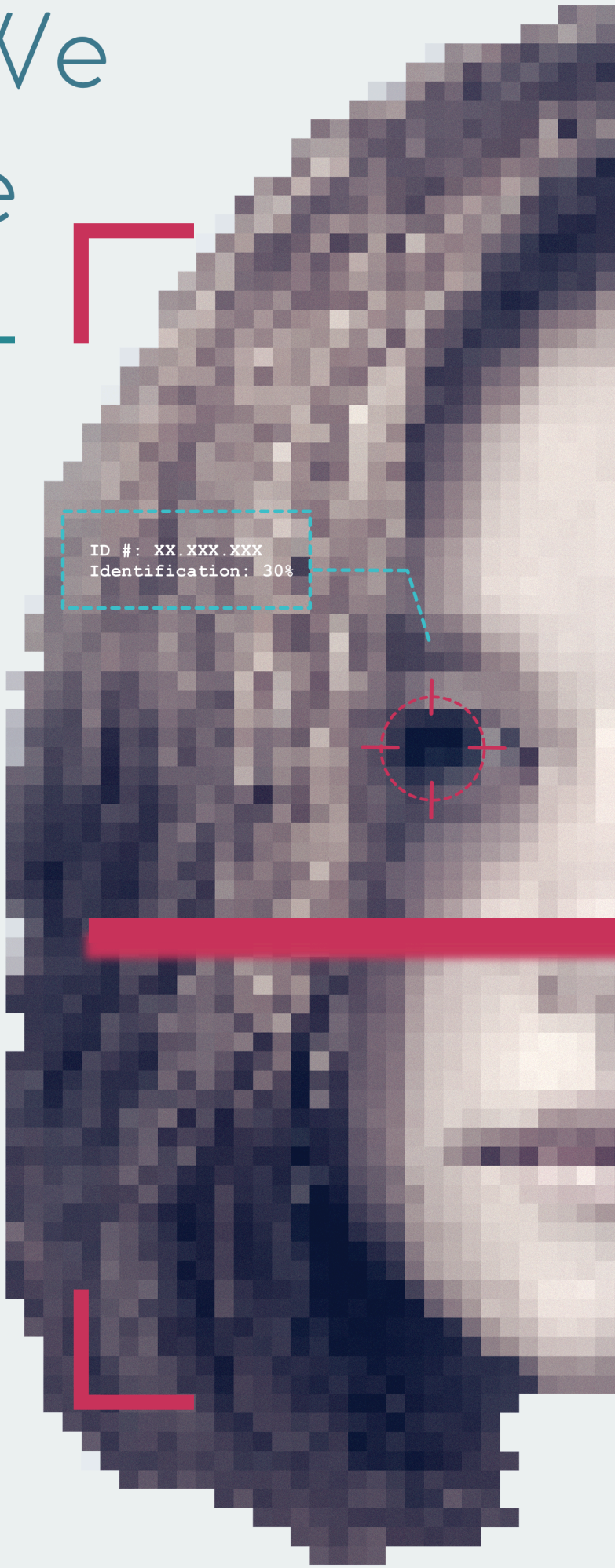
The Identity We Can't Change

How biometrics undermine our human rights



por los Derechos Civiles

Digital Area
Asociación por los Derechos Civiles

With the support of
PRIVACY INTERNATIONAL

December 2017
https://adcdigital.org.ar

This report was produced as part of a project funded by the International Development Research Centre (IDRC), it is published under a Creative Commons Attribution-NonCommercial-ShareAlike license.
To see a copy of this license, visit:
https://creativecommons.org/licenses/byncsa/2.5/

The report *The Identity We Can't Change. How biometrics undermine our human rights* is for public dissemination and has no commercial purpose.

Table of contents

The Identity We Can't Change

How biometrics undermine our human rights*

I Introduction

At the beginning of 2015, ADC published a report "Si nos conocemos más, nos cuidamos mejor" ["The more we know ourselves, the more protected we are"][1], which focuses on the analysis of biometric policies in Argentina. This work represented the first step of the organization toward studying surveillance technologies that are based on individuals' biological and behavioural features, and, in particular, it sought to shed light on the main state system designed to that end: the Federal Biometric Identification System for Security, referred to as SIBIOS [For its acronym in Spanish] and globally catalogued as one of the most invasive systems regarding people's privacy.[2]

This first approach allowed us to arrive at some conclusions. On the one hand, the legal framework based upon which citizens' data is collected has a shady democratic status. On the other hand, the Argentine population has got used to and naturalised this kind of practices, compared to other countries around the world, where the implementation of this type of systems has encountered various degrees of resistance on the part of citizenship.[3] Finally, the research showed us that prior to the report being published, SIBIOS had not yet been fully implemented.

