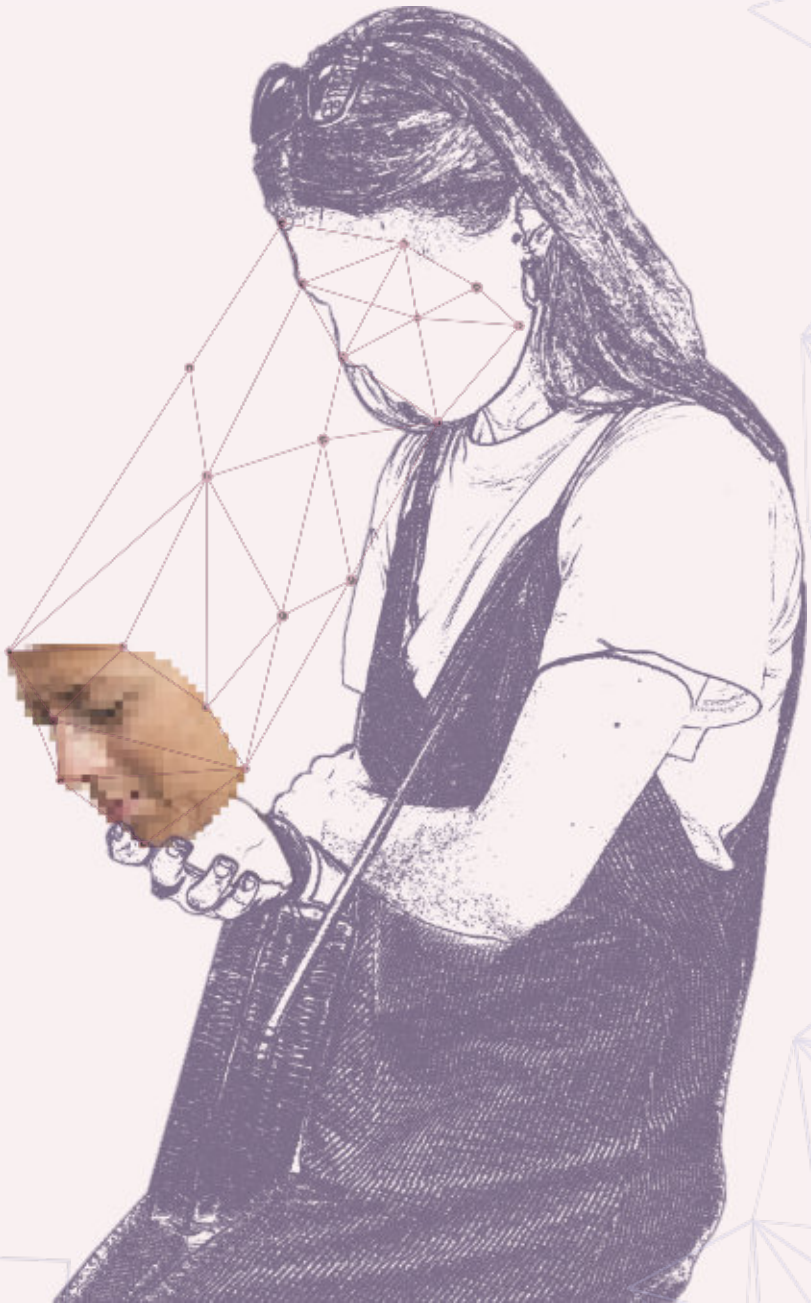
# YOUR DIGITAL SELF

## Discovering narratives on identity and biometrics in Latin America: The case of Argentina, Brazil, Colombia and Mexico



APC
por los Derechos Civiles

Asociación por los Derechos Civiles


April 2019
https://adc.org.ar

This report was prepared as part of a project supported by Ford Foundation. 


InterletLab (Brazil), Fundación Karisma (Colombia) and Red en Defensa de los Derechos Digitales (Mexico) have contributed to the research done for this work.

The document *Your digital you. Discovering narratives on identity and biometrics in Latin America: The case of Argentina, Brazil, Colombia and Mexico* is for public dissemination and has no commercial purpose.

# Executive Summary

Biometric technologies have permeated people's daily lives, being promoted by States as the infallible solution to the structural problems faced by society. In this research, we will go deeper in the analysis of the current situations faced by Argentina, Brazil, Colombia and Mexico regarding the narratives on people's identity and their relationship with the implementation of technologies which collect, store and process biometric data.

By studying legal frameworks and the public policies promoted, we will describe the impact that biometric technology may have on the exercise of rights. Its impact affects individual rights such as the right to privacy and freedom of speech, assembly and association, as well as collective rights, such as the rights to health, education and social security.

The relationship between identity and people, as something that the State is entitled to manage, unveils a logic of control where public institutions govern the population as resources. This becomes more conspicuous when the provision of social benefits or welfare schemes are conditioned by the submission of biometric data without any other alternatives, deepening social inequality further.

The legal analysis is complemented with an examination of various case studies in each country, which give us an overview of the reasoning behind the systems promoted by State institutions. Finally, we conclude this report with a series of recommendations designed to pave the way for the development of public policies based on the respect and safeguard of fundamental rights.

# Table of contents

# Your Digital Self

## Discovering narratives on identity and biometrics in Latin America*

## I. Introduction

Establishing an exact date on which we began to assign ourselves names can be tricky. However, we may argue that the development and consolidation of languages, the invention of professions and private property –in parallel with the growth of communities as they developed into societies– made it necessary to assign a characteristic to ourselves so that we can interact more easily and differentiate from one another. Even without noticing it, this characteristic that we carry every day, despite its actual intangibility, can shape various aspects of our lives regarding the way we relate and interact within society. A name, generally given to us when we are born, sets off a chain reaction throughout our lives and shapes the perspective through which we observe and experience the actions and decisions that we are driven by.

When we read or hear a name, we automatically and implicitly "begin to assign it different characteristics and, without noticing it, pass judgments which are not related to the actual abilities and aptitudes of their bearers", explains María Konnikova.[1]

The development and evolution of modern societies, which are growing more complex in terms of their geographical expansion and growing populations, have reinforced the idea that our names are an irrevocable part of our identities.

However, in the attempt to gain greater control over people, a new way of identification would begin to perfect itself. The use of biological, morphological or behavioral traits helps obtain a digital template that can be assigned to any human being in order to uniquely recognize them.

In the last two decades, the number of private sector companies that develop technology using biometric data and the number of States which have implemented said technology in various spheres of society have grown significantly.

---

* This document was drafted by **Leandro Ucciferri**, public policy analyst, lawyer and researcher at Asociación por los Derechos Civiles (ADC), with contributions from the following countries: **Dennys Antonialli** and **Maria Luciano** from InternetLab for Brazil; **Juan Diego Castañeda**, **Lucía Camacho** and **Joan López** from Fundación Karisma for Colombia; and **Santiago Narváez** from Red en Defensa de los Derechos Digitales (R3D) for Mexico. Cover design and layout by Leandro Ucciferri. https://adcdigital.org.ar|https://adc.org.ar

[1] Konnikova, Maria, "Why Your Name Matters", The New Yorker, December 19, 2013, available at https://www.newyorker.com/tech/annals-of-technology/why-your-name-matters

For the last five years, the *Asociación por los Derechos Civiles* (ADC) has been working on the monitoring, analysis and criticism of public policies that naturalize and systematize the identification of individuals using biometric technologies, given their potential interference with fundamental rights, in particular the right to privacy and freedom of speech.

By the end of 2016, under the Internet Governance Forum (IGF) held in Guadalajara, Mexico, we organized an event where we invited a group of experts from different countries with the view of sharing initiatives and policies involving the implementation of biometric technologies. The workshop allowed us to understand, mainly through the lenses of civil society, the current situation in countries such as Peru, Chile, Mexico, Colombia, Brazil, India, Paraguay, Canada, United Kingdom, United States and Poland, and how this matter is dealt with in different contexts.

In May 2017, based on this background experience, we published our first regional report, which describes the public policies and initiatives implemented in Latin America for the identification of people using biometric technology. This first report was made possible thanks to the contributions of professionals and various organizations located in Chile, Brazil, Colombia, Mexico, Paraguay, Peru and Venezuela.[2]

After this initial exploration we concluded that, in general, public policies designed to implement some type of biometric data are carried out with little or no transparency towards the public. On top of that, there is a lack of information on the technologies and mechanisms used for the collection, analysis and processing of biometric data; the scope of the policies; the actors with whom this data is shared and those who have access to it. All of this occurs within a context where legal frameworks are insufficient for the adequate treatment of the biometric data used and the advances of identification policies.

In this report we examine more closely the situation in Argentina, Brazil, Colombia and Mexico in order to help achieve a greater transparency in public policies and initiatives designed to implement identification systems using biometric technology. At the same time, this report strives to deepen the analysis of the national legal frameworks that said policies are based upon and compare the state narratives used to justify them.

This report was made possible thanks to the work done by the organizations Internet Lab in Brazil, Fundación Karisma in Colombia, and Red en Defensa de los Derechos Digitales (R3D) in Mexico. All of them collaborated with ADC by providing information of their countries' current situations, resulting in the elaboration of joint conclusions drawn to give an account of the urgent issues posed by this issue.

The report unfolds as follows: in the second section, we analyze how countries address the definitions of biometrics and biometric data, explaining the need to narrow down their definition for the development of public policies. In the third section, we explore the legal frameworks of each country and describe the legal scenarios underlying the narratives on identity and the implementation of biometric technology. In the fourth section, we provide details of some case studies that have become landmark cases in each country, so as to shed light on how biometric data is used in state policies.

Finally, we provide information on the trends displayed by the four countries under analysis and the shortcomings found in their narratives and legal frameworks. Based on this information, we propose a number of recommendations to guide the development of public policies involving the use of biometrics.

## II. Comparing concepts

The definition of what we understand by biometrics has been the result of a series of debates regarding the

[2] ADC, "Cuantificando identidades en América Latina", May 2017, available at https://adcdigital.org.ar/portfolio/cuantificando-identidades-en-america-latina/

different meanings ascribed to it by different professions.[3]

The origin of the word biometrics stems from two terms from the Greek language: *bio*, life and *metron*, measurement or the act of measuring. In its most traditional definition, biometrics refers to the statistical and mathematical analysis of phenomena and biological observations, i.e., life measurements.

Biometric technologies make it possible to collect, store and process biometric information of a person including their biological, morphological and behavioral characteristics. Once collected and processed, these features or characteristics are then converted into a matrix or digital template that can be read by computers and compared to other matrixes and templates, generally of the same type. Once these digital templates are matched to a person's profile, they can be used to identify[4] or verify[5] their identity.

The biometric identification or verification process is based on statistics, not on a simple "yes or no" answer. On the contrary, it consists in a process of probabilities which involves striking a balance between error rates based on the results one wishes to obtain with the identification system. This process results in a more or less likely identification.

