Biometric Technologies & Human Rights:

A critical overview of the possibilities and limits of biometric identification

CONTENTS

For some years now, the use of biometrics to verify identities has been growing steadily. Already consolidated biometric applications, such as fingerprint capture for administrative and security purposes, have been joined by the use of facial features, while work is also being done on the use of the iris and retina, the vascular pattern of the hands, DNA, gait or voice for commercial, banking or access control purposes, with the promise of greater security, convenience and verifiability. In the face of this explosion of applications, however, the question arises as to whether biometrics are the best answer to the problems faced, and what are the risks of this commitment to the use of bodily traits to verify identities.

.

DEFINITION

Biometrics is a method for recognizing people based on their physiological or behavioral characteristics (INCIBE 2016). It began to be used in the 19th century, initially for the verification of the identity of criminals or suspected criminals based on different body measurements, although the use of the fingerprint soon spread, which until then was used in some parts of the world to verifiably sign documents, as it was much simpler to collect and much more secure than other body traits, susceptible to change over time.

It is generally understood that any biometric feature useful for identification purposes must meet four basic requirements: it must be **universal**, **unique**, **remain over time** and be quantitatively **measurable**. Fingerprint biometrics meet these requirements, and they are very easy to collect, but they have an important limitation: they can only be recorded under conditions of direct contact and, therefore, with the person's permission and knowledge, which is a limitation for the exploration of mass recognition systems. Therefore, for some time now, other options have been investigated, such as facial, gait or voice biometrics, which would allow mass identification applications or identification from a distance. Other possible identifiers, but so far less explored, would be the ear, body odor, heartbeat or the way we type.

Biometrics supplements, and sometimes replaces, traditional identification systems based on cards, numbers or documents external to the body. It is generally understood that biometrics makes it difficult or impossible to impersonate identities, providing greater security in identity verification processes and consequently limiting the fraudulent use of identities to access services.

VERIFICATION VS. IDENTIFICATION

The current boom in these technologies is not accidental, but is closely linked to the increase and improvement of computing capabilities in recent decades, which

have allowed the leap from the use of biometrics to verify identities to their use for identification. Initially, when fingerprints were first used in the police field, they allowed a person's present identity to be matched with a pre-existing fingerprint in the event of a repeat offense. They thus allowed the verification of an identity, but it was necessary to have two matching records. To be able to make that identification, it was necessary to create databases that not only stored the fingerprint records, but also classified them to facilitate their location. Today's computational capabilities, both algorithmic and regarding storage, allow the creation of large records with multiple databases in which data matching occurs automatically. When a record is captured (when we access our workplace or are fingerprinted by the police, for example), it can be checked against other databases to verify our identity. Furthermore, even in our absence our fingers will reveal our identity to anybody with access to our fingerprint. This is one of the great promises of biometrics: without our cooperation, our face, fingerprint, voice, DNA or gait can reveal who we are and thus hinder errors or fraud.

CASES

Biometrics are used to verify identities in both the public and private spheres. In the **public sphere,** their traditional use was limited to security and population control, mainly through the use of fingerprints on identity documents. Police databases have incorporated facial features, which are now essential for instance to apply for a visa or cross a border, and the use of facial recognition in open spaces through security cameras is rapidly increasing in several countries. In Argentina, for example, there has been a Federal Biometric Identification System for Security (SIBIOS in Spanish) since 2011 that collects people's fingerprints, hand palms and faces and is used for police purposes. Pakistan has a similar system, NADRA, initially developed in 2000 during the dictatorship. NADRA is synchronized with a network of high-resolution surveillance cameras in many cities, and incorporates geolocation data and the unique identifier of citizens' cell phones.

The other major area of biometrics deployment in the public sector is social services, with the aim of increasing efficiency in the allocation of benefits and reducing fraud. The most important effort in this regard is the one developed by the Indian state with its Aadhar card, a biometric document essential to access financial services, subsidies and other benefits. In Spain, the Basque Country's employment system started collecting facial features and fingerprints of benefit recipients to minimize fraud, a system that at the time was still being tested, and denounced by civil society for privacy issues and the stigmatization of vulnerable groups. The initiative had to be canceled due to the controversy and a sanction

imposed on the Basque government by the Spanish Data Protection Agency (AEPD)[1][2].

In addition, several countries are synchronizing their identification systems, moving towards what is known as "digital identity". These systems based on biometrics, gather in large centralized databases all the information related to a particular person, which facilitates the control of their activities, benefits or needs. It also enables the incorporation of data not only from national or civil registries, but also information generated in the interaction with private services, transactions and online activity, social interactions, etc.