This document is meant to be the continuation and updated version of the work we began some years ago. In order to be as accurate as possible and facilitate the understanding of this report, we

*This report was produced by **Leandro Ucciferri**, lawyer and researcher of the Digital Area at Asociación por los Derechos Civiles [ADC, for short]. ADC Digital Area Director **Valeria Milanes**, Digital Area lawyer and researcher **Eduardo Ferreyra** and Strategic Litigation Director **Alejandro Segarra** have also collaborated. Design and layout: Leandro Ucciferri. English translation by: Rodrigo Sebastián.

[1] "Si nos conocemos más, nos cuidamos mejor", ADC, 2015, available in (PDF): http://www.adc.org.ar/wp-content/uploads/2015/05/InformeBiometriaADC2015.pdf

[2] Infobae interview with Julián Assange, June 2013: https://www.youtube.com/watch?v=h_Q6kLqpRuA

[3] A case in the UK (2010) is worth mentioning: "Success Story: Dismantling UK's Biometric ID Database", EFF, https://www.eff.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database; as well as the case in Australia described in the following report by Privacy International in 1996: "On Campaigns of Opposition to ID Card Schemes", https://www.privacyinternational.org/node/921

will explain some concepts and information we have already included in our previous document.

In order to obtain detailed and relevant information to update our work, we filed a request for access to public information, which is a crucial tool not only to enrich our research but also to provide evidence regarding the transparency of the State when it comes to sensitive issues such as security and surveillance. The requests were made before the Ministry of Security, the Ministry of Interior, the Ministry of Modernisation (specifically the National Office of Information Technology) and the National Data Protection Directorate (DNPDP, for its acronym in Spanish).

The report will unfold as follows. In the second chapter, we explain the areas of concern in the field of biometrics from a technical point of view; we also explore the effects of surveillance on people's behaviour and briefly describe how the world in general sees the use of technology in identifying individuals. The third chapter is devoted to the Federal Biometric Identification System (SIBIOS), where we analyse the way it works, the data it collects, the process of collecting said data, the agencies and provinces that are part of the System, the technology used, and the practical uses of the System. Finally, in the fourth chapter we ponder the implementation of technology for biometric identification in relation to the actual and potential violation of fundamental rights that may result from implementing said system the way it is being done.

II Biometrics and human rights

i The infallible (in)security of biometric technology

Biometrics refers to the process used to recognise, authenticate and identify an individual based on their physical or behavioural traits. It is generally classified into three types of characteristics: biological, morphological and behavioural.

Biological characteristics include DNA and blood; morphological characteristics include hand geometry, palm prints, fingerprints, palm veins, face features, iris and retina vein patterns, voice and ear print. Finally, behavioural characteristics include gait, signature and typing rhythm.

The introduction of biometrics in the technology we use daily has made an enormous leap forward in the last few years. A clear example is the popularity gained by fingerprint recognition among manufacturers of devices who use it to protect these items, transitioning from a business-oriented professional niche to products targeted at the general public. The use of fingerprint scanners in our smartphones and tablets –as is the case with Apple's products and the main manufacturers of Android cell phones– began to naturalise the use of biological traits in our daily routine: we unlock our smartphone approximately 80 times a day[4], we buy applications and multimedia content just by

[4] "Apple says the average iPhone is unlocked 80 times a day", Nick Statt, The Verge, April 2016, http://www.theverge.com/2016/4/18/11454976/apple-iphone-use-data-unlock-stats

placing the finger on the reader. Likewise, Microsoft has introduced a new function in the latest versions of its operating system which grants access to users through their fingerprint (notebooks have been implementing this technology since the turn of the century) or face authentication, known as Windows Hello. [5]

As stated by Deibert: "One of the more lucrative of these markets, and potentially the most troubling for privacy, is for biometrics and facial recognition systems. While developed for military, law enforcement, and intelligence purposes – approximately 70 percent of current spending – the broader consumer market is growing fast. Many social media and mobile platforms use facial recognition technology on their digital photo apps so that users can tag, categorize, and verify their own and their friends' identities."[6]

Even though it is praised as an infallible technology, biometrics is not exempted from being vulnerable.[7] In this sense, it is worth considering two key aspects in the analysis of the systems that use biometric data.

In the first place, our biometric data is public for the most part. Given its nature, it is not confidential at all compared to passwords. This characteristic poses an obstacle when using biometrics as a security or protection measure.