Since error rates are set by technology developers, there is a multiplicity of factors that may render the system a tool capable of affecting human rights, for example, by discriminating against vulnerable groups given this technology is more prone to misidentify persons who are not white.

In this sense, it is necessary to tell the difference between the concepts of "biometrics", "biometric technologies" and "biometric data" to avoid using these terms as one and the same, which would be a mistake with potential legal consequences, as we shall see later in this section.[6]

It is essential to analyze what is understood by biometrics in different countries and socio-economic contexts, taking into account that the range of data contained in a biometric system determines the way said system affects various fundamental rights.

In addition, narrowing down the scope of these concepts would allow enforcing laws that respect the legality principle and guarantee an agenda to comply with minimum standards on necessity and proportionality.

No country under analysis in this report has passed a law through its legislative body providing a clear and detailed definition of the concepts mentioned before.

In Argentina, the term biometrics linked to the identification of persons began to appear in various decrees and resolutions in 2011 when the Federal System of Biometric Identification for Security (SIBIOS) was established. This System was a point of inflection regarding the introduction of biometric technology in different public agencies, marking a before and after in the way the State addresses the identity of persons.[7]

Notwithstanding, Argentina was a pioneer in the use of fingerprints for the identification of people since the end of the 19th century, specifically through the work done by Juan Vucetich (1858-1925) in the Police Department of the Buenos Aires Province, who exported his ideas to the rest of Latin America and Europe. Hence, the term

[3] See https://bib.irb.hr/datoteka/425577.IJCSI_SchattenBacaCubrilo2009.pdf; and https://www.merriam-webster.com/dictionary/biometry:
[4] Identification refers to the comparison of a person's biometric data with those of a given number of persons stored in a database. In other words, it means comparing a person's data with that of an entire group represented as *1:n*.
[5] Verification refers to the process of corroborating that a person's biometric data matches previously enrolled data in the database, i.e., it is a *1:1* comparison.
[6] Catherine Jasserand, "Avoiding Terminological Confusion Between the Notions of 'Biometrics' and 'Biometric Data': An Investigation Into the Meanings of the Terms From a European Data Protection and a Scientific Perspective", September 1, 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230339
[7] Catherine Jasserand, "Avoiding Terminological Confusion Between the Notions of 'Biometrics' and 'Biometric Data': An Investigation Into the Meanings of the Terms From a European Data Protection and a Scientific Perspective", September 1, 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230339

dactyloscopy has been used even before 2011.[8]

The first regulation that used this concept was decree-law 17.671 on "Identification, registration and classification of national manpower" enforced under the military dictatorship of Juan Carlos Onganía in 1968. Article 9 allows for the use of "photographs" and "dactyloscopy imprints" for the identification of individuals. Even though it makes sense that this decree-law originally did not make any reference to biometrics per se, it is worth highlighting that it has never been amended to expressly incorporate the term or to provide a definition of "biometric technology" or "biometric data".

Law 25.326 on Data Protection does not mention the term "biometrics" or "biometric data" either. However, in January 2019, the Access to Public Information Agency (AAIP, in Spanish), an agency in charge of the enforcement of said law, issued Decree 4/19[9], which sets forth the need to clarify the scope of the term pursuant to the law on personal data currently in force in the country, considering that most modern legal frameworks in this field are already contemplating it and, thus, it is necessary to follow international trends.

In this sense, the AAIP establishes that "biometric data refers to personal data obtained by means of a specific technical treatment involving physical, physiological and behavioral characteristics of a human being which allow for their single identification" and that such data shall be deemed sensitive[10] when its use is potentially discriminatory against the data subject.[11]

In Brazil, law 13.709 on protection of personal data, passed in 2018, places biometric data under the classification of sensitive personal data[12], which is linked to greater processing restrictions such as the need for obtaining the data subject's consent (art. 11).

In Brazilian law, there is no express definition for 'biometrics' or 'biometric data', even though these concepts are mentioned by some of the regulations established by identification systems.

Given that the Electoral Court uses this technology for identifying voters by means of their fingerprints, the Supreme Electoral Court has a glossary of terms including concepts such as 'biometrics', which is defined as "a technology which allows identifying a person based on their unique biological characteristics, i.e., body parts having special features such as the iris, retina, digital prints, voice, the shape of the face and hands."[13]

On the other hand, "biometric identification" is defined as "the identification system which collects biometric data (digital prints and photographs) of voters to check they are properly registered in the election roll and prevent them from casting more than one vote".[14]

In Colombia, the data protection law classifies data as sensitive when it has the potential of affecting a person's privacy or discriminating[15] them and also contemplates data related to a person's health, sex life and biometric information. The Constitutional Court and the Data Protection Office (DPO)[16] have considered that the sensitivity

[8] Fingerprinting is a discipline based on the study and comparison of fingerprints for the identification of individuals. The term was first recorded in an Official Gazette in 1912, available at https://www.boletinoficial.gob.ar/#!DetalleNormaBusquedaAvanzada/11370722/19120903

[9] Available at https://www.boletinoficial.gob.ar/#!DetalleNormaBusquedaAvanzada/200224/20190116

[10] Article 2 of Law 25.326 sets forth that sensitive data refers to "personal data which reveals racial and ethnic origin, political inclinations, religious, philosophical or moral beliefs, trade union membership and information relative to health or sex life".

[11] A detailed analysis on biometrics and personal data under the microscope of relevant current legislation can be found in: https://adcdigital.org.ar/portfolio/desafios-la-biometria-la-proteccion-los-datos-personales/ (ADC, 2017)

[12] Article 5, section II of Law 13.709 sets forth that sensitive personal data refers to data revealing racial or ethnic origin, religious beliefs, political inclinations, membership of a trade union or of a religious, philosophical or political organization; as well as data relative to a person's health or sex life and the genetic or biometric data of a natural person.

[13] Available at http://www.tse.jus.br/eleitor/glossario/termos-iniciados-com-a-letra-b#biometria

[14] Available at http://www.tse.jus.br/eleitor/glossario/termos-iniciados-com-a-letra-i#identificacao-biometrica

[15] Law 1581, 2012, "article 5. Sensitive Data. For the purposes of this law, sensitive data shall refer to data affecting the Holder's privacy; data whose undue use may discriminate its holder, such as data revealing racial or ethnic origin, political inclinations, religious or philosophical beliefs, membership of trade unions, social or human rights organizations or data which promotes the interests of some political party or which promotes the rights and freedoms of opposing political parties, as well as data relative to an individual's health or sex life and biometric data".

[16] The Data Protection Office of the Industry and Commerce Superintendency (SIC, in Spanish) is the authority in charge of monitoring,

of the data lies in its connection to the privacy of individuals[17].

Despite this explicit reference, the law does not provide a specific definition of biometric data. However, the Data Protection Office has drafted a general definition. Essentially, biometric data is associated with some physical characteristic which makes a person unique and which permits identifying one individual from the rest.[18] Despite the fact that this definition may involve many types of biometric data, the Constitutional Court and the Data Protection Office have –as far as we know– settled cases only involving fingerprints, photographs or videos.

There is an exception regarding face pictures, as the DPO considers these are personal data but not necessarily biometric and, therefore, sensitive. In those cases where the administration of a building had taken pictures of persons entering the site or installed a surveillance system,[19] the data so obtained was deemed to be private personal data. This classification stems from another line of case law of the Constitutional Court according to which information is classified based on how it is disseminated.[20]

The Data Protection Office decided that a photograph or video would be classified as biometric, and therefore sensitive, only when some technique is used to "extract some special facial feature".[21] This line of interpretation casts doubts as to the type of technique and connection with other databases needed to change the classification of data to biometric, as it would require a repository for contrasting the results of the measurements obtained from the facial features, an aspect which has not been addressed by the DPO.

After reviewing some citizens' requests for information submitted to the DPO[22], we noticed the agency defined biometrics based upon a classification of data into different types. The answers provided by the Superintendency show that it has used the definition adopted by the International Telecommunications Union (ITU), which refers to biometric data as "automated methods used to accurately recognize individuals based on distinguishing physiological and/or behavioral characteristics".[23]

Besides, the Superintendency defines biometrics as the "security technology based on the recognition of a physical and unique trait of an individual, such as fingerprints, which permits distinguishing one human being from the next".[24]

In Mexico, the legal data protection framework does not contemplate the concepts of "biometric identification", "biometric data" or "biometrics". However, the National Institute of Transparency, Access to Information and Data Protection (INAI, in Spanish) published a guide for the treatment of biometric data in March 2018.[25]

The guide includes a glossary of terms where it defines biometrics as "a recognition system for identifying

---

inspecting and controlling the treatment of personal data in Colombia within the private sector (article 19, Law 1581, 2012).

[17] Court ruling C-1011 of 2008 cites a passage occasionally used by the Constitutional Court and the Data Protection Office regarding the definition of sensitive data: "sensitive data is related to, among other aspects, a person's sexual orientation, religious and political beliefs. In these cases, such data is deemed to belong to the sphere of the right to privacy". *Cf.* Constitutional Court, ruling C-1011, October 16, 2008, M.P. Jaime Córdoba Triviño.

[18] Industry and Commerce Superintendency, Data Protection Office, concepts C-2014-273515 and C-2018-29956.

[19] Industry and Commerce Superintendency, Data Protection Office, Resolution N. 60460, 2017; Resolution N. 43530, 2018; Resolution N. 55405, 2018.

[20] Cf. Constitutional Court, ruling C-1011, October 16, 2008, M.P. Jaime Córdoba Triviño, "Regarding this personal data, case law proposes two classification types. The first one involves the level of protection afforded to the right to privacy and divides data into personal and impersonal information, the latter being defined as data which does not meet the requirements previously mentioned. (…) The second classification divides data based on its qualitative nature and the extent to which it may be disseminated. Thus, information may be further classified into public, semi-private, private and confidential". These parallel classifications were also upheld by ruling C-748 of 2011.

[21] Industry and Commerce Superintendency, Data Protection Office, Resolution N. 60460, 2017, available at http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/201706046resolucion.pdf

[22] Requests for information: N. 13-2733515, 2014, N. 0171259, 2018, N. 0297406, 2018, and N. 0299565, 2018.

[23] Industry and Commerce Superintendency, Legal Office, request for information N. 13-2733515, 2014.

[24] Ibid.

[25] INAI. Guide on treatment of biometric data. March, 2018. Available at http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf

persons based on their biometric data'; biometric data as "physical, physiological, behavioral and personality traits of a measurable nature which belong to a single person"; and biometric recognition as "identification or verification of a person's identity based on biometric template comparison". Besides, it defines biometric templates as "the alphanumeric representation of information extracted from one or more biometric samples".

INAI cites the following sources for the above definitions: Opinion 3/2012 issued by Article 29 Working Party and the report Privacy & Biometrics. Building a conceptual foundation (2006) from the subcommittee on biometrics under the National Science and Technology Council of the United States.

INAI establishes that sometimes biometric data cannot be classified as personal data. Based on Mexican laws, two conditions must be fulfilled for this to happen: first, data must belong to a physical person, and second, it must identify or facilitate the identification of the data subject. Only then will it be classified as personal data.