One of the first concrete efforts to move towards a regulatory framework regarding biometrics has come from Scotland, where a binding ethical Code of Practice[3] for the use of DNA and other biometric data by law enforcement was published in 2022[4].

In the **private sector**, biometrics are especially visible in cell phones, which use fingers and faces to unlock, but many applications make use of less typical traits as typing analysis to recognize users, voice biometrics to analyze interactions and identify preferences, or facial or gait recognition through smart sensors in order to develop user profiles that are as accurate as possible. The banking sector is also making a major effort to standardize biometrics as a system for both employee control and identity verification in digital banking, in order to improve customer relations, combat fraud and enhance transaction security. Similarly, a multitude of services have opted for these systems to control access, from gyms to offices, including vehicles.

Biometrics, and specifically facial recognition, is also becoming essential in the data industry. Applications such as Facebook where users upload pictures of themselves and their surroundings, utilize these images to complete user profiles, which are then sold to third parties for commercial activities based on the resulting profiles, which combine biometric and non-biometric information to define preferences, income levels, employability, social status, etc.

Finally, in the context of biometric capture and analysis technologies, there are many **public-private collaborations**. Often, the public sector does not have the systems or the know-how to develop its own devices, so private companies capture and analyze the data, define the algorithms, and program the decision

[1] https://elpais.com/sociedad/2018/11/09/actualidad/1541758148_321672.html

[2] https://www.diariovasco.com/gipuzkoa/lanbide-cierra-uso-huella-digital-rgi-20220520212347-nt.html

[3] https://www.gov.scot/binaries/content/documents/govscot/publications/consultation-paper/2018/07/consultation-enhanced-oversight-biometric-data-justice-community-safety-purposes/documents/00538315-pdf/00538315-pdf/govscot%3Adocument/?inline=true

[4] https://eandt.theiet.org/content/articles/2022/11/scotland-publishes-first-code-of-practice-for-the-use-of-biometric-data/

systems also for public services and also, as we will see below, for the development and humanitarian aid sector.

In fact, biometrics are so widespread that it is estimated that half of US adults, some 117 million people, are enrolled in biometric data networks used by US law enforcement[5]. Also 20% of the world's 22 million refugees are enrolled in the UN Refugee Agency's (UNHCR) database, with their 10 fingerprints, facial features, information about their families, and administrative status[6].

RISKS

Biometrics has emerged as the latest great promise of technology to improve everyday security. At the beginning of the 21st century it seemed that surveillance cameras were going to provide safer and more livable environments. Today, the hope for a better future lies in the use of the body to increase security and reduce fraud. However, in the same way that trust in cameras did not achieve the horizon of coexistence they promised, trust in biometrics is leading to the abuse of highly sensitive personal data that, once compromised, we can no longer change. We tend to minimize the risks and social impact of biometrics, and use it in contexts where other solutions would be more effective.

The history of biometrics has also been controversial, as skull measurement has been used to determine race superiority, for instance, and other non-white physical traits have been associated with criminal behaviour. At one point France forced Roma residents to carry anthropometric cards until 1968[7], and the German National Socialist party and the nazi movement have used eugenics as a political programme with catastrophic consequences.

Security and Privacy

One of the most obvious risks of all biometric identifiers is that they are permanent personal data. Unlike other "external" identification systems (identity documents, official certificates or passwords) that identify us on the basis of codes or non-biometric personal data, our biometric traits will be with us throughout our lives. Our iris, voice, facial features or fingerprints will change very little, so any situation of vulnerability or hacking will have permanent consequences on our identity and privacy. Collecting biometric data to control access, therefore, emerges as an **irresponsible practice with irreversible consequences**.

[5] https://www.perpetuallineup.org/

[6] https://www.biometricupdate.com/201803/uganda-launches-biometric-program-to-verify-identities-of-1-million-refugees

[7] https://paradojas.hypotheses.org/1008

It is also unclear how to implement emerging digital rights such as the right to be forgotten, a right recognized by some data protection legal frameworks, or how the right to disappear or change identity will be guaranteed in specific cases (people who must be protected because of their role in legal proceedings, people fleeing situations of human rights vulnerations or women at risk of abuse, for example), or how cases of identity theft will be addressed and victims compensated in effective ways.

