FACIAL RECOGNITION AND THE PRIVATE SECTOR

Guide for the adoption of good practices

WHO ARE INTERNETLAB AND IDEC?

InternetLab is an independent interdisciplinary research center that produces knowledge and fosters debate on different areas related to technology, rights, and public policy. We are a São Paulo-based non-profit organization that acts as a liaison between researchers and public, private and civil society representatives.

Our initial argument is that the formulation of good public policies depends on more accurate diagnoses of the relationship between new information and communication technologies – such as the internet – and people's rights. Read more about it on our website: www.internetlab.org.br

Idec (the Brazilian Consumer Protection Institute) is a non-profit consumer association. Our mission is to promote education, awareness, the defense of consumer rights, and ethics in consumer relations, emphasizing political and economic independence. We work on policies to universalize telecommunication services and internet access in Brazil, ensuring proper levels of quality and respect towards information rights, transparency, non-discrimination, and personal data protection. Read more at: https://idec.org.br/

WHAT IS THE PURPOSE OF THIS DOCUMENT?

This report, jointly produced by InternetLab and Idec, seeks to introduce good practices that can guide the private sector in the development of its activities, regarding the offer products and services based on facial recognition technologies. The report offers an overview of the main issues related to the use of facial recognition technologies by private legal entities in Brazil, presenting the basic characteristics of how these tools work and some concepts required to understand the discussion. We believe adopting good practices in the use of facial recognition technologies is an ethical and legal necessity for companies that intend to promote innovation in a responsible manner.

ACKNOWLEDGMENTS

The process of preparing this report involved workshops with civil society and private sector representatives, whose contributions were essential for the development of a more complete and detailed guide. InternetLab and Idec are thankful for all those who took part in these workshops and who helped prepare document.

In order not to be unfair to all those who helped us, we will not mention their names individually, but we reiterate our acknowledgment of their essential contributions.

PROJECT TEAM

Preparation:

Bárbara Simão (Researcher in the area of Telecommunications and Digital Rights at Idec)

Nathalie Fragoso (Coordinator of InternetLab's Privacy and Surveillance Area)

Enrico Roberto (Researcher at InternetLab)

Collaboration:

Diogo Moyses (Coordinator in the area of Telecommunications and Digital Rights at Idec)

Juliana Oms (Researcher in the area of Telecommunications and Digital Rights at Idec)

Francisco Brito Cruz (Director at InternetLab)

Heloísa Massaro (Coordinator of the Information and Policy area at InternetLab)

Dennys Antonialli (former director of InternetLab until October/2019)