INAI states that "even though there is biometric data to identify a person, such as the face of a known individual, most data requires additional information processing for its subject to be identified (…) as is the case with fingerprints". It goes on to add that "data will not be considered personal when it is not enrolled in a biometric system and when it cannot be attributed to a single person or compared with other samples".

Likewise, the guide establishes that not all biometric data should be automatically considered sensitive under data protection laws but must be analyzed on a case by case basis. Data may be considered sensitive when it is a part of a person's most private sphere; when its undue use results in discrimination against its subject; or when its illegal use poses a great risk for them. In this sense, INAI provides examples with the use of the iris and fingerprints.

We may therefore conclude that the introduction of biometrics has not been properly limited in the countries under analysis. Even though only Brazil and Colombia make reference to biometric data in their laws on data protection, the term is used only to refer to sensitive data, failing to specify the concept and determine what type of biometric information they refer to. The inaccurate use of the concepts referred to impacts the way biometric technology and biometric data are used, as will be shown in the following sections.

## III. Biometrics and identity: guarding the gateway to your rights

In this section, we go deeper into the socio-political context and background situation of the four countries, focusing on the legal frameworks underlying public policies on the identity of individuals and the use of biometric technologies.

### I. Argentina

In June 1966, the military junta, self-proclaimed "Argentine Revolution", seized power through a State coup. Once in control, it enacted a ten-article Statute that prevailed over the National Constitution. Article 5 granted the president almost all[26] the legislative powers typically conferred to Congress.

In a context where institutions were not working as originally designed and where citizen participation was nonexistent, Decree-Law 17.671 was passed for the "identification, registration and classification of national manpower". The law establishes the functions of the National Registry of Persons (RENAPER, in Spanish) for procedures followed for the identification of people domiciled in Argentine territory and of all Argentines no matter their whereabouts.

Following Vucetich's advancements, the systematic use of fingerprints and the introduction of the National Identity Document (DNI, in Spanish), Argentines gradually naturalized its use. Citizen's relationship with the State

[26] "Except for those under articles 45, 51 and 52 on impeachment cases involving judges of national courts".

was built under these foundations, which later encompassed private players too. Even RENAPER promotes the issuance of DNIs under the motto "the entrance door to your rights", in reference to the idea that individuals need their DNI to file requests with the State. In other words, a person exists before the eyes of the State as long as they hold an identification number.


*RENAPER's mobile center for the issuance of DNI.*

The identification system of the population is based on laws which ultimately lie on the ideology and rationale of the military dictatorship, a situation that has never been questioned neither from political nor legal grounds.

The formal defects of the applicable law are worth highlighting, but the way said law handles the identity of persons is even more revealing. The very same title refers to persons as "manpower", which reflects on the conception of the human being itself, who is seen by State institutions as an available asset or resource that can be controlled and managed.

During the five decades after its enactment, Decree-Law 17.671 was used by different democratic governments as the basis to further develop identification systems. Article 9 was invoked to justify the legality of biometric technologies, advancing on the regulation of such technologies almost exclusively through decrees and resolutions.

Article 9 sets out that, for the purposes of identifying a person, RENAPER must collect "birth certificate, photos, fingerprints, description of physical traits, individual data and blood type and factor."

Thus, by means of Decree 1501 of 2009, RENAPER, a decentralized agency under the Ministry of Interior, authorized the use of biometric technology for issuing DNIs.[27] Later, Resolution 1474 of 2012 introduced the biometric passport.[28] The reasoning behind both measures was the authenticity of the documents issued.

In November 2011, by means of Decree 1766[29], the national government created SIBIOS, the greatest biometric

[27] Decree 1501, 2009, RENAPER, Ministry of the Interior.
[28] Resolution 1474, 2002, RENAPER, Ministry of the Interior.
[29] Decree 1766, 2011, Ministry of Security.

database in the country, under the Ministry of Security. Article 1 of the decree establishes that the goal of the System is to "provide a centralized information service regarding patronymic and biological registries to contribute to the accurate and timely identification of persons and footprints, optimize scientific criminal investigations and improve security measures".

After a request for access to public information made by ADC in 2016 and 2017, the Ministry of Security established that the biometric data stored by SIBIOS includes fingerprints, palm prints and face records.

Since existing databases were incomplete before Decree 1766/11 was enacted and in order to keep records of the more than 40 million inhabitants, RENAPER became the main source for SIBIOS' database, as it is the authority in charge of issuing DNIs and passports.

The technology behind this System was acquired from two companies: the French Morpho Safran (currently known as IDEMIA) on the part of the Ministry of Security and the Cuban DATYS on the part of the Ministry of Interior.[30]

Furthermore, since SIBIOS aims to be a federal database, a scheme was implemented so that each province can use the System and contribute their own records. In this way, State Provinces can sign a Participation Agreement with the National State. Pursuant to this Agreement, the Superintendency of the Forensic Police of the Federal Police can file and store fingerprints (of all 10 fingers), faces, palm prints and patronymic data provided by each Provincial Police. In order to update the System, a province may file the appropriate records directly.

*Biometric fingerprint identification, Argentine Federal Police.*

Pursuant to article 3 of Decree 1766, the main users of the System are: the Argentine Federal Police, the National Gendarmerie, the Argentine Maritime Authority, the Airport Security Police, the National Registry of Persons and the National Immigration Office, apart from the provincial police departments that have signed the Participation Agreement.

At the beginning of April, 2017, Decree 243[31] was enacted to promote the incorporation to SIBIOS among "those agencies under the Executive or Judicial Power, both National and Provincial or in the City of Buenos Aires" so that they may request biometric information in real time.

[30] "The identity we can't change", ADC, 2017.
[31] Decree 243, 2017, Ministry of Security.

SIBIOS is used both for criminal and civil purposes; the former involves scientific criminal investigations, and the latter the identification of persons in events such as natural disasters or accidents. However, the number of applications is constantly growing. To perform queries on SIBIOS, users are not required to obtain a court order.

For its launch, the national government carried out a propaganda campaign under the slogan "The more we know ourselves, the more protected we are", emphasizing how certain traits of a person can help identify them without error. SIBIOS's video advertisement focuses on crime prevention and identity theft and highlights that thanks to this System "now you are yourself."[32]

Besides the databases under the Ministry of Security and the Ministry of Interior previously mentioned, there are two government initiatives which developed their own solutions; one did so within the field of taxation and the other one within social security.

In 2010, the Federal Administration of Public Revenue (AFIP, in Spanish) issued General Resolution 2811 creating the Tax Register,[33] where individuals must provide a digital record of their face, signature and fingerprints for enrollment and for obtaining a Unique Tax Identification Code (CUIT, in Spanish) and a Security Level 3 Tax Code.

The Tax Code is needed to file online requests with AFIP such as preparing affidavits, making payments, adhering to *Monotributo* (a simplified tax scheme for the self-employed) and requesting tax deregistration. This means that there is a great percentage of the population that must enroll in AFIP's database.


*ANSES ad for the program "My Print".*

In December 2014, the National Administration of Social Security (ANSES, in Spanish), by means of Resolution 648, began the enrollment process of the program "My Print", whereby retirees, pensioners and their agents were required to enroll their fingerprints in the Biometric Identification System. The goal of the program is to implement biometric technology for them to provide proof of life and receive their pensions.

The implementation of biometric technology in ANSES began with Resolution DE- N 567 of 2013. Later, the agency expanded and improved the collection, processing and use of biometric data by means of its own resolutions.

[32] SIBIOS' video advertisement is available at https://youtu.be/Pj6II4eazxE
[33] General Resolution 2811, April 24, 2010, Federal Administration of Public Revenue.

## II. Brazil

A citizen's identification is mandatory for obtaining social benefits and enjoying many rights. Since biometric data is closely associated with the concept of citizenship, collecting such data for the issuance of identity documents has never encountered fierce opposition. The identification initiatives promoted by the Brazilian Government are traditionally seen with a positive light by most of the population.[34]

Brazil has various identification systems which include more than ten different types of numbers that frequently overlap. Such is the case with the identification card ("RG"), the driver's license ("CNH"), the voting ID card[35] and the number which links Brazilians to their financial services ("CPF") and passport. Law 7.116 of 1983 established that Brazilian federal states ("Federative Units") would be responsible for issuing identification cards ("RG") containing a citizen's photograph and fingerprints[36]. This scheme resulted in decentralized information, given that the Units do not share data between them[37], which means any person may obtain a different identification in each one of the 27 states of the country.[38]


*Folha de Sao Paulo Investigation, where 9 identity cards were obtained in different Federative Units in Brazil*

Since 1997, Brazil has been trying to implement a single identification card. After two decades of various projects[39] from different parties, Law 13.444 of 2017 created the National Civil Identification. In this way, a single

[34] Kanashiro, Marta Mourão. Biometria no Brasil e o Registro de Identidade Civil: novos rumos para identificação. 2011, p. 81.
[35] In Brazil, voting is mandatory for citizens between 18 and 70 years old.
[36] The birth certificate is the only document needed to obtain the identification card. However, the issuance procedures and data processing are established by the state authority in charge of the identification of persons via administrative acts.
[37] Akiyama, Thaís Gualda Carneiro; Almeida, Veronica Eberle de; Godri, Lucina; Guarido Filho, Edson Ronaldo. Organizações e Ambiente Legal: a construção do sistema de identificação civil brasileiro. RAM, Rev. Adm. Mackenzie, 16(6), Special Edition, SÃO PAULO - SP, Nov. /Dec. 2015, p.104.
[38] In an investigation report for "Folha de Sao Paulo", a journalist was able to obtain 9 valid identification cards. Due to the lack of interoperability, the journalist obtained an identification card in Belo Horizonte with his photo and fingerprint, but using a colleague's name. Available at https://www1.folha.uol.com.br/cotidiano/2013/10/1355762-reporter-tira-carteira-de-identidade-em-9- estados.shtml
[39] The "Registro de Identidade Civil" created by President Fernando Henrique Cardoso by means of Law 9.454 of 1997 was an attempt to streamline the issuance of the identity card across Brazil. Not until 2010 were the first credentials issued during Lula's administration, but after the first 14,000 credentials were issued by Casa da Moeda, the project was abandoned and the agreement with the Casa was not

document was established which would contain civic, patronymic and biometric data, including a photograph and a chip, presumably for fraud prevention.[40]

Public officials from the Supreme Electoral Court participated in its implementation during the pilot program. They were provided with a digital version of the document in July 2018. Said document would be implemented nationwide a month later for all citizens.[41] However, not until January 2019 did government ministers of President Jair Bolsonaro reportedly resume dialogues on the initiative.[42]

The Supreme Electoral Court (TSE) has implemented biometric technology since 2003 for the issuance of voting ID cards, based on the need to "ensure a truly democratic and safer voting system", adding that biometrics casts no doubts as to the identity of each voter.[43]

It is worth highlighting that the biometric data collected by the Electoral Court –which are essential for the exercise of citizenship and voting rights– have been used and shared for other purposes, especially for criminal investigations. This has been done through technical cooperation agreements and pursuant to the terms set forth by Decree 8.789/16[44], without any transparency, public control or safety measures, all of which represents a significant violation of the rule of law.