This concern for security in case of biometric data misuse becomes even more important if we take into account, for instance, that fingerprints are very easy to **forge** using plasticine or silicone, with either a real finger or a photograph of a finger[8]. The resulting mold can be used to unlock a cell phone, but also to leave fingerprints in scenarios where the person to whom they correspond has never been, resulting in false incriminations difficult to escape from. Furthermore, "master" fingerprints developed by machine learning are able to unlock any cell phone with a 76% success rate[9].

In the case of facial features, these vulnerabilities are even more serious. Obtaining a fingerprint is relatively difficult (in fact, a high-resolution picture of a hand is enough), but our faces are found in a multitude of databases, both commercial (such as Facebook) and security databases. For example, a journalist from Forbes magazine printed his face on a 3D printer and managed to unlock several cell phones[10]. Other people have also achieved it simply using pictures of third parties obtained from social networks[11].

Voice biometrics are not secure either. Back in 2015 researchers demonstrated that it was possible to fake anyone's voice using voice morphology software[12]. In fact, there are applications that allow you to scan and reuse any voice to bypass the biometric voice systems of banks, phones or any other application. Iris recognition systems have also been the target of successful attacks. Different researchers have demonstrated on several occasions that a high-resolution photo of an eye (which can be taken from the Internet), or a picture and a contact lens, can fool commercial iris recognition systems[13].

The examples described so far point to vulnerabilities that exist when matching a biometric item with its registry. However, security problems can occur in many

---

8 https://www.xataka.com/seguridad/cinco-minutos-plastilina-y-un-molde-con-eso-basto-para-falsear-mi-huella-y-desbloquear-mi-movil

9 https://www.eldiario.es/tecnologia/Llegan-dactilares-inteligencia-artificial-desbloquear_0_837466910.html

10 https://retina.elpais.com/retina/2018/12/19/innovacion/1545217900_127070.html

11 https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/

12 https://www.uab.edu/news/research/item/6532-uab-research-finds-automated-voice-imitation-can-fool-humans-and-machines

13 https://media.ccc.de/v/biometrie-s8-iris-fun#t=90

other instances. A biometric database can be **hacked**, so that its information can be used to forge identities and gain access to services in someone else's name. It is estimated, for example, that the Aadhar system mentioned above, has leaked the data of some 135 million Indian citizens due to security problems[14]. In these cases it is important to define the encryption standards used by the service provider to assess whether they are up to the risks. Unfortunately, biometric encryption standards are still recent and it is rare for suppliers of these technologies to provide details about their security measures or reliability.

It is also unclear whether at the time of data collection and storage, these companies implement the principle of data minimization precisely to reduce the risks in case of data hacking. According to the specialized literature, the difference between the reliability of a biometric identification using 2 fingerprints or 10 is insignificant. And yet, many operators insist on collecting 10 images, multiplying exponentially the privacy risks without significantly increasing the reliability of the system.

Finally, one of the reasons that most affects the efficiency of biometric systems is related to **data quality**. Using personal data, and especially particularly sensitive information such as biometric data, requires a costly effort to maintain, update and safeguard it. Many of the mistakes identified in databases are due to the incorporation of "bad data", defined by the BadData project as data that is incomplete, incorrect or duplicated, inconsistent or biased, or no longer valid because it has not been updated[15]. The lack of good security and privacy policies, but also of maintenance and updating, as we will see below, is one of the aspects that most contributes to widening the gap between the expectations and the reality of biometrics.

False Identifications

Biometrics promise security and convenience, understood as “easy to use”, and use these as arguments to undervalue biometric security and privacy risks. However, security and convenience rarely go hand in hand.

The promised “easy to use” consists in not requiring documents or the effort of remembering impossible passwords. After all, our fingers, face and voice are always with us. But any rigorous identification process will require time and data quality, neither of which is common in today's biometric contexts. In the case of access control identification (workplace, airports, etc.), it is essential that the time required to capture biometric data and verify it in the relevant databases, is as reduced as possible, to avoid long lines or inconveniences for users. To shorten

[14] https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1

[15] https://eticasfoundation.org/baddata

times, systems must **lower their reliability levels** to process the maximum amount of data as fast as possible and minimize false positives (cases in which the system erroneously triggers an alarm). Unfortunately, the biometrics industry is extremely opaque in this regard, and does not provide data on false positives (and negatives) from its systems. How many travelers with valid and correct visas is it acceptable to stop at a border checkpoint because the database generates an error due to a bad system update (false positives)? How many potential terrorists is it acceptable to allow access to ensure that lines move quickly (false negatives)? These questions, unfortunately, are not asked openly and are solved by technical systems without any transparency or control.