How to cite this document

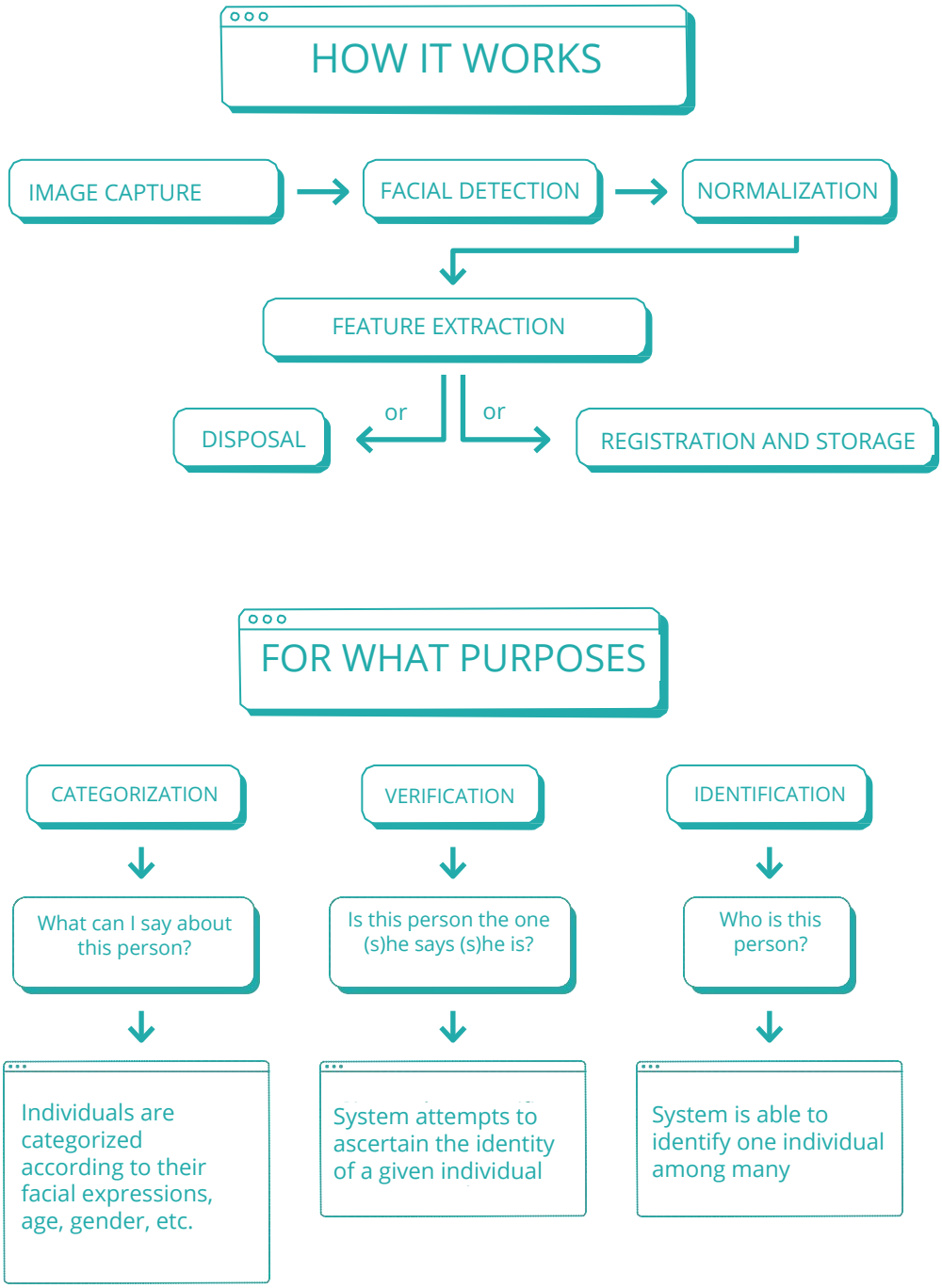
SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; *Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas.* InternetLab/IDEC, São Paulo, 2020

EXECUTIVE SUMMARY

1. FACIAL RECOGNITION – WHAT IT IS, HOW IT WORKS, AND WHAT IT IS FOR

DEFINITION

FACIAL RECOGNITION → Automated processing of images containing individuals' faces in order to identify, verify, or categorize these individuals



2. ASSUMPTIONS

_ Any technology capable of detecting a human face can be considered facial recognition

Even if the ultimate goal of a given piece of technology is not the identification of a specific person, in order for detection to take place, it is necessary to collect and process data from human faces, at which point the attributes and reference points of a face are read.

_ Data regarding to human faces are personal data

According to art. 5, item I, of the Brazilian General Data Protection Law (LGPD), all information related to an *identified or identifiable* individual is personal data.In general, it is considered that the image of a person and the information resulting from said image constitute personal data, thus falling under the scope of this legislation.

_ All facial recognition involves the processing of personal data

All facial recognition processes require the processing of images of human faces. This is because, in order for the basic functionalities of a facial recognition algorithm to be performed, a face will always have to be detected and its image will have to be treated, even if such data is subsequently deleted or anonymized.

Since it involves the processing of the image of a face – a piece of personal data –, it is impossible to think about facial recognition without assuming that personal data will be processed.

_ Data from human faces treated in the context of facial recognition are sensitive (biometric) data

From the moment a facial recognition system is able to analyze reference points on a face, extracting inferences about its personal features from these points of reference, it is performing sensitive data processing. Specifically, regarding biometric data: Even though Brazilian law does not provide precise definition of biometric data[1], the definition outlined by the General Data Protection Regulation in Europe can be illustrative: these are "personal data resulting from a specific technical treatment related to physical, physiological or behavioral characteristics of an individual that allow or confirm the unique identification of that individual, namely facial images or fingerprint data."