*Electronic ballot box used for identity verification by fingerprint in Brazilian elections.*

As Law 7.444 of 1985 granted the Court legal powers to set out the instructions on the use and processing of databases of the Electoral Court (article 9), the TSE has gradually implemented biometric technology by means of administrative resolutions[45]. In September 2018, the Supreme Federal Court upheld the validity of rules authorizing the cancellation of voting IDs for people who fail to enroll their biometric data.[46]

---

renewed. In 2015, President Dilma Rousseff proposed bill 1.755/15, aimed at creating the National Civil Registry; the bill was finally passed in 2017 under Michel Temer's administration by means of Law 13.444 under the name "Identificação Civil Nacional".

[40] Available at http://www.casacivil.gov.br/central-de-conteudos/noticias/2017/maio/temer-sanciona-lei-da- identificacao-civil-nacional

[41] Available at http://www.planejamento.gov.br/assuntos/tecnologia-da-informacao/documento-nacional-de- identidade/dni-1

[42] Available at https://brasil.estadao.com.br/noticias/geral,aposta-de-moro-investigacoes-com-auxilio-de-dna- crescem-28-no-pais,70002668739

[43] Available at http://www.tse.jus.br/imprensa/noticias-tse/2014/Fevereiro/recadastramento-biometrico-e- amparado-por-lei

[44] Decree 8.789 of 2016 revolves around the exchange of databases in the federal public administration.

[45] Resolução-TSE no. 21.538/2003, no. 22.688/2007, no. 23.061/2009, no. 23.335/2011, no. 23.345/2011 and no. 23.366/2011.

[46] Supreme Federal Court, Arguição de Descumprimento de Preceito Fundamental (ADPF) 541, case reported by justice Luís Roberto Barroso, September 26, 2018. Available at http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=390875

Driver's licenses are also a valid national identification document, but they use an integrated database linked to the *Registro Nacional de Carteiras de Habilitação* (RENACH), an agency created by Law 9.503 of 1997 (Brazilian transit code). RENACH keeps a database for all the country in the National Department of Transit and other databases located in the offices of each state, which are constantly interconnected[47]. In 2017, administrative resolution 684/17 established that the issuance and renewal of licenses would require the enrollment of a photograph, fingerprints and the signature of the interested applicants.

Ultimately, data collection and processing in Brazil is governed by resolutions, provisions and ordinances, as well as by cooperation agreements and contracts. In their attempt to innovate in the legal field by creating rights, duties, sanctions and prohibitions, these regulatory acts seem to challenge the legality principle enshrined in article 5, section II of the Constitution.

## III. Colombia

"Biometrics is the ideal method for human identification", stated the National Civil Registry (RNEC)[48]. This trust in the certainty of scientific and technical methods for the verification of a person's identity based on their physical traits is influenced by our concept of the State and the way citizens access public services.

In Colombia, the process of citizens' biometric data collection started with two differentiated efforts that converged in the 21st century. First, there is the criminal database which, as was the case in other countries, was created at the beginning of the 20th century to record criminals' fingerprints, anthropometric measures and pictures.[49] Secondly, in 1934 the Department of National Identification, in its attempt to combat electoral fraud, began to provide Citizen IDs containing anthropometric data, a picture and the fingerprint of the right forefinger.[50]

In 1948, amid an institutional crisis and partisan violence, Law 89 was passed to reform the electoral system, creating an agency independent of parties to administer the elections. This law introduced the requirement to hire a foreign mission involving countries of the global North to help "decide upon the systems that must be implemented for the identification and issuance of IDs."[51]

Two years later, a Canadian mission made a series of recommendations which included the adoption of a fingerprinting system called "Henry" and the implementation of a centralized microfilmed fingerprints archive.[52] Based on the report issued by the mission, in 1951 Decree 2628 was adopted to begin printing the new IDs.[53] The consolidation process of the national identity database was made possible by means of Law 39 of 1961, which made the ID a requirement for "all the civilian, political, administrative and legal acts".[54] This Law began a process that combined the enrollment of citizenship for the purposes of claiming their rights with the collection and classification of their biometric data.

In 1970, by means of Decree 1260, the RNEC took over the production of IDs and data collection.[55] The transition of the archive into digital format began in 1997 with the Technological Modernization Project, designed to improve the security standards of the former IDs and digitalize the data of the Registry and the biometric

[47] More information available at RENACH website
[48] National Civil Registry, "La biometría: método ideal de identificación humana". Available at https://www.registraduria.gov.co/La-biometria-metodo-ideal-de.html
[49] Alzate, Juan David, Entre rostros y huellas. Una aproximación a los procedimientos aplicados a la investigación judicial por homicidio en Medellín-Colombia (1900-1930). TRASHUMANTE | Revista Americana de Historial Social, (2013): 32-55.
[50] Decree 944 of1934.
[51] Law 89, 1948.
[52] It is interesting to point out that Canada did not have nor currently has a system of national identification cards.
[53] Decree 2628, 1951.
[54] Law 39, 1961.
[55] Decree 1260, 1970.

databases. The process was carried out in two phases and the RNEC sought the support of the French multinational Morpho SAFRAN (currently known as IDEMIA[56]).[57]

The first phase, developed between 1997 and 2005, involved preparing the data of the Registry in order to install an Automated Fingerprint Identification System (AFIS). During the second phase (2005-2010), the database was broadened to include people with previous ID models and the AFIS system was finished. It included a web service that enabled its implementation in the public and private sectors[58]. In addition, in 2008 there began the issuance of biometric identity cards for minors so that they would be included in the Registry's databases.[59] By 2010, former models had become ineffective and the system transfer was completed. The greatest consolidated biometric database was in place in the country, with a 10 per cent under-registration.[60]

*Citizen IDs issued by RNEC in Colombia.*

In 2011, Decree 4057 eliminated the Security Administrative Department (DAS) and its enrollment functions were transferred to the National Police[61]. Finally, that same year, under inter-administrative contract No. 3, a cooperation agreement was signed by RNEC and the Police which permitted using the web service to reduce consultation time. As a result, criminal records converged with civil records in the biometric database of the Registry.

After the consolidation of the Registry's biometric database, an automation and interoperability process for digital identity were implemented at state level. Hence, Decree 19 of 2012 introduced the use of electronic fingerprint verification for carrying out administrative procedures and formalities before agencies and private parties.[62] This decree enabled the use of the Registry's biometric database for the purposes of identifying any kind of relationship between an individual and the State.

---

[56] https://en.wikipedia.org/wiki/IDEMIA

[57] Martins, Alexandre, The Colombian Identification System Implementation and technological advancement of the civil identification and registration systems. Keesing Journal of Documents & Identity, (2013): 25-28.

[58] Ibidem.

[59] Registraduría Nacional del Estado Civil. «Historia de nuestra cédula de ciudadanía.» Nuestra huella - Revista Electrónica Mensual, (2012)

[60] Inter-American Development Bank, Inventory of Civil Registries and Identification in Latin America and the Caribbean. (Washington: IDB, 2010), 14.

[61] Decree 4057, 2011.

[62] Decree 019, 2012, article 18.

Later, Law 1753 of 2015 expanded the use of biometric verification, consolidated the interoperability of RNEC's biometric database and converted it into a basic requirement of citizenship. This law made the biometric identification of individuals mandatory within the social security system (health, pensions and labor risks). At the same time, it required all public and private entities invested with public powers to verify an individual's identity using their own infrastructure or one of the providers chosen by the Registry to that effect.[63] Moreover, the Law made it possible for financial institutions and insurance companies to use the database to identity people by paying an amount of money established by the Registry.[64]

The trends created by this law were institutionalized by Resolution 5633 of 2016, which set out the conditions and procedures required to access the Registry's database. First, any agency or private entity with public powers can request access to the database by filing an application and only if they meet the technical requirements needed to utilize the database. Secondly, the Resolution made it possible for private parties to enter into agreements with the Registry to access biometric authentication by means of payments made to the RNEC.[65] Finally, it set out the technical requirements that would allow providers to charge for their technology services offered to agencies and private parties that may be interested in the authentication of people.[66]

*Colombia's National Police using biometric fingerprint identification.*

Verifying a person's identity in the RNEC's database through biometrics is a way of processing biometric data. However, in those cases where biometrics is used by law to establish an individual's identity, individuals may refrain from providing their biometric data as long as they relinquish the service or benefit, which renders Decree 1377 of 2013 void, in the sense that no activity should be dependent on the delivery of sensitive data.

The cases where biometrics is used to verify the identity of a person therefore show a contradiction between the data protection regime and the creation and use of state biometric databases.

The Constitutional Court has handled many cases where fingerprints are used as a substitute for the identity document. In one of them, an individual filed a claim to demand that his right to life and health be protected after his health insurance company's decision not to deliver the drugs he needed for his Parkinson disease. The insurance company required that the beneficiary's identity be verified using his fingerprint. In practice, this amounts to the violation of the right to access health services, as the person in question was unable to appear

[63] Law 1753, 2015.
[64] Ibid, article 159.
[65] Resolution N. 5633, 2016, article 33.
[66] Ibid.

before the facility where the drug was delivered due to the advanced stage of his illness. Instead, he asked a person he trusted to appear on his behalf. The Court stated:

> For this Court it is understandable that SaludCoop E.P.S. shall require that this kind of drugs be obtained by the person directly affected so as to avoid fraud and improper use. However, these safety rules should not be applied without regard to the circumstances of the case in point, where, despite needing the drugs, the patient cannot obtain them in person and therefore has no alternative than to authorize a representative to obtain them on his behalf before the respective E.P.S.[67]

The decision issued by the Constitutional Court synthesized the relationships between identity and biometrics before different state registries. It considered that having a right is different from the way in which identity is proven. Hence, verification rules should be flexible in a context of modernization, simplification and elimination of paperwork, while considering "scientific and technological advances" in connection with identity. Specifically, the Court stated that "the means of personal identification are not static systems. On the contrary, they should be updated in parallel to the technological and scientific advances on the subject in order to achieve more security, reliability and efficiency in identification processes, always ensuring the respect for human dignity and constitutional rights."[68]

The steps taken by the RNEC shows that the concept of identity is clearly changing. In an attempt to make the identification process safer and more modern, the population's sensitive biometric data are being increasingly collected, while at the same time acquiring expensive systems to automate processes. Thus, the relationship between citizens and the State is becoming more dependent solely on identification, as a result of which public institutions are compelled to implement costly technologies or third party contracts even in areas that lack adequate infrastructure for their proper use.

Furthermore, the RNEC is becoming an administrator of the population's biometric identity, as it charges private parties (mostly financial companies) who are interested in citizens' sensitive personal data and want to be certain of their individuality.

