security regulatory mechanisms for facial recognition in the retail sector. *Fordham Intell. Property Media Entertainment Law J.* **29**(2), 611–686 (2019)
 27. G1: The facial recognition system of the RJ’s PM, and women is mistakenly detained. <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml> (2019). Accessed 03 Sep 2020
 28. European Union Agency of Fundamental Rights—FRA: Facial recognition technology: fundamental rights considerations in the context of law enforcement. <https://fra.europa.eu/en/publication/2019/facial-recognition> (2019). Accessed 20 Jan 2020
 29. Galic, M., Timan, T., Koops, B.: Bentham, deLeuze and beyond: an overview of surveillance theories from the panopticon to participation. *Philos. Technol.* **30**, 9–37 (2017)
 30. Article 29 Data Protection Working Party—Art29WP: Working document on biometrics https://iapp.org/media/pdf/resource_center/wp80_biometrics_08-2003.pdf (2003). Accessed 20 Jan 2020
 31. Howe, N., Strauss, W.: Millennials rising: the next great generation. Knopf Doubleday Publishing Group, New York (2009)
 32. Auxier, B., et al.: Americans and privacy: concerned, confused and feeling lack of control over their personal information. <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/> (2019). Accessed 20 Jan 2020
 33. Fulton, J., Kibby, M.: Millennials and the normalization of surveillance on Facebook. *J. Media Cult. Stud.* **31**(2), 189–199 (2017)
 34. Pinho, M.: Governo anuncia R\$ 10 mi em bolsas de estudos para combate ao crime. <https://noticias.r7.com/brasil/governo-anuncia-r-10-mi-em-bolsas-de-estudos-para-combate-ao-crime-08012020> (2020). Accessed 20 Jan 2020
 35. Sloan, R., Warner, R.: Algorithms and human freedom. *Santa Clara High Technol. Law J.* **35**, 4 (2019)
 36. Solove, D.: Data mining and the security–liberty debate. *Univ. Chicago Law Rev.* **75**(1), 343–361 (2008)
 37. Ferguson, A.G.: Big data and predictive reasonable suspicion. *Univ. Pennsylvania Law Rev.* **163**(2), 327 (2015)
 38. National Institute of Standards and Technology—NIST: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects’ <https://doi.org/10.6028/NIST.IR.8280> (2019). Accessed 20 Jan 2020
 39. Hagemann, R., Huddleston, J., Thierer, A.: Soft law for hard problems: the governance of emerging technologies in an uncertain future. *Colorado Technol. Law J.* **17**(1), 37 (2018)
 40. Thiago Guimarães Moraes: A spark of light in the going dark: legal safeguards for law enforcement’s encryption circumvention measures’ (master’s thesis. Tilburg Univ. **2019**, 50 (2019)
 41. Aranha, M. I.: Manual de direito regulatório: fundamentos de direito regulatório, 3rd edn. Laccademia Publishing (2015)
 42. da Mota Alves, F., Vieira, G.A.S.: Sem a ANPD, a LGPD é um problema, não uma solução. https://www.jota.info/paywall?redirect_to=https://www.jota.info/opiniao-e-analise/artigos/anpd-lgpd-problema-solucao-06012020 (2020). Accessed 20 Jun 2020
 43. Danish Standards Foundation: A World Built on Standards: A Textbook for Higher Education. <https://www.ds.dk/media/px5jhn/a-world-built-on-standards.pdf> (2015). Accessed 20 Jan 2020
 44. Chamber of Deputies: The collegial will have 120 days to draw up the preliminary draft, which will then be examined by the Congress. <https://www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/> (2019). Accessed 9 Jan 2020

45. Lee, D: San Francisco is the first US city to ban facial recognition' BBC. <https://www.bbc.com/news/technology-48276660> (2019). Accessed 20 Jan 2020
46. Zetzsche, D., et al.: Regulating a revolution: from regulatory sandboxes to smart regulation. *Fordham J. Corporate Financial Law* **2018**, 30 (2018)
47. Information Commissioner's Office –ICO: The Guide to the Sandbox (beta phase). <https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/> (2019). Accessed 20 Jan 2020
48. International Federation of Accountants—IFAC: Regulatory divergence: costs, risks, impacts. <https://www.ifac.org/system/files/publications/files/IFAC-OECD-Regulatory-Divergence.pdf> (2018). Accessed 20 Jan 2020
49. Babuta, A., Oswald, M., Rinik, C.: Machine learning algorithms and police decision-making legal, ethical and regulatory challenges. https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf (2018). Accessed 20 Jan 2020
50. Banco Central do Brasil–BCB: Detalhamento da Consulta n. 72. <https://www3.bcb.gov.br/audpub/DetalharAudienciaPage?5&pk=321> (2019). Accessed 20 Jan 2020
51. Comissão de Valores Mobiliários—CVM: Audiência Pública da CVM para criação de ambiente regulatório experimental (sandbox regulatório). <http://www.cvm.gov.br/noticias/arquivos/2019/20190828-1.html> (2019). Accessed 20 Jan 2020
52. Tsai, C.: To regulate or not to regulate? A comparison of government responses to peer-to-peer lending among the United States, China, and Taiwan. *University of Cincinnati Law Rev* (2019)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.