Furthermore, several pieces of intimate information can be inferred from the extraction of facial features: its racial or ethnic origin, age, gender, etc.

1. Although it is still under discussion among legislative representatives, Decree No. 10.046/2019, which establishes the Citizen's Base Registry, presents the following definition of biometric attributes: "measurable biological and behavioral characteristics of an individual that can be collected for automated recognition, such as the palm of the hand, fingerprints, retina or iris, the shape of the face, voice and gait" (Art. 2, II)

_ Data anonymization does not mischaracterize the processing of personal data

Although data can no longer be individualized after anonymization, the processing that has been applied up to that point involves the processing of a person's image. Therefore, subsequent image anonymization or exclusion should not exempt the operator from complying with the requirements and principles contained in the applicable legislation.

3. FACIAL RECOGNITION RISKS

_ Abuse of rights and control

Facial recognition is a technology that allows for the identification and obtaining of sensitive information about individuals by those who control and access the system. If misused, whether deliberately or through negligence in mitigating risks, they can be used as control tools and result in abusive practices, discrimination[2] and privacy breaches. If biometric data stored in the context of this technology is not handled with due care, or if it is shared with law enforcement and government authorities, for instance, this data can also serve as a basis for surveillance tools. Therefore, there are potential risks to fundamental rights, including the right to the protection of personal data.

_ Discrimination and bias

Another source of risk concerns the "algorithmic bias", i.e. the reproduction of discriminatory patterns in the results presented or in the use made by algorithms. For instance, in the case of a facial recognition tool trained with references to a database mostly made up of white-skinned people, its accuracy will be reduced when used to identify black-skinned people, thus generating discriminatory results. Studies have shown that the error rate of these tools is systematically higher for black women compared to other groups, for instance [3].

2. We emphasize that discrimination, in this report, is a term used mainly in its legal sense, that is, the sense of damage to the fundamental right to equality and dignity, especially against historically oppressed or minority groups. It does not refer to discrimination as mere separation into categories.

Algorithm-based discrimination can lead to discriminatory practices (denial of services, price distinction), essential technologies that do not work well with the entire population (facial authentication of black individuals, for instance), and other potential problems.

_ Privacy risks

To a greater or lesser degree, facial recognition will allow access to multiple pieces of private data on the data subjects: gender, age, race, etc. The excessive use of this data or failure to comply with the purposes of its collection may represent violations to the privacy of individuals analyzed by facial recognition.

_ Poor recognition of emotions

The recognition of emotions has been questioned in regards to its accuracy. The difficulty in obtaining reliable results may represent a risk if such systems are used as a criterion for access to the exercise of a right – such as an automated job interview that takes the candidate's emotions into consideration, for example.

---

3. https://ieeexplore.ieee.org/document/6327355; Buolamwini and Gebru conducted a study that analyzed three commercially available facial recognition tools that detect an individual's gender. The research tested the accuracy of this system and concluded that the error rates found in the three tools are significantly higher in black women compared to white men. http://proceedings.mlr.press/v81/buolamwini18a/buo-lamwini18a.pdf http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf

_ Security incidents

The security of storing this data is another crucial matter, especially since it involves biometric data.Unlike passwords and email addresses, which can be changed, biometric data are unchangeable, which worsens the consequences of any leak.

4. GOOD PRACTICES

_ Prior analysis of proportionality and respect towards principles

The use of facial recognition systems, even if the recommendations we provide in this report are met, present risks to fundamental rights. The good practices that we have pointed out seek to mitigate such risks, but they cannot and do not intend to remove these risks.

Thus, before using any facial recognition system, businesses should assess whether this is the only way to achieve their goals. If less invasive and less risky measures are possible, they should be adopted.

In addition, there must be an analysis on whether the technology to be implemented is in line with the principles espoused by the applicable legislation. For instance, analyzing whether the purposes of collection are being upheld, whether accountability measures are being adopted, among others.

_ Transparency to Data Subjects

As a prerequisite for the exercise of consent and the set of fundamental rights involved, transparency requires the provision of complete and accurate information to data subjects, especially in regards to: *the use of image collection devices; the data collected, its form of processing and the purposes for which it is performed; the term, storage conditions and security measures adopted for its protection; cases in which the data can be shared with third parties; the rights of data subjects over their data and the risks involved in this data treatment.*

In reality, devices such as tablets, televisions or signs can be placed at establishment entrances, as well as warning signs indicating the use of technology,

presenting the company's policies regarding the collection of this data, pointing out the cameras that are capturing images and contact information for the exercise of related rights.