In the first place, a biometric database, originally planned for the identification of voters during the elections turned into a civil registry required for citizens to claim for their rights before the State. This enlarged the amount of individuals required to undergo the process of biometric data collection. Secondly, the biometric database, which was reserved –at the beginning of the century– for "unwanted populations" such as persons with criminal records, ended up converging with civil registries. Thirdly, the database designed for civil enrollment with the State became a prerequisite for accessing basic citizenship rights, a tool of the public force and a mechanism of individualization and identification before private parties too.

## IV. Mexico

The reform of the General Population Law passed in 1992 required Mexican citizens to enroll before the Population National Registry (RENAPO) under the Office for Domestic Affairs to obtain an identification card which included the holders' patronymic data and fingerprints. This information would be linked to a Unique Population Registry Code (CURP) and stored in a centralized database.

In 2011, by means of a presidential decree, the Office for Domestic Affairs amended the Rules of the Population Law to introduce the collection of additional biometric information. On top of the existing data –fingerprint and

[67] Constitutional Court, ruling T-312, April 4, 2008, M.P. Rodrigo Escobar Gil.
[68] Constitutional Court, ruling T-1000, November 26, 2012, M.P. Jorge Iván Palacio Palacio.

signature[69]– the iris of both eyes, the ten fingerprints and the biometric photograph were added.[70] The Federal Institute of Access to Information (currently the National Institute of Access to Information or INAI) criticized the greater treatment of biometric data for violating the principle of purposiveness, alleging that the identification process was 99% reliable with the use of fingerprint verification.[71] Besides, the National Commission on Human Rights (NCHR) requested the adoption of precautionary measures to protect the rights of the minors registered.[72]

Despite criticism, the enrollment program continued according to plan, collecting the biometric data of about 6 million minors. After some hiccups and doubtful budget allocations[73], by the time the program was suspended, more than four billion Mexican pesos had been invested between the administrations of former presidents Felipe Calderón and Enrique Peña Nieto, from 2006 to 2018.[74] The current administration does not plan on resuming RENAPO's identity card program.[75]


*Enrollment Center of the National Electoral Institute in Mexico.*

As provided by the articles of the Population Law reform, due to the lack of the citizen identity card (such as the one proposed by RENAPO), the identity card issued by the National Electoral Institute (INE), used in electoral processes to avoid fraud, can also be used as a means of personal identification in those administrative formalities where there is an agreement between the electoral authority and the other authorities and private

[69] Article 107 of the General Population Law.
[70] Presidential Decree amending and adding various provisions in the Rules of the General Population Law published in the Official Gazette of the Federation on January 19, 2011. Available at http://dof.gob.mx/nota_detalle.php?codigo=5174983&fecha=19/01/2011
[71] IFAI. RDA 310/12.
[72] El Informador. "Acepta Segob recomendaciones de la CNDH para la cédula". Informador.mx. February 12, 2011. Available at https://www.informador.mx/Mexico/Acepta-Segob-recomendaciones-de-la-CNDH-para-la-cedula- 20110212-0124.html
[73] Sánchez, Eduardo. "Armenta, uno de los responsables del fracaso del Renapo". Exclusivas Puebla. June 7, 2018. Available at http://exclusivaspuebla.com.mx/armenta-uno-de-los-responsables-del-fracaso-del-renapo/
[74] Redacción Quehacer Político. "Calderón y Peña tiraron más de 4 mil millones en una credencial única... que nunca se concretó". Quehacer Político. December 8, 2018. Available at http://quehacerpolitico.mx/calderon-y- pena-tiraron-mas-de-4-mil-millones-en-una-credencial-unica-que-nunca-se-concreto/
[75] Sánchez, Enrique. "Descartan continuidad de Cédula de Identidad Ciudadana", Excelsior, January 22, 2019. Available at https://www.excelsior.com.mx/nacional/descartan-continuidad-de-cedula-de-identidad- ciudadana/1291866

sector parties.[76]

Between 1992 and 2016, the INE signed 102 support and collaboration agreements with various local and federal authorities and public entities, in order to introduce the use of the electoral card as a means of identity verification.[77] In 2013, a "pilot" agreement of this type was signed with Banamex, one of the biggest banks in Mexico. Two years later, at INE's request, the National Transparency Institute, Access to Information and Personal Data Protection (INAI) issued an opinion on the use of the Data Verification System for the Voting Card.[78]

### I. Trends

Studying the legal frameworks of the countries under analysis allows us to shed light on the commonalities that arise regarding the way biometric technologies and biometric data have been introduced.

The introduction of rights, duties, sanctions and prohibitions by means of decrees and resolutions challenges the legality principle. Instead of having legislative, open and transparent debates inclusive of citizens' opinions and experts' concerns, we are faced with policies promoted without prior studies or analyses and implemented with little regard to democratic principles.

The connection between identity and people, as something that the State is entitled to manage, unveils a mechanism of control where public institutions treat the population as resources. This becomes more evident when the provision of social benefits and services depends on the mandatory collection of biometric data, which reinforces social inequality.

## IV. Applications of biometrics in daily life

Taking into account the previous analysis on the legal frameworks, in this section we will explore different case studies which highlight the consolidation of the narratives about people's identities and the use of biometric data for the most varied purposes.

### I. Argentina

As was stated in the previous section, the implementation of technology using biometric data has increasingly engulfed civilian life. Currently, Argentines are obligated to use their fingerprints and face recognition in different fields and for multiple purposes. In the field of public security, biometrics is allegedly used as a way of combating crime and fraud. In social security, it is used in order to avoid identity theft and is advertised as a fast, secure, effective, reliable and simple system. In the tax system. In education, to monitor teachers' attendance. In the electoral field, it is used to authenticate the identity of voters as a way of combating "transborder electoral migration"[79]. In sports events, biometrics is used to monitor access to football stadiums.[80]

[76] https://www.ine.mx/credencial/

[77] General Council of the National Electoral Institute. INE/CG92/2016. April 12, 2016. Diario Oficial de la Federación. Available at http://dof.gob.mx/nota_detalle.php?codigo=5432730&fecha=12/04/2016

[78] IFAI/CPDP/0022/15.

[79] See: "Prueba biométrica en las PASO: la Cámara Electoral respondió a ADC", October 18, 2017, available at https://adcdigital.org.ar/2017/10/18/prueba-biometrica-las-paso-la-camara-electoral-respondio-adc/ and "¿Es necesario un sistema de identificación biométrica electoral?", November 7, 2017, available at https://adcdigital.org.ar/2017/11/07/es-necesario-un-sistema-de-identificacion-biometrica-electoral/

[80] For more information per area see report "Cuantificando identidades en América Latina", ADC, 2017.

By mid-2018, the Ministry of Interior and the Secretariat of Modernization (formerly created as a ministry) announced the implementation of a joint project known as Digital Identity System (SID, for its acronym in Spanish) with the view of simplifying and speeding up requests made by individuals and filed with the State. It would permit authenticating identity through the use of face recognition.


*Ad from the Ministry of Interior and Secretariat of Modernization on the Digital Identity System.*

SID is under the scope of the current national administration, which strives to promote the State digitalization and technological improvement, making public entities readily accessible to citizens. In this context, in December 2017, the Ministry of Interior and the Secretariat of Modernization entered into a cooperation agreement to create SID.

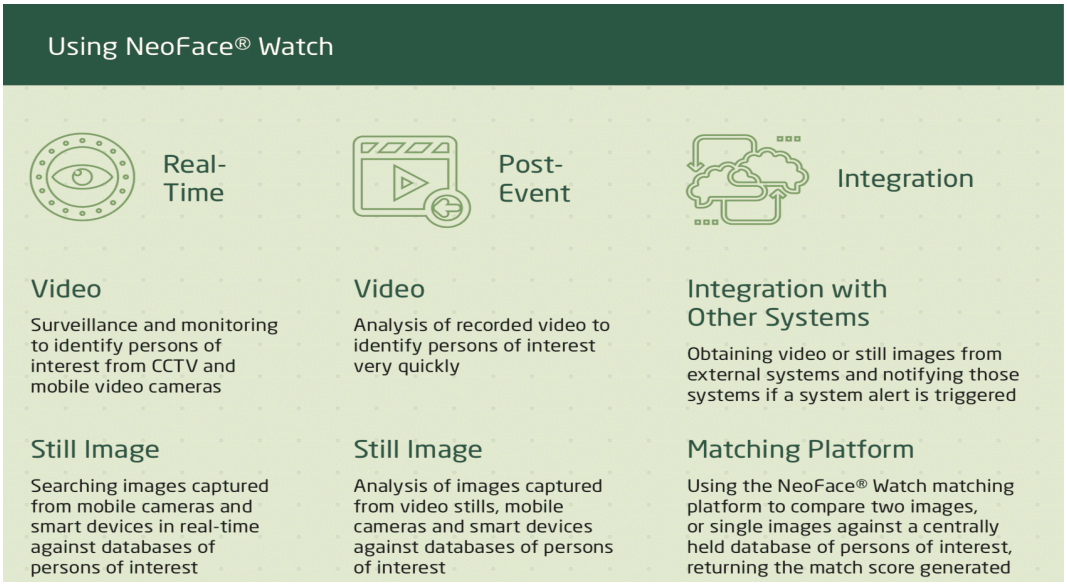
Articles 9 and 11 of Law 17.671 and article 1 of Decree 1501/09 constitute the legal basis used by the State to justify the implementation of SID and the introduction of biometrics as a legally valid identification method. As previously noted throughout this report, these regulations are not adequate when analyzed under a human rights perspective.

In March 2018, the Digital Government Office, under the Secretariat of Modernization, directly awarded the software acquisition contract for face recognition to NEC Argentina S.A., an affiliated company of the Japanese multinational based in Tokyo, for a total 834,403.90 US dollars, as shown by the negotiating records accessed by ADC after making a freedom of information request.

The solution provided by NEC was NeoFace Watch[81], which was implemented directly in RENAPER to utilize the existing face database.

Based on the information provided by the manufacturer, NeoFace Watch works as follows: once face images are obtained from videos, photographs and external systems, the algorithm analyzes individual close-ups of the videos and images to detect faces and identify facial traits of each individual. Then it creates a small template for each face and checks it against the available records in the database until a match is made. The system can store a record of the matches found and can be set so that an alert will be raised in real time.[82]

[81] https://www.nec.com/en/global/solutions/safety/face_recognition/NeoFaceWatch.html
[82] NEC brochure for the NeoFace Watch software.




*NEC's description of the functions of its face recognition software NeoFace Watch.*

NEC claims to have high rates of positive identification, even with images of low-quality resolution, and to be highly resilient to varying environmental conditions (such as light, face angle and accessories used by the person, etc.).

In theory, SID is a service available for public entities and private companies which can be accessed from the Online Transactions platform once authorized.[83] There are three types of packages that can be chosen to authenticate different types of information held by RENAPER.