Our facial features are readily accessible through the photos we publicly upload to the internet on a daily basis; they can even be analysed from the photos we are taken without our realising it. Our fingerprints may be obtained from an innumerable amount of elements we touch daily on our way; they can even be used without our consent, as was the case with the six-year-old boy who used his mother's thumb while she was sleeping in order to buy presents in Amazon.[8]

Many experts in computer security and researchers have explained how easy it is for fingerprints to be recreated using photos. This was observed in a study carried out by a group of Japanese researchers who were able to capture the fingerprints of people who were making the peace sign when posing for a photo.[9] On the other hand, hacker Jan Krissler delivered a presentation on the 31st Chaos Communication Congress (2014)[10], an annual meeting of hackers, security and technology, in which he demonstrated his method for copying and recreating fingerprints using a glass bottle, a

[5] Windows Hello face authentication

[6] Deibert, Ronald J. "Black Code: Surveillance, Privacy, and The Dark Side of the Internet", 2013, P.67.

[7] Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection, Galbally, Fierrez, Ortega-Garcia, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.186.3317

[8] Your Children Already Know What They're Getting for Christmas—Thanks, Internet", Laura Stevens, The Wall Street Journal, December 2016, https://www.wsj.com/articles/those-ads-that-follow-you-around-the-internet-are-ruining-christmas-1482507745

[9] "Japan researchers warn of fingerprint theft from 'peace' sign", Phys.org, January 2017, https://phys.org/news/2017-01-japan-fingerprint-theft-peace.html

[10] The Chaos Communication Congress is organised by the Chaos Computer Club, for more information please visit: https://www.ccc.de/en/

smartphone screen and a photo; in this case of German Defence Minister Ursula von der Leyen.[11]

Studies on the use of fingerprint models designed to bypass biometric systems have been conducted since the beginning of the century. In 2000, Putte and Keuning carried out and developed numerous analyses and methods for counterfeiting fingerprints –both with and without the co-operation of the owner– and arrived at the conclusion that 5 out of 6 fingerprint scanners accepted them in the first attempt, while the sixth scanner did so in the second attempt.[12] In 2002, Matsumoto, Yamada, and Hoshino examined 11 types of biometric identification systems in which they tested copies of "gummy" fingerprints made of gelatine and they found that all of the fingerprint systems accepted the gelatine fingerprints with the probability of more than 67%.[13] In May 2016, The Verge –a technology news and media network– published an article where they describe a technique used to counterfeit fingerprints in order to unlock a smartphone.[14]

Based on the abovementioned, when the State collects citizens' fingerprints, what precautions are taken to avoid the manipulation and counterfeiting of the fingerprint dummies stored? What kinds of safeguards are needed to secure the integrity of any data obtained?

Secondly, biometric data cannot be replaced. If we forget our password or someone steals it, we can create a new one. In the case of biometrics, this is practically impossible; how do we go about generating new fingerprints for our fingers? Let alone a new face, a new voice, a new iris?

According to Dr. Hugo Scolnik:[15] "All identification methods first collect an individual's information (fingerprints, face features such as spacing of the eyes, mouse size, nose width, etcetera) and then set a "distance" with respect to the data stored in the database. If the "distance" is within "tolerance" rates, the person and their identity will match. Hence, results depend on both parameters and this explains potential errors, as a broad "tolerance rate" means a larger number of "coincidences" while a small tolerance rate means there are bound to be no coincidences, given that factors such as lighting, camera angle, background colours, among others also play a role."[16]

[11] "Hacker fakes German minister's fingerprints using photos of her hands", Alex Hern, The Guardian, December 2014, https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands Click on the following link to see the complete presentation in the CCC –in German: https://www.youtube.com/watch?v=YE1EoxKV53w

[12] "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned", Ton van der Putte and Jeroen Keuning, 2002, https://cryptome.org/fake-prints.htm

[13] "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems", Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino, 2002, https://cryptome.org/gummy.htm

[14] "Your phone's biggest vulnerability is your fingerprint", Russell Brandom, May 2016, http://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security

[15] B. Math from the University of Buenos Aires and PhD in Mathematics from the University of Zurich. Head Consultant Professor, Department of Computer Sciences at FCEN-UBA and CEO at Firmas Digitales SRL. Since 2009 he has been Adjunct Director at the Master's programme in Computer Security at the University of Buenos Aires.

[16] Report developed for Asociación por los Derechos Civiles, December 2016. Filed in ADC's Database.

Designers of biometric identification systems describe three types of error rates:[17]

- **False Reject Rate**: The system does not allow valid access when it should;
- **False Accept Rate**: The system allows access when it should not;
- **Crossover Error Rate**: The point at which the False Reject Rate equals the False Accept Rate.