In one case, journalists uncovered a confidential document acknowledging that facial recognition systems at Manchester airport had been "recalibrated" to reduce lines so that with matches of only 30%, travelers were validated to cross the border, generating an error rate of 70%. At these levels, the machines would let, for example, Bin Laden through with Wynona Ryder's passport[16].

The United Kingdom, where facial recognition cameras are used at large public events such as concerts, festivals or sporting events to identify individuals in the crowd whose faces are wanted, is among the few countries to have provided information about the use of this technology. Police data shows how between 2017 and 2018, cameras alerted about 104 of individuals in the crowd at various events. 98% of these (102 individuals) were false positives who were required to show their documents to prove their innocence. Out of the two correct identifications, one person had been listed in the suspect database erroneously and the other one was in a disability database. No arrests were made, calling into question the promises of efficiency and effectiveness of these systems[17].

Different civil rights advocacy groups have conducted experiments to warn about the problem of false identifications. The ACLU, for example, used a facial recognition tool from Amazon to collect 25,000 images of people arrested for a crime, and matched them with the faces of members of the U.S. Congress. Of its 535 members, the system identified 28 as possible criminals[18].

Algorithmic Discrimination

False identifications are worsen by another risk inherent to the use of biometrics: algorithmic discrimination. To verify data extracted from physiological or behavioral traits, these are converted into code ("points") that is matched against other pieces of code. This, through a pre-established algorithmic calculation,

[16] https://www.telegraph.co.uk/news/uknews/law-and-order/5110402/Airport-face-scanners-cannot-tell-the-difference-between-Osama-bin-Laden-and-Winona-Ryder.html

[17] https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

[18] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

determines whether or not there is a match with an existing record. The success of this process depends on both the quality of the initial data and the processes for converting it into code and the algorithms that identify matches. These algorithms often have the ability to "learn," that is, to evolve as they gain experience and are exposed to more data. However, that learning will also incorporate the biases that the algorithms encounter along the way.

Already in 2007 some experts warned of the "**racialized forms of representation**" that shape facial recognition algorithms, which often have trouble processing biometric features that do not fit the standards of white "normality" (Pugliese 2007: 106). This was confirmed in the ACLU experiment described above, in which the congressmen identified as possible criminals were mostly African American, due on the one hand to the over-representation of this group in police databases and on the other hand to the fact that the algorithms are better trained to process white features and therefore fail more often with non-white ones. In 2015, for example, Google had to apologize when its facial recognition application for pictures started labeling black people as gorillas[19].

Data continues to show that discrimination persists. A study from 2018 shows that different commercial facial recognition software achieves success rates of 99% on the faces of white men, but falls short 65% for black women, mainly because the data used to train the algorithms comes precisely from white (75%) men (80%)[20].

Discrimination does not occur only in algorithmic processes. Different reports have already pointed out that the quality of biometric traits can be affected by elements related to the **social status or age** of individuals. Agricultural or manual workers, for example, especially if they are older, have poorer quality fingerprints than other people who are younger or with less arduous occupations. However, fingerprint collection systems are tested only with optimal profiles, leaving these individuals to bear the problems related to the difficulty of inserting their data into biometric systems. In the Indian system described above, people with poor quality fingerprints are often prevented from completing administrative procedures or collecting benefits for days until they can hydrate their fingers to a level acceptable for the machines[21].

This points to something that many voices have been saying: that **technology is not neutral**, and that technological devices are shaped by the politics of representation, power relations and social definitions of what constitutes "standard" or accepted, actively contributing to the exclusion of everything that

---

19 https://www.cnet.com/news/google-apologizes-for-algorithm-mistakenly-calling-black-people-gorillas/

20 http://proceedings.mlr.press/v81/buolamwini18a.html

21 https://www.thehindu.com/opinion/op-ed/To-pass-biometric-identification-apply-Vaseline-or-Boroplus-on-fingers-overnight/article12450793.ece

falls outside those definitions and the technical specifications that make them into code. In this context, it seems that biometrics tend to aggravate, rather than solve, these dynamics of the "quantified society"[22].

Fundamental Rights

As we noted earlier, although different biometric features pose different risks, there is one that they share: the irrevocability in case of error, loss or misuse of such data. This represents a qualitative leap in the assessment of these risks, since there is no way back. Any violation of privacy or the presumption of innocence, therefore, will have consequences that will accompany the victim of these processes throughout their life, since they will not be able to change the biometric traits that incriminate or misclassify them.