The first service package requires the user to provide a copy of the front and back of the National Identity Document (DNI, in Spanish), apart from a face photo as proof of life[84]; the second package requires the user to enter their DNI number, select their gender and provide a face photo[85]; finally, the last package only asks for the DNI number, gender and relevant transaction number[86]. The fees for data verification are established by RENAPER and were last updated in July, 2018 by Resolution 430.[87]

The company or agency may implement SID in three different ways[88]:

1. Using the application programming interface (API[89]) from a website or mobile app.
2. Integrating it directly into its app using the software development kit (SDK[90]) provided, available for Android and iOS.
3. Linking the process to RENAPER's app using a QR code or link. The app later processes the biometric identification separately.

From the users standpoint, the people who access the services that have implemented SID, when carrying out a transaction from their smart phones or tablets, they are required to provide a face photo. This information is sent

83 https://www.argentina.gob.ar/sid/adherir
84 https://www.argentina.gob.ar/sid/modalidades-y-productos/paquete1
85 https://www.argentina.gob.ar/sid/modalidades-y-productos/paquete2
86 https://www.argentina.gob.ar/sid/modalidades-y-productos/paquete3
87 Resolution 430/18, Ministry of the Interior.
88 https://www.argentina.gob.ar/sid/tecnologias-soportadas
89 https://es.wikipedia.org/wiki/Interfaz_de_programaci%C3%B3n_de_aplicaciones
90 https://es.wikipedia.org/wiki/Kit_de_desarrollo_de_software

to RENAPER and checked against its database to provide the company or agency of that app a “hit” or “no hit” result, i.e., whether there was a data match or not. For this reason, when questioned by ADC, RENAPER claimed that there is no biometric data transfer on their part.

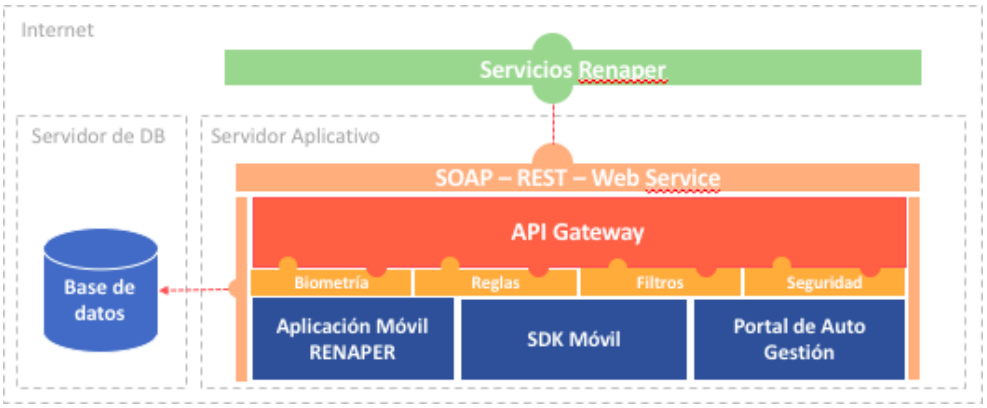



*Chart by the Ministry of Interior and the Secretariat of Modernization showing SID’s architecture.*

By September 2018, RENAPER saw 116 public and private entities interested in using SID, as shown by the freedom of information request made by ADC. 47 entities conducted a total 14,452 test runs in a (non-productive) development environment, which add to the 10,535 tests conducted by RENAPER.

In answer to the request for information made by ADC, Modernization informed that a meeting was held in April 2018 with representatives of the Access to Public Information Agency and RENAPER’s Office of Information Technology with the view of welcoming their recommendations on SID’s compatibility with the current data protection law.

Financial services is the most interested sector in implementing SID, specially companies catalogued as fintech, such as mobile payment platforms and digital banks. The Innovation Work Team of the Central Bank, which represents the main public and private players in the field, allowed members to implement a testing process.

Regardless, the very discourse of the Argentinean government aims at expanding the Digital Identity System to include a multiplicity of sectors, services and fields, thus turning it into the new tool used by individuals to interact with public and private bodies.

## II. Brazil

In recent years, arguments involving public safety began to burst into the debate as the adoption of surveillance technologies in public services and related policies increased.

In March 2015, the government of Rio de Janeiro announced the implementation of a transport card that would collect users' fingerprints.[91] Likewise, the Legislative Assembly of Rio de Janeiro authorized the use of biometric identification via face recognition in buses.[92] The implementation of biometric technology in the transport system is the result of collaboration efforts between public and private entities.[93]


*Face recognition system for public buses in Rio de Janeiro.*

In 2016, the National Institute for Educational Studies and Research (Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira or Inep), a federal agency under the Ministry of Education, announced the collection of fingerprints of students taking the National High School Exam (ENEM, in Portuguese).[94] In the last decade, it has gained importance as many federal universities and educational institutes use ENEM as an admission exam.

Inep published communication Edital ENEM 2016 in the Official Gazette establishing it would begin the collection of biometric data of candidates on exam day.[95] The following year, through Edital ENEM 2017, Inep established that "candidates who refuse without good cause to provide biometric data will be eliminated from the Exam".[96] The same measures were put into place in the 2018 edition.[97]

Inep's reasoning for this initiative is making the Exam a safer process. According to Inep's president, Maria Inês Fini, thanks to the fingerprint database of the Federal Police, they can attest to the candidates' identity. However, no further details were given regarding the processing of biometric data, what would constitute good cause for refusing to enroll the fingerprint or how data would be collected.

---

[91] Available at http://www.rj.gov.br/web/setrans/exibeconteudo?article-id=2383637
[92] Law 7.123, December 8, 2015. Available at https://chupadados.codingrights.org/wp-content/uploads/2016/11/Lei_7123_Controlebiometrico.pdf
[93] More information in "RioCard: concentración de datos y dinero en el transporte público", available at https://chupadados.codingrights.org/es/com-o-riocard-seus-dados-passeiam-pelo-rj-e-ninguem-sabe-onde- vao-descer-2/
[94] "MEC fará cadastramento biométrico surpresa no Enem", O Globo, April 14, 2016, available at https://oglobo.globo.com/sociedade/educacao/enem-e-vestibular/mec-fara-cadastramento-biometrico- surpresa-no-enem-19085113
[95] Diário Oficial da União (DOU), April 15, 2016.
[96] Diário Oficial da União (DOU), April 10, 2017.
[97] Diário Oficial da União (DOU), March 21, 2018.

Since 2010, there have been frequent reports about fraud cases and information leaks involving ENEM.[98] However, fraud cases have been associated with cheating and the electronic transfer of answers to candidates[99]; cases where other individuals fake the identity of students taking the exam are extremely exceptional.

In November 2018, the National Council of Justice (CNJ) announced a program which uses biometric technology to register people imprisoned and the updating and issuance of personal documents such as the social security number ("CPF") or the birth certificate.

The president of the National Council of Justice and the justice of the Supreme Court, Dias Toffoli, stressed the importance of ensuring citizenship rights of imprisoned individuals, establishing that "most of them do not even have a birth certificate", which makes visible the relationship between citizenship and public safety.[100] Raquel Dodge, Brazil's Attorney General, justified the program from the standpoint of due process, arguing that "people under custody must be identified and the State must know their crimes; whether they are repeat offenders; their whereabouts and whether they are serving their sentences.[101]

In January 2019, the Rio de Janeiro Press Office announced the implementation of a face recognition software to monitor crowds during the Carnival taking place in March, beginning with the city of Copacabana.[102] According to the State Secretary of the Military Police Department Rogério Figueredo de Lacerda the goal was to allow authorities to monitor celebrations remotely and identify individuals with detention orders, police records and missing people.[103]

## III. Colombia

The chief state agencies running biometric databases are RNEC, the National Police and Colombia Migration.

As mentioned in the previous section, the National Development Plan (2010-2014) made it possible to use databases created by public entities and private sectors carrying out public functions "permanently and free of charge" for other entities that may so require for the programs and projects of that Government.[104]

The process regarding the use of biometric databases changed upon the approval of Decree 019 of 2012, which introduced the use of electronic means to authenticate citizens in procedures carried out by public entities or those performing public functions of different nature involving, for example, financial or pension-related matters, public registries, issuance of passports and visas, among others.[105] The following regulations of the Registry made RNEC's biometric databases available to those public and private entities providing public services, to fight

[98] After the investigation on the information leakage no relevant conclusions have been published nor have sanctions been imposed on responsible parties. http://g1.globo.com/educacao/noticia/2010/08/vazamento-de-dados-de- estudantes-do-enem-sera-apurado-diz-inep.html

[99] Available at https://www1.folha.uol.com.br/educacao/2018/04/estudo-inedito-indica-alta-chance-de-fraude-em-mil-provas-do-enem.shtml

[100] Available at http://www.cnj.jus.br/noticias/cnj/87773-biometria-e-digitalizacao-vao-melhorar-justica-criminal

[101] Besides, Minister of Justice and Public Security Sérgio Moro brought before the plenary of the Deputies' Chamber Bill 882/2019 as part of his proposed anticrime measures, one of which involves the creation of a Multibiometric and Fingerprint National Bank using data collected in "criminal investigations or criminal identifications" in order to subsidize criminal investigations.

[102] Available at http://www.pmerj.rj.gov.br/2019/01/policia-militar-vai-implantar-programa-de-reconhecimento-facial-e-de-placa-de-veiculos/ According to a spokesperson, the project will not have any initial costs, as the telecommunications company responsible for the software has an enforceable contract with security agencies involving the installation of communication programs in police vehicles. "Oi is already a state contractor. The cost has already been added to the services provided by Oi to the state, which involve data trafficking." Should the pilot project be approved, it will pave the way for a future tender agreement that will allow other companies to participate. Available at http://agenciabrasil.ebc.com.br/geral/noticia/2019-01/rio-programa-de-reconhecimento-facial-entra- em-operacao-no-carnaval

[103] "PM anuncia que vai começar a usar programa de reconhecimento facial e de placas de veículos no carnaval", Globo, January 30, 2019, available at https://g1.globo.com/rj/rio-de- janeiro/carnaval/2019/noticia/2019/01/30/pm-anuncia-que-vai-comecar-a-usar-programa-de-reconhecimento- facial-e-de-placas-de-veiculos-no-carnaval.ghtml

[104] Law 1450, 2011, article 227

[105] Ibid, article 17 and 18.

against identity theft and fraud prevention [106]

After the implementation of this policy, there emerged the so-called "technological allies" or providers of technological infrastructure that allow entities and private individuals to access RNEC's databases upon fulfilling the requirements[107] established by the agency. This means that the actors who want to use the Registry's biometric database depend on technological allies to fulfill their functions. In short, RNEC turned the biometric database into a business for private companies to render their technological services to the State and for private entities to perform public functions.[108]

In 2016, the National Police began the process of acquiring and implementing the Appolo system for the use of mobile biometric verification devices with a cost of 895 million pesos (287 thousand US dollars, approximately).[109] Based on Resolution 3341 of 2013, for the system to work, it was necessary to sign an agreement with RNEC in order to have direct access to the biometric databases.