The process of biometric identification is based on statistics, it is not just a matter of a "yes or no" answer; quite the contrary, it is a process of probabilities which involves striking a balance between error rates depending on the expected results obtained through the identification system. The outcome will be a more or less reliable identification. Considering that error rates are exclusively determined by those designing the technology, several factors are at stake in this respect which may turn the system into a tool capable of violating human rights.

A recent study from the Centre on Privacy & Technology from the University of Georgetown established that compared to fingerprinting, face recognition is significantly less reliable and well-tested.[18] Poor reliability of face recognition systems results from the way certain factors influence how algorithms[19] determine the probability of identification or verification of a person.

In this sense, the camera's angle, variable backgrounds, lighting (whether it is natural or artificial, time of day, etcetera), database size used by the system (that is, the number of people's photographs), ageing, facial hair, facial expressions, objects obstructing the face (such as hair, glasses, hats or caps), may alter the result obtained by the algorithm of the face recognition system.[20]

Yet, there is an ongoing basic problem. It is generally believed that technology is amoral, objective and neutral. This may be true when we think about technology in the abstract, that is, its concrete applications. However, we cannot separate the material object from the purpose or use for which it

[17] Hidden Risks of Biometric Identifiers and How to Avoid Them", Dr. Thomas P. Keenan, Blackhat 2015. https://www.blackhat.com/docs/us-15/materials/us-15-Keenan-Hidden-Risks-Of-Biometric-Identifiers-And-How-To-Avoid-Them-wp.pdf

[18] "The Perpetual Line-up: Unregulated Police Face Recognition in America", C. Garvie, A. Bedoya, J. Frankle, Center on Privacy & Technology, Georgetown University Law School, October 2016. https://www.perpetuallineup.org/findings/accuracy

[19] An algorithm is an "a procedure for solving a mathematical problem (as of finding the greatest common divisor) in a finite number of steps that frequently involves repetition of an operation". https://www.merriam-webster.com/dictionary/algorithm

[20] More information can be found in: "Face Recognition Vendor Test: Performance of Automated Gender Classification Algorithms", M. Ngan, P. Grother, NIST Interagency Report 8052, available in: http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8052.pdf; "Biometric Recognition: Challenges and Opportunities", J. N. Pato, L. I. Millett, The National Academies Press, available in: https://www.nap.edu/read/12720/chapter/1; "Face Recognition Algorithms", I. Marqués, País Vasco University, available in: http://www.ehu.eus/ccwintco/uploads/e/eb/PFC-IonMarques.pdf

was created. Thus, the objectivity of technology is a relative concept, as technology reproduces the biases of the individual who uses it to achieve a particular end.[21]

Taking into account that algorithms are a set of instructions or rules designed to find a solution to a problem, we must depart from the fact that such instructions have been decided upon by an individual whose bias and prejudices may, consciously or unconsciously, extrapolate to the moment they write the algorithm code (algorithmic bias),[22] considering that they are the ones who will ultimately decide on the design used in the development of the technology;[23] this occurs more often in the case of machine learning algorithms[24], where biases may be replicated and learned by the algorithm without human intervention.

To overcome the problems of face recognition accuracy, field experts agree that a human reviewer must double-check the results of the searches to ensure that they are correct. However, according to the Georgetown study, "Simple human review of results is not enough [...]. Without specialised training, human reviewers make so many mistakes that overall face recognition accuracy could actually drop when their input is taken into account. Humans instinctively match faces using a number of psychological heuristics[25] that can become liabilities for police deployments of face recognition. For example, studies show that humans are better at recognizing people they already know and people of the same race."[26]

This calls for an important question to ponder regarding technology, which bears more relevance when the user is the State itself. When we buy technology to give life to biometric identification systems, do we take into account their characteristics?

Regardless of the formal contracting procedures followed in the public sphere, as is the case with tendering, which strive to guarantee the correct use of public funds and transparency in the process of acquiring goods or services, the purchase of technology requires that certain considerations be

[21] Is Technology Neutral? Part II", Colin Rule, The Centre for Internet and Society, Stanford Law School, September 2006, https://cyberlaw.stanford.edu/blog/2006/09/technology-neutral-part-ii

[22] "The Foundations of Algorithmic Bias", Zachary C. Lipton, November 2016, http://approximatelycorrect.com/2016/11/07/the-foundations-of-algorithmic-bias/