There are other impacts on fundamental rights that go beyond privacy. When your body is your identity, your body can also give you away or reveal things you would rather not share. Treating the human body as information that can be digitally encoded and checked against databases, with the individual no longer having agency in telling their own story or control over their body, has profound implications for how we relate to ourselves or to those who have our data. When your body tells on you, it becomes your enemy, something that in the medium and long term can have profound psychosocial consequences for the entire population, as well as aggravating the **lack of transparency and asymmetry in the control of data** between those who generate it and those who exploit it (Van der Ploeg 1999). Some of these aberrations are already being suffered by groups such as the **poor, migrants and asylum seekers**, who are subjected to much greater levels of biometric scrutiny than other population groups. There have been cases of migrants who self-mutilate to avoid being identified through their fingerprints in countries such as Sweden[23] or Japan[24].

These indissoluble connections between the body and authentication and identification processes, often rely on what are known as "**data doubles**" or "data shadows": the result of extracting and regrouping data about a person from different sources to reconstruct his or her profile in code. The result is a disembodied body, a purely virtual data double that determines whether a person can cross a border, access credit, a job or a concert (Haggerty & Ericson, 2000: 611), without the individual often having knowledge or control over this virtual "self" on which decisions are based. There are some initiatives to rebalance this situation, and give back to the population some rights eroded by the data society. The European Data Protection Regulation, for example, incorporates the **right to an**

[22] https://www.opensocietyfoundations.org/explainers/life-quantified-society

[23] http://news.bbc.co.uk/2/hi/europe/3593895.stm

[24] https://abcnews.go.com/Technology/GadgetGuide/surgically-altered-fingerprints-woman-evade-immigration/story?id=9302505

explanation in cases where one's biometric data is used to make algorithmic decisions. Similarly, the US Equal Credit Opportunity Act obliges credit bureaus and data analytics agencies to explain how individual credit risk is determined. However, the safeguards and mechanisms for **redressing damages** caused by the misuse or mismanagement of biometric data, and their long-term consequences, are still unclear.

Literature explores how data processing impacts many areas of our lives. Thus, it has been described how the emergence of sensors and the constant collection of information on citizenship impacts on the development of autonomy, collective freedoms (assembly, demonstration, etc.) or on freedom itself. The philosopher Elizabeth Anderson, for example, defines **freedom** as the possibility of not having a fixed identity that we must move between the different spheres of our life (at work, with family, intimately, with friends, at the gym, etc.), but to move between these spheres by negotiating our values and norms and reformulating and renegotiating this identity[25]. If this is the case, and this possibility of managing our identity is part of the very definition of being free, the processes of identity fixation on which the biometric society or the "quantified self" depends, imply an important redefinition of the social values by which modern societies have been governed.

Finally, some authors have warned about the impact of data processing on the right to the **presumption of innocence**. It is difficult to reconcile the right not to have to defend oneself against accusations until they have been proven, as established in the penal frameworks of Western countries, with the way in which technologies that preemptively identify entire populations or groups, and with high false positive rates, operate.

Impact on Vulnerable Groups

Earlier we saw how biometrics can incorporate ethnic and income biases that cause false positives or errors to have a disproportionate impact on vulnerable groups. However, this impact is not only due to data quality and training issues. All over the world, at-risk groups such as migrants and asylum seekers are witnessing how the **welfare and humanitarian sector** is becoming a testing and experimentation ground for biometric data. Organizations such as the United Nations, Oxfam or the Red Cross have been testing these systems with vulnerable groups due, according to these same organizations, to pressure from donors and the existence of weak (or outright undemocratic) regulatory environments in some recipient countries. In some cases, moreover, refusing to hand over biometric data means giving up access to humanitarian protection, without alternatives or the possibility of validating rights and consequences[26].

[25] https://www.newyorker.com/magazine/2019/01/07/the-philosopher-redefining-equality

[26] https://reliefweb.int/report/world/biometrics-humanitarian-sector

Thus, for example, the United Nations World Food Program uses iris scans with refugees in Syrian camps who want to use food vouchers, and centralizes the information in the SCOPE system. The Red Cross has a program called Trace the Face to reunify families that relies on biometric databases of refugees. The same organization's High Commissioner for Refugees (UNHCR) uses biometrics to execute transfers of money, food or access to shelter[27] through its Population Registration and Identity Management EcoSystem (PRIMES), used at more than 200 locations in 43 countries, and believed to hold data on more than 4 million refugees, from whom any interaction with the organization's systems is recorded, generating long-term profiles (or "data doubles"). In other cases, organizations such as the European Union Development Fund or USAID have financed the biometric registration of entire populations in countries such as Somalia or Kenya, without paying attention to the risks denounced by different organizations for their impact on human rights, and the lack of guarantees on the management of this data or the economic costs[28]. Finally, countries such as the European Union or the USA require recording biometric data of all those who enter their borders without being citizens, an extreme measure that is not required for residents.