According to the Police, the system stems from three major concerns. First, there is the need to innovate in the field of criminal investigations. Secondly, it addresses the problem of national security, as the complete identification of individuals would allow taking more effective and reliable decisions in support of national security.[110] Thirdly, the device would facilitate the authentication of an individual's identity at any time and would help combat the forgery of documents and identity theft.[111]

As of 2018, the National Police began using a device manufactured by Olimpia to access the Registry's database online, in order to verify the identity of a person and corroborate whether national or international arrest warrants have been issued. The device also makes it possible to check data on the Citizen Card (found in the bar codes) against data in RNEC's database, which helps determine if the document is legitimate.[112] The Police expect the devices will include new characteristics such as face and iris recognition.[113]

The policies promoted by RNEC have also aroused the interest of financial and banking institutions. By means of Contract 27 of 2016, the Registry signed a single agreement with the Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria)[114], whereby it allows all member institutions to access RNEC's databases upon a service payment.

---

[106] Resolution N. 3341, 2013 and Resolution N. 5633, 2016.

[107] Some of the requirements include having certified experience in biometric authentication of at least three years, having technological infrastructure and financial capacity and passing a technical assessment designed by the Registry.

[108] RNEC has published a list of public entities and private entities performing public functions that have entered into an agreement with RNEC regarding access to the National Identification Archive. Said list is available at https://www.registraduria.gov.co/-Consultas-ANI-.html

[109] Telematics Office of the National Police, «Estudios previos para Contrato de Compraventa 06-7-10081-16: Sistema de Biometría Móvil.» (2016), available at https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=16-1-157976

[110] Ibidem.

[111] Ibidem.

[112] El País, «Los nuevos gadgets de la Policía con los que verifican identidad y antecedentes en segundos.» El País.com.co, (May 9, 2018), available at https://www.elpais.com.co/judicial/los-nuevos-gadgets-de-la- policia-con-los-que-verifican-identidad-y-antecedentes-en-segundos.html

[113] Camacho, Laura, «La Policía ahora revisará sus antecedentes judiciales con la huella.» El Tiempo, (May 21, 2018), available at https://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/policia-implementa-la-identificacion-biometrica-en-sus-procedimientos-214926

[114] Asobancaria. «Autenticación biométrica para usuarios del sistema financiero colombiano.» (2016), available at https://www.asobancaria.com/biometria/

*Biometric fingerprint identification machine used in Colombia.*

According to Asobancaria, biometric authentication in the Colombian financial system is beneficial both for individuals and financial entities. In the first case, the use of this modern technology enhances transactions, reduces the risk of identity theft and promotes a transition towards digital formats through "zero paper" policies. Regarding the latter, biometric authentications give entities the possibility to offer automated services and verify clients' financial data.[115]

Ten years ago, RNEC used biometric authentication for the first time in atypical electoral processes. According to the Registry, the idea was to implement three new controls in the voting process: the identification of voters against the database of the electoral census, the issuance of the identity document and fingerprint authentication. These procedures would help avoid identity theft and duplicate votes in atypical elections.[116] In fact, RNEC argued that the new procedures were based on the ruling of the State Council of 2005, which confirmed that there had been more votes than voters in the elections for the Congress of the Republic in 2002.[117] From then on, the Registry has gradually increased the use of biometrics in electoral processes; so far it has been used in approximately 33 elections.[118]

By the end of 2017, the Migration and Immigration Authority Control of the Colombian State (Autoridad de Control

[115] Asobancaria, «Biometría: conveniente y segura.» Semana Económica 2018 (2018).
[116] National Registry of Civil Status, «Suplantación de electores: un fraude más recurrente en el mapa de riesgo electoral.» Nuestra Huella, (2009), available at https://www.registraduria.gov.co/Edicion-No-34-Ano-V- diciembre-de.html#01
[117] National Registry of Civil Status, "Este domingo los habitantes de Salazar de las Palmas (Nor- te de Santander) y Belén de los Andaquíes (Caquetá) eligirán sus nuevos alcaldes", 2009, available at https://www.registraduria.gov.co/ESTE-DOMINGO-LOS-HABITANTES-DE,1563.html
[118] National Registry of Civil Status, «La huella dactilar: la base del sistema de identificación en Colombia.» Nuestra Huella, (2012), available at https://www.registraduria.gov.co/rev_electro/2012/rev_elec_noviembre/revista_noviembre2012.html#10

Migratorio y de Extranjería) began using the Biometric Migration system (BIOMIG). It is an automatic identification system for border control which uses biometric data of the iris to identify nationals older than 12 years entering the country through the most important airport in the country, Bogota's "El Dorado". The system currently runs on 10 terminals and enrollment is voluntary, by presenting the citizenship card, passport and the collection of people's biometric data.[119]


*Colombia Migration ad about iris recognition system*

The Director of Colombia Migration informed the press that during the migration process the terminal "automatically connects with the different national and international databases [INTERPOL] so as to verify whether the person in question has some sort of arrest warrant".[120]

The purchase of the equipment was made under contract number 117 of 2017 with the Temporary Union of Border Control (Unión Temporal de Control Fronterizo) INCOMELEC-GEMALTO. The first phase of the contract cost more than two thousand one hundred million Colombian pesos (675 thousand US dollars approximately). Despite the Union, the company in charge of the system is the multinational Dutch Gemalto, which develops the software for biometric face recognition, used by terminals EF-45, and for iris recognition, by the company CMI Tech.[121] The contractor has an ample record and links with the Colombian government and Colombia Migration.[122] Currently, the system runs in terminals in four airports of Colombia and there are plans to implement

[119] Presidency of Colombia, «Migración Colombia empezó a usar sistema de inmigración de colombianos por medio de reconocimiento del iris.» (February 25, 2018).
[120] Caracol Televisión, «Con solo una mirada, colombianos podrán ingresar en segundos al país.» Caracol Televisión, (February 27, 2018): https://noticias.caracoltv.com/colombia/con-solo-una-mirada-colombianos-podran-ingresar- en-segundos-al-pais
[121] Migración Colombia, Contract No 117 of 2017 with the Unión Temporal de Control Fronterizo INCOMELEC- GEMALTO, (2017).
[122] GEMALTO, "Los ojos son la solución".

it in migration mobile units by satellite.[123]

According to Colombia Migration, the system has several goals, such as the enhanced perception of security at an international level, the optimization of migratory processes, financial efficiency, the entity's modernization and national security.[124] In this sense, the BIOMIG system seems to be a solution for all the entity's concerns in terms of national security and efficiency as regards traveler customer service. All the same, the main aim of the system is to focus on Colombian nationals so it can later encompass persons from other nationalities too.[125]

*Iris recognition device used in the migratory process with the BioMig system.*

Colombia Migration acknowledges that despite the fact biometric data is sensitive and must be kept confidential pursuant to Law 1581 of 2012, its treatment does not require prior authorization due to the nature of its functions. Given that Colombia Migration is a civil security authority of the State, the Law allows it to treat biometric data, regardless of its sensitive nature, for security and national defense reasons.[126]

## IV. Mexico

The implementation of biometric technology has been more ample in the private sector, especially in the financial field. However, in recent years, the State has begun to undertake initiatives which promote the use of biometric data as an infallible solution to old problems. In the following paragraphs we present two relevant cases from two different sectors. The first case concerns the use of biometric data enrolled by voters for identity verification in financial entities; whereas the second case deals with the collection of biometric data of migrants.

[123] Becerra, Laura, «Cuatro aeropuertos del país ya cuentan con sistema de migración automática.» La República, (April 5, 2018).
[124] Colombia Migration, Previous Research for Contract No 117 of 2017 with the Unión Temporal de Control Fronterizo INCOMELEC-GEMALTO, (2017), 1-4
[125] Ibidem, 6.
[126] Office of Legal Counsel for Colombia Migration, "Memorando Concepto Jurídico".

## Financial sector

In 2016, the Collaboration Agreement was signed in Mexico to prevent identity theft through the financial system. It was agreed to allow banking institutions to use INE's Verification System. Under this collaboration agreement, banking institutions in Mexico may collect information from their clients and check it against data contained in the electoral roll of the National Electoral Institute in order to assess the identity of their clients.

In 2017, the National Banking and Securities Commission (CNBV) amended the general provisions applicable to credit institutions, obliging banking entities to verify the biometric information of persons using identifications issued by INE. Should an individual use their passport or migratory documents for identification purposes, they are under no obligation to undergo the verification process.

A year later, the CNBV once again amended the general provisions applicable to credit institutions to allow banks to collect at least six fingerprints in order to verify the identity of persons. The period during which banking institutions may use biometrics in the verification process of clients who hire o perform banking transactions has also been extended by CNBV till 2020. It is expected that the use of biometric data in this field will become the norm, thereby replacing passwords and other means of verification.

## Migrations

In the modernization report of the National Institute of Migration (INM) under the 2006-2012 administration, the agency declared that it had a centralized biometric database containing biometric data (fingerprints, iris and face pictures). According to the sixth progress report of the INM published in 2012[127], in December 2011 the facilities of the Institute saw the arrival of the Central Biometric Engine, which has the "capacity to exchange [biometric] information with Mexican authorities and work together with agencies of the US government."[128]

Up until 2012, more than 84 kiosks were installed and equipped to enroll biometric data within national territory, in 24 of the 32 federative entities of the republic. On top of this, 167 additional kiosks were installed by the Anti-Drugs Office of the United States Embassy (NAS)[129]. Biometric data is treated in five cases[130]; for example, in registering migrants entering and leaving the migration facilities and in settling cases involving duplicate identities or other anomalies.

*Kiosks installed for the enrollment of biometric data in the migration process in Mexico.*

[127] Secretaría de Gobernación. "Sexto Informe de labores, Instituto Nacional de Migración". pg. 15. Available at http://www.inm.gob.mx/static/transparencia/pdf/Informe_de_labores_2012.pdf

[128] Instituto Nacional de Migración. "Modernización tecnológica del INM: Gestión 2006 - 2012". pg. 10. Available at http://www.inm.gob.mx/static/transparencia/rendicion_de_cuentas/MD_DGTIC_05OCT12.pdf

[129] Ibid, page 22.

[130] The other three cases involve the enrollment, issuance and verification of the Regional Visitor Migration Form and the Migration Form for Frontier Workers. Ibid, page 28.

According to the journalist Jesús Esquivel, at least since 2014, the INM shares biometric data of detained migrants with the government of the United States[131], without the immigration agents enrolling this information even knowing about it.[132] Once obtained by the United States, the biometric data is used to identify "unwanted persons" against the databases run by the US government.

After a freedom of information request made by R3D before INM in 2017[133], the Institute replied that it only treated biometric data of foreigners as part of the Reliable Traveler Program, which allows Mexican, Canadian and US citizens to reduce waiting time when entering Mexican territory by plane. In a subsequent freedom of information request on the treatment of biometric data of migrants[134], the Institute refused having performed such treatment.