[23] More information can be obtained from the following sources: "When Algorithms Discriminate", Claire C. Miller, The New York Times, July 2015, https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html; "Why We Should Expect Algorithms to Be Biased", Nanette Byrnes, MIT Technology Review, June 2016, https://www.technologyreview.com/s/601775/why-we-should-expect-algorithms-to-be-biased/; and specifically on algorithms applicable in facial recognition: "Google apologises for Photos app's racist blunder", BBC News, July 2015, http://www.bbc.com/news/technology-33347866

[24] https://en.wikipedia.org/wiki/Machine_learning

[25] "In psychology, heuristics are simple, efficient rules which people often use to form judgments and make decisions. They are mental shortcuts that usually involve focusing on one aspect of a complex problem and ignoring others". https://en.wikipedia.org/wiki/Heuristics_in_judgment_and_decision-making

[26] "The Perpetual Line-up: Unregulated Police Face Recognition in America", C. Garvie, A. Bedoya, J. Frankle, Center on Privacy & Technology, Georgetown University Law School, October 2016, P.49. https://www.perpetuallineup.org/

born in mind when choosing the type of solution that will be used for running a system and deciding how it will meet the needs of the user in relation to the goals they have in mind.

Throughout this section of the report, we have mentioned some of the main problems inherent to the functioning of the software used in biometric identification systems. In this sense, any acquisition made of this technology must be based and decided upon the analysis of minimum factors such as the accuracy of the identification or verification software (facial, fingerprinting, etcetera), which calls for an answer to and assessment of questions such as: have algorithms been tested?; if so, to what extent?; what were the results?; how was the algorithm trained?; may conflicts arise regarding the identification/verification of certain ethnic groups?; is there an assessment of the overall security of the system that will be used?

So far, we have seen some of the vulnerabilities that may be found in biometric identification systems per se, yet we should highlight another problem we may encounter in the implementation of biometric identification systems: the centralisation of information in a unique database.

Martin Scheinin, United Nations' former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, stated in his report published in 2009 that, while the use of biometrics can, in some circumstances, be a legitimate tool for the identification of terrorist suspects, the Special Rapporteur is particularly concerned about "cases where biometrics are not stored in an identity document, but in a central database, thereby increasing the information security risks and leaving individuals vulnerable. As the collection of biometric information increases, error rates may rise significantly." [27]

The increase in error rates may result in the wrongful criminalization of individuals or social exclusion. Meanwhile, the Rapporteur highlights an aspect we mentioned before: the irrevocability of biometric data. "(...) once copied and/or fraudulently used by a malicious party, it is not possible to issue an individual with a new biometric signature."[28]

The inherent danger of centralised databases naturally lies in their characteristics: being the only point of access, storage and exchange of information. From a computer security standpoint, this raises serious concerns in relation to the measures that must be taken to protect the data stored therein. If adequate precautions are not taken, any individual could access the whole amount of information stored in the servers.

In this regard, it is worth commenting on a recent landmark case on IT security involving the main ministry in charge of SIBIOS. By the end of January 2017, the account of Security Minister Patricia Bullrich, along with 30 institutional e-mail accounts from said Ministry, were hacked as a result

[27] Report of United Nations' Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 2009, P.10-11. http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

[28] Ibid.

of phishing[29], as informed by the Department of Cybercrime of the Argentine Federal Police[30] and noticed by Twitter users while the accounts were being manipulated.[31]

These events show there is a systematic lack of attention and importance placed on the security of the information handled by state agencies. Meanwhile, there are concerns about the capacity of the Ministry's personnel to maintain basic information security practices designed to overcome the ever-growing issues of the digital world.

With respect to cybersecurity, ADC did a study on the situation in Argentina from 2011 to mid 2016, where emphasis is laid on the lack of a national strategy in place to face the challenges befalling the country in cybersecurity matters, including public and private infrastructure, information security and cybercrime, just to name a few.[32]

ii The invisible effects of surveillance

When dealing with technologies that facilitate the massive identification of humans, one of the aspects we cannot fail to address is the effect surveillance has on the exercise and enjoyment of our human rights (*chilling effects*[33]).

As stated by Scheinin, "In addition to constituting a right in itself, privacy serves as a basis for other rights and without which the other rights would not be effectively enjoyed."[34] Privacy is a person's right to decide by themselves to what extent they are willing to share their thoughts, feelings and personal experiences with others.[35] Thanks to it we can create spaces to compartmentalise all that makes us human, such as our family and romantic ties, friendships, professional relationships, our tastes, thoughts and all that which defines our personality.

Thanks to the privacy zones this right allows us to have, we are able to fully exercise other rights and freedoms, particularly freedom of speech, freedom of thought, freedom of association and assembly, freedom of worship, as well as the freedom to request and receive information.

[29] Phishing involves