The use of biometric data in these contexts not only has a disproportionate impact on vulnerable groups, but also calls into question some of the basic principles of data protection, such as the right to understand the consequences of data transfer and free consent. Not only because both the United Nations and the European Union Agency for Fundamental Rights have pointed out that migrants do not receive sufficient information about their rights[29], but also because who can refuse to give their data if their livelihood, their opportunities or their lives depend on it? In the known cases of collective refusals to provide this data, this has resulted in the exclusion of these groups from the services to which they aspired[30].

The neglect of these risks has already had consequences on specific groups. For months, UNHCR has been assisting Rohingya Muslims fleeing persecution in Myanmar. In the camps in Bangladesh, all refugees over the age of five are registered with their fingerprints and facial features, in addition to all their personal data, to be entered into PRIMES. In this case, UNHCR shares this data with the Bangladeshi government, which controls their status if they want to leave the camps. But in November 2017, Bangladesh signed a refugee repatriation agreement with Myanmar that will be implemented with the support of biometric data collected by UNHCR. People who provided their bodies to escape

[27] https://www.wired.com/story/refugees-but-on-the-blockchain/

[28] http://www.privacyinternational.org/sites/default/files/2017-12/Aiding%20Surveillance.pdf

[29] https://fra.europa.eu/en/publication/2018/biometrics-rights-protection

[30] https://www.news24.com/Africa/News/burundi-refugees-refuse-biometric-registration-in-drc-20171207

persecution may now see that same data used to return them to the persecuting country[31].

Within the migrant population, the case of **minors** is even more serious, since in humanitarian contexts biometric data is collected from children as young as five years old, something that is not allowed in Western countries. In addition, and as exemplified in the case of the Rohingya, in these contexts there is a proliferation of "function creep": the use of data or technologies for functions beyond those initially defined, generating an erosion of privacy and fundamental rights. It is difficult to justify the testing of biometrics on groups such as migrants or children, since the sum of vulnerability, dictatorial or weak regulatory environments and scenarios of great violence, would seem to justify an approach based on protection and precaution, and the deployment of technologies only after their social and economic impacts have been indisputably proven. Currently, the mainstream approach is the opposite.

Efficiency and Effectiveness

The last issue to highlight in this critical review of the use of biometrics as a proxy for identity is that of efficiency and effectiveness. Unfortunately, we do not have rigorous studies that incorporate alternative or **cost-benefit** analyses prior to the incorporation of biometric systems, basically because they have not been done. In addition, as mentioned above, the opacity of the industry regarding false positives and the algorithms used makes it difficult to evaluate these systems in a rigorous manner. We also do not have impact studies in this area, despite the fact that they are mandatory in the European Union whenever specially protected data such as physiological or behavioral data are processed or used for profiling.

However, there are some worrying figures if we approach this technology from the point of view of one of its great promises: the fight against **fraud**. One of the first identity verification systems based on iris reading was implemented precisely by UNHCR in a Middle Eastern country, Afghanistan. The system was intended to prevent fraud in applications for repatriation assistance offered by the United Nations from 2002 onwards, by identifying people who tried to use the system twice. According to the organization's data, the biometric system identified 1,000 potentially fraudulent uses among the 202,000 people processed, or less than 0.5% fraud attempts. Apparently, another 20,000 people would have attempted to subvert the system, but had been previously identified by non-biometric triage systems. In the case of the Spanish employment system described above, the fraud figures would be less than 1%, a figure consistent with other global comparative studies on welfare benefit fraud rates (0.8% in Great Britain, 2% in Ireland according to Harrikari and Rauhala, 2016: 50) or 2.67% in unemployment

[31] https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh

benefits in the USA[32], figures which should be noted do not detail whether the fraud is due to misuse of identities or other voluntary or involuntary errors.

With fraud rates below 3%, it is difficult to justify the incorporation of biometric systems. Not only because of their cost (both acquisition and maintenance), but also because the incorporation of biometric identification processes in any administrative process involves a real **digital transformation** process that implies an enormous training and organizational redefinition effort, which is not only costly in economic terms. In the process of incorporating biometrics, not only cost and impact studies are lacking, but also the development of implementation plans that incorporate training, organizational and technological needs. Often the first step in the incorporation of biometric systems is the acquisition of software and hardware, when in fact this should be the last step, after the definition of technical needs and precautions, staff training, administrative reorganization and the development of protocols for use.