This is a way to empower people undergoing or potentially undergoing facial recognition with information. Through transparency, data subjects must be able to make informed decisions about the use of their biometric data.

_ Public Transparency

In the case of facial recognition, not only should data subjects have the means to act consciously, but measures of public control, accountability and auditing should be adopted as well.

For instance, all practices adopted in the implementation and execution of this technology must be documented in personal data protection impact reports. A suggested good practice is that said reports should also be made available to the public, containing information about which fundamental rights may be affected by the system and what is being done to mitigate such impacts, in a format similar to the Fundamental Rights Impact Assessment advocated by European Union.

Additionally, regular information about the use of the system must be made publicly available, such as the fact that the system is being used, its purpose, places of use and people affected, etc.

And, finally, independent internal bodies that analyze and monitor the use of technology by the company should be instituted. Such bodies should make recommendations, be accountable to public authorities and the general population, ensure respect towards the measures adopted, develop internal policies for access and use of data, etc.

_ Consent

Obtaining consent is one of the main legal requirements for this form of personal data processing. In Brazil, consent must be free, express and informed, and, in the case of sensitive data, provided in a specific and highlighted manner. Even though it is a legal requirement, good practices can be adopted to maximize their protection of fundamental rights.

Therefore, data subjects must necessarily be able to have access to the product, service or functionality, even if they do not consent to the capture of their face data. Additionally, consent must be obtained before the start of image capture, which, therefore, will depend on a positive action by the data subject (such as their express consent through a device available at the store entrance or through an activation QR code).

Since the technology involves sensitive data, processing cannot take place based on legitimate interest. Data may only be processed for the specific uses to which the data subjects consent.

_ Locations where cameras are used

Cameras must be installed in locations that allow prior consent to be obtained from the data subjects. This means that consumers must have the option of not being subject to the collection of their image, without this implying the restriction of other rights, such as the right to access goods and services or the right to easy displacement.

_ Anti-discrimination Measures

At all times in the development and use of this type of system, special care must be taken to ensure that categories such as race, gender, ethnicity, sexual orientation, and others, are not used in a discriminatory manner. For instance, they should not be used, directly or indirectly, and under any circumstances, for the denial of goods or services, price variations or to offer less favorable conditions.

In practice, this requires actions not only from those who use the system, but also from those who develop it. Thus, algorithmic control, testing and correction measures must be adopted to ascertain whether such information has an influence on the system results, in addition to an active effort and training of all those involved in the system's development and use chain.

_ Biometric data deletion, anonymization, and protection

Once the images have been collected and the desired features have been extracted from them, the images must be permanently deleted so that their later retrieval, even by system developers, can be prevented.

In addition, all data permanently stored and/or presented to system operators must be anonymized – for instance, only volumetric data, graphics and the like should be exposed.

Finally, without prejudice to the use of other security measures, we recommend that all (temporary) storage of face images should take place in secure and encrypted environments, logically separated from the environments where the anonymized data is stored. Ideally, this data should always be stored offline, and any connections used to access it should be encrypted.

_ Children and teenagers

According to with Brazilian law, and in an attempt to interpret it in the best interests of children and teenagers, facial recognition for this group cannot take place unless there is specific consent from the child's legal guardian. In the case of teenagers aged 16 through 18, their own consent must also be collected.

Additionally, it should occur in their best interest, which excludes the possibility of using their data in market research, such for the targeting of advertising or business intelligence.

In practice, this means an indication at the door outside the establishment that the entry of unaccompanied children or teenagers is prohibited and that, if they are accompanied, their legal guardians must provide their consent. Other than that, if the image of a child or teenager is captured (with consent), said image must be excluded, and, as pointed out above, data related to it that may be captured or inferred may not be used for commercial purposes, especially for targeting publicity.

_ Security incidents

As this is an eminently sensitive activity with elevated social risk, any and all security incidents must be investigated, immediately reported to public authorities, to civil society and to the data subjects, especially the incidents entail relevant risks or damages.