Irazú Gómez, coordinator of incidences and linkages at Sin Fronteras[135], declared in an interview for R3D, having witnessed since 2012 the enrollment by the Migration National Institute of migrants' faces and irises when accessing migration stations. The biometric data system used to enroll migrants, called SICATEN[136], shared data with governments of some Central American countries and the United States. The transfer of biometric data aimed to identify persons tagged as terrorists by said countries so as to prevent them from accessing the country, commented Gómez.

Regarding the way migrants' consent was obtained for the treatment of their biometric data, Gómez explained:

"Upon entering the immigration hall migrants had to fill out a form and then went through a machine that scanned their irises and faces. As far as I could see, they were not given any information on the procedures unless they would ask for it. In general they were just given a bunch of papers for them to sign saying they had been informed of their rights and that they had received the necessary information. People would not read the documents and signed them without ever knowing what it was about." According to Gómez, the biometric registry of detained migrants remains operative.

According to the INM, the legal basis for treating biometric data is found in articles 18, 19, 20 and 63 of the Migration Law. These articles grant powers related to immigration policies such as establishing requirements for accessing Mexican territory; monitoring the entry and exit of persons in the country; revising their documents and maintaining the National Registry of Foreigners[137]. Moreover, article 60 of the law's Rules, issued by the executive power, explicitly establishes that the immigration authority can corroborate, among others, migrants' information and personal data.

The Law is ambiguous and vague regarding the practices the INM can follow when implementing migration policies. It does not establish in explicit terms the possibility to treat biometric data, but it treats biometric data as personal data.

---

131 Aristegui noticias. "México entrega a EU datos biométricos de migrantes y mexicanos: Jesús Esquivel". May 7, 2018. Available at https://aristeguinoticias.com/0705/mundo/mexico-entrega-a-eu-datos-biometricos- de-migrantes-y-mexicanos-jesus-esquivel/

132 Ibid.

133 Request for access to information number 0041110022117, available at https://r3d.mx/wp- content/uploads/Respuesta-Instiuto-Nacional-de-Migraci%C3%B3n-Biom%C3%A9tricos.pdf

134 Request for access to information number 0411100139918, available at https://r3d.mx/wp-content/uploads/0411100139918.pdf

135 Sin Fronteras is a secular, nonpartisan and nonprofit organization of the Mexican civil society which contributes to the promotion, protection and defense of Human Rights of migrants who are subject to international protection in order to dignify their living conditions through direct attention and influence in the public agenda. https://sinfronteras.org.mx

136 System of Assurance Control and Transfers in Migration Centers.

137 Pursuant to article 63 of the Migration Law, the National Registry of Foreigners contains information relative to all those foreigners who are granted temporary or permanent resident status in Mexico.

por los Derechos Civiles

## V. Conclusions

Drawing from the countries analyzed and the case studies explored, we have shown the expansive effect of identity narratives together with the implementation of biometric technologies. It is alarming that States resort to specific technology to solve their problems and are always finding new applications to introduce biometrics in public policies, without taking alternative methods into consideration.

The construction of identity narratives promoting an increasing use of biometric data is based upon laws which challenge the legality principle, as most of them are decrees issued by the executive power and ministerial resolutions. Moreover, the rules, guidelines and protocols which restrict the collection and processing of biometric data are designed by the same entities that implement these programs.

The introduction of biometrics has neither been clearly nor expressly outlined by law in any of the countries under study. In general, norms use the concepts without defining them and in many cases leave said definitions open to the interpretation of those entities that implement biometric technology and treat biometric data. This poses various issues regarding the limitation, use and processing of the different types of biometric data that can be collected, as States can opt for more broad interpretations with respect to the data they wish to use for different purposes.

In Brazil and Colombia, the legislation classifies biometric data as sensitive data, while in Argentina and Mexico that classification has resulted from the interpretation of the data protection authority and not from a legal provision. However, it is evident that data protection authorities in each country lack enough power in order to enforce the law and avoid abuses in the use of biometric data by the State and the private sector.

Based on the case studies analyzed in this research, it is clear that countries with unitary States, such as Colombia, have greater chances of implementing public policies through initiatives promoted by one single central entity. Nevertheless, even in federal countries, as is the case with Argentina, Brazil and Mexico, public administrations have been able to promote and unify narratives linked to the need of biometric technology for the infallible recognition of people's identity and, therefore, for the exercise of certain rights.

The countries under study have shown the justifications used by States in their attempt to incorporate more biometric technologies in people's daily lives. The prevailing narrative conceives public security and biometrics as the ideal formula for solving major security problems, such as criminal investigations and the fight against crime. Furthermore, the provision of benefits and social services is conditioned by mandatory biometric data collection. Migratory control, taxation activities (such as tax payments or mandatory requirements for practicing an independent profession), the financial sector, electoral processes and public transport have also been permeated by the implementation of biometric technologies.

The impact that biometric technologies pose to the exercise of fundamental rights depends on the type of data used and various factors regarding its implementation, hence, each case must be analyzed individually. However, we can highlight some considerations with respect to the implications of the uses for such technology.

Collecting and processing data in biometric databases to identify people (1:N), for investigation and crime prevention purposes, challenges due process guarantees and the presumption of innocence. People who have their biometric data stored in a database are turned into potential suspects and the burden of proof shifts, as individuals must "prove" they are not the ones the authorities are looking for (which occurs the moment their biometric templates are discarded after showing no matches).

In the case of facial recognition, the algorithms in charge of finding similarities between templates and facial traits

may be biased as a result of their setting and/or training. This means the system may be prone to discriminate against certain groups or communities, given the high rate of false positives, as has been shown to be the case with African Americans in the United States.[138]

The State's development of biometric systems for population monitoring not only has an impact on the right to privacy and individual freedoms such as expression, association and assembly. The fact that they are used as a tool for controlling citizens or a mechanism for managing the provision of essential benefits by the State means that we should also take into consideration its collective perspective.

In this sense, biometrics affects people in three different dimensions:

1. Collective dimension of individual rights: Even though the right to privacy is a classical example of the first generation rights, it is necessary to think about how the power of surveillance technologies affects this right in a collective way. Biometrics involves actions that may affect a crowd or group of people at the same time. Thus, privacy becomes a collective right that concerns society as a whole. In this respect, it must be mentioned that in Argentina, the use of collective actions began with a case involving the violation of the right to privacy.[139]

2. Impact on social rights: Biometric technology can also be used to restrict rights which are essentially collective, such as social rights. As mentioned throughout this report, the provision of health, education and social security services increasingly relies upon the mandatory enrollment of biometric data. Hence, refusing to provide this kind of data means we cannot fully enjoy our social rights.

3. Particular consequences for specific groups: The use of biometric data has concrete harmful effects on certain ethnic and religious groups. In this case, the collective aspect does not have to do with the nature of the right at stake, but with the damages that biometric technology causes particularly to a subgroup of the population. Hence, biometrics poses the risk of maintaining or promoting the reproduction of inequalities or grievances within sectors that have already experienced a long record of vulnerabilities.

## VI. Recommendations

The enrollment of biometric data must be voluntary, without conditioning the provision of services and state benefits (such as social security) to the collection of such data. Likewise, States must provide alternative means of identification not involving the enrollment of biometric data.

Before implementing biometric data systems and technologies, States must perform the following assessments:

1. In the first place, they should conduct assessments that provide scientific grounds for understanding the dimension and seriousness of the problem that is being addressed through biometrics and the different approaches that can be taken to solve such problem. States should always choose the measure least invasive and restrictive of fundamental rights. Unless they have ruled out all other measures, States should not opt for measures restricting civil rights and individual freedoms.

2. Secondly, it is essential to analyze the impact that biometric systems and technologies can have on human rights. This allows identifying the risks posed to the exercise and enjoyment of rights such as the rights to privacy, freedom of expression, association, free assembly, equal treatment before the law and the right to no discrimination, so that the necessary actions can be taken to prevent and mitigate said risks.

[138] Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots", ACLU, July 26, 2018, available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons- face-recognition-falsely-matched-28

[139] Halabi, Ernesto c/ P.E.N. - Ley 25.783 - dto. 1563/04 s/ amparo Ley 16.986, February 24, 2009.

3. Finally, a risk assessment must be carried out regarding the security of the personal data collected, stored and processed in order to identify and implement best practices in the protection of information, prevent incidents and design protocols for security information failures. Independent technical audits should also be conducted periodically. All of this should aligned to the national cybersecurity strategies in each country.

Legislative bodies should consider updating current legal frameworks to reflect international human rights standards and promote open, inclusive and transparent debates, especially regarding the definitions of "biometrics", "biometric technology" and "biometric data". The collection and processing of biometric data, with the subsequent creation of huge databases, must be carried out in accordance with the principles of necessity and proportionality and based on the standards adopted by the Inter-American System of Human Rights. The use of biometric data should have a legitimate purpose established by laws passed by the legislative body.

Laws on biometrics should incorporate provisions on monitoring and accountability mechanisms. In this sense, the first step would be having independent authorities to detect and sanction the wrong use of biometric data or the implementation of systems deemed disproportionate and illegal based on international human rights standards. It is necessary to establish specific controls over the access to databases and the identification of individuals, such as, for example, court authorizations in criminal cases. In addition, said criminal cases must involve crimes of a more serious nature.

Regarding biometric data treated as personal data, the laws –on data protection– of all the countries under analysis must be updated in order to define more specific goals for the use of data and enhance the protection levels afforded to its treatment. This also means reviewing the roles and powers of data protection authorities relative to the implementation of biometric technology by the State and the private sector, together with their power to impose sanctions upon a violation of the law. This requires making these authorities fully independent from State powers, by providing them with the financial resources and trained personnel needed to achieve this goal.

In view of the imminent creation and expansion of identification systems fed by biometric data, considering that these systems are growing complex and are used by multiple public agencies, we should reassess what we understand by "informed consent". The implementation of biometric technologies for public security reasons and the fact that access to essential services for the most vulnerable social groups depends on the provision of biometric data should also make us reconsider.

Likewise, the fact that many initiatives of the countries under study are implementing biometric technology for the provision of services and social benefits shows the value of freedom when having to provide consent. Hardly is consent free when citizens depend on the State for access to essential services.

However, regardless of the fact that consent must always be free and informed, this does not mean it can be used as a carte blanche or excuse for these technologies to violate other key principles regarding the treatment of data, such as the purpose principle. For this reason, minimum standards are unwaivable for the data subject. They cannot be revoked nor transferred when consent is provided –in accordance with the principle in dubio pro data subject– as there is always an unequal power relation between those who treat data and their subject.

Finally, depending on the biometric system, some minimum considerations should be incorporated to reduce the negative impact on privacy: restricting the type of biometric data stored in the same database; prioritizing verification (1:1) over identification (1:N); and avoid storing patronymic information with biometric data in the same database.


por los Derechos Civiles