CONCLUSION

For someone versed in security and technology issues, it is difficult to understand why biometrics have been consolidating as an identification solution. The risks linked to security, its impact on fundamental rights and doubts about its effectiveness would justify a much more cautious approach to these systems, especially because there are alternatives for identity verification that offer better levels of security and lower risks, from the use of combinations of external identifiers along with passwords, or the implementation of secure document verification systems through blockchain, a technology that allows to increase the security and verifiability of identification processes without the need to incorporate biometric data. Biometrics, then, may be an optimal solution in specific cases, but we do not have data to justify its standardization as a proxy for identities.

However, the current debate around this technology seems to be resistant to figures and facts. Probably the security anxieties of this 21st century, together with the fascination with all things technological that seems to permeate today's environment, do not provide the ideal context for the promotion of a conversation based on reality. However, the very high cost of biometric systems in terms of rights and democratic guarantees, as well as the existence of alternatives with better results and lower risks, makes it necessary to put these arguments on the table.

[32] https://www.dol.gov/general/maps/data

ACKNOWLEDGEMENTS

Project team: Publications Library - Tech and Rights Series
Project Lead & Research Director: Dr. Gemma Galdon-Clavell, Founder of Eticas
Writing and Research: Marta Burgos, Ethics and Technology Researcher at Eticas

REFERENCES

BBC News (April 2, 2004) *Sweden refugees mutilate fingers.* Available from http://news.bbc.co.uk/2/hi/europe/3593895.stm (Accessed September 2022)

Big Brother Watch Team (May 2018) *Face off. The lawless growth of facial recognition in UK policing.* Available from *https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf* (Accessed September 2022)

Buolamwini, J. and Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, in *Proceedings of Machine Learning Research* 81:77-91 Available from https://proceedings.mlr.press/v81/buolamwini18a.html (Accessed September 2022)

Burt, C. (March 5, 2018). *Uganda launches biometric program to verify identities of 1 million refugees.* Available from https://www.biometricupdate.com/201803/uganda-launches-biometric-program-to-verify-identities-of-1-million-refugees (Accessed September 2022)

CODE OF PRACTICE. On the acquisition, use, retention and disposal of biometric data for justice and community safety purposes in Scotland. (n.d.). Available from https://www.gov.scot/binaries/content/documents/govscot/publications/consultation-paper/2018/07/consultation-enhanced-oversight-biometric-data-justice-community-safety-purposes/documents/00538315-pdf/00538315-pdf/govscot%3Adocument/?inline=true (Accessed November 2022)

El País Retina (November 20, 2018). *Una cara impresa en 3D consigue desbloquear casi todos los móviles.* Available from

https://elpais.com/retina/2018/12/19/innovacion/1545217900_127070.html (Accessed September 2022)

E&T editorial staff (November 16, 2022) *Scotland publishes first Code of Practice for use of biometric data*. Available from https://eandt.theiet.org/content/articles/2022/11/scotland-publishes-first-code-of-practice-for-the-use-of-biometric-data/ (Accessed November 2022)

European Union Agency for Fundamental Rights, (2018) Under watchful eyes : biometrics, EU IT systems and fundamental rights, Publications Office, 2018. Available from https://data.europa.eu/doi/10.2811/136698

Gardham, D. (April 5, 2009) *Airport face scanners´cannot tell the difference between Osama bin Laden and Winona Ryder.* Available from *https://www.telegraph.co.uk/news/uknews/law-and-order/5110402/Airport-face-scanners-cannot-tell-the-difference-between-Osama-bin-Laden-and-Winona-Ryder.html* (Accessed September 2022)

Garvie, C.; Bedoya, A. and Frankle, J. (October 18, 2016). *The perpetual line-up. Unregulated police face recognition in America.* Available from https://www.perpetuallineup.org/ (Accessed September 2022)

Gorospe, P. (November 11, 2018) *Huellas dactilares para acceder a ayudas sociales en País Vasco.* Available from https://elpais.com/sociedad/2018/11/09/actualidad/1541758148_321672.html (Accessed September 2022)

Hay Newman, L. (August 19, 2016) *Hackers trick Facial-Recognition Logins with photos from facebook (what else?)* Available from *https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/* (Accessed September 2022)

Heller, N. (December 31, 2018) *The philosopher redefining equality.* Available from https://www.newyorker.com/magazine/2019/01/07/the-philosopher-redefining-equality (Accessed September 2022)

Hempel, J. (March 14, 2018) *How refugees are helping create blockchain´s brand new world.* Available from https://www.wired.com/story/refugees-but-on-the-blockchain/ (Accessed September 2022)

Heussner, KM. (December 10, 2009) *Surgically altered fingerprints help woman evade immigration.* Available from

https://abcnews.go.com/Technology/GadgetGuide/surgically-altered-fingerprints-woman-evade-immigration/story?id=9302505 (Accessed September 2022)

Hosein, G. and Nyst, C. (October 2013) Aiding Surveillance. An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries. Available from https://www.privacyinternational.org/sites/default/files/2017-12/Aiding%20Surveillance.pdf (Accessed September 2022)

Martí, A. (February 18, 2016) *Cinco minutos, plastilina y un molde; con eso bastó para falsear mi huella y desbloquear mi móvil.* Available from https://www.xataka.com/seguridad/cinco-minutos-plastilina-y-un-molde-con-eso-basto-para-falsear-mi-huella-y-desbloquear-mi-movil (Accessed September 2022)

Media Team. (May 23, 2017) *Die Sendung mit dem Chaos-Iris Scanner im Samsung Galaxy* Available from https://media.ccc.de/v/biometrie-s8-iris-fun (Accessed September 2022)

News 24 (December 7, 2017) *Burundi refugees refuse "biometric" registration in DRC.*Available from https://www.news24.com/News24/burundi-refugees-refuse-biometric-registration-in-drc-20171207 (Accessed September 2022)

Nieva, R. (July 1, 2015) *Google apologizes for algorithm mistakenly calling black people "gorillas"* Available from *https://www.cnet.com/tech/services-and-software/google-apologizes-for-algorithm-mistakenly-calling-black-people-gorillas/* (Accessed September 2022)

Nyst, C.; Rahman, Z. and Verhaert, P. (April 5, 2018). *Biometrics in the Humanitarian Sector,* Oxfam the Engine Room. https://reliefweb.int/report/world/biometrics-humanitarian-sector (Accessed September 2022)

Open Society Foundations Team (May 2019) *Life in Quantified Society.* Available from *https://www.opensocietyfoundations.org/explainers/life-quantified-society* (Accessed September 2022)

Sarabia, D. (November 19, 2018) *Llegan las huellas dáctilares maestras: inteligencia artificial para desbloquear cualquier teléfono.* Available from https://www.eldiario.es/tecnologia/Llegan-dactilares-inteligencia-artificial-desbloquear_0_837466910.html (Accessed September 2022)

Shoreshy, K. (September 25, 2015) *UAB research finds automated voice imitation can fool humans and machines.* Available from https://www.uab.edu/news/research/item/6532-uab-research-finds-automated-voice-imitation-can-fool-humans-and-machines (Accesed September 2022)

Sierra, M. (September 16, 2015) *Anthropometric Cards: The "Gypsy" under liberal law*. Available from https://paradojas.hypotheses.org/1008 (Accessed November 2022)

Sinha, A. and Kodali, S. (November 5, 2018) *(Updated) Information Security Practice of Aadhaar (or lack thereof): A documentation of public availability of Aadhaar Numbers with sensitive personal financial information* Available from *https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1* (Accesed September 2022)

Snow, J. (July 26, 2018) *Amazon´s Face Recognition Falsely Matched 28 Members of Congress With Mugshots* Available from https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28 (Accessed September 2022)

U.S Department of Labor. *Unemployment Insurance Payment Accuracy Datasets.* Available from https://www.dol.gov/agencies/eta/unemployment-insurance-payment-accuracy/data (Accessed September 2022)

Tejada, M. (May 20, 2022) *Lanbide cierra la puerta al uso obligatorio de la huella digital para evitar el fraude de la RGI.* Available from https://www.diariovasco.com/gipuzkoa/lanbide-cierra-uso-huella-digital-rgi-20220520212347-nt.html (Accessed September 2022)

Thomas. E. (March 12, 2018) *Tagged, tracked and in danger: how the Rohingya got caught in the UN´s risky biometric database.* Available from https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh (Accessed September 2022)

Yadav, A. (December 15, 2012) *To pass biometric identification, apply Vaseline or Boroplus on fingers overnight.* Available from https://www.thehindu.com/opinion/op-ed/To-pass-biometric-identification-apply-Vaseline-or-Boroplus-on-fingers-overnight/article12450793.ece (Accessed September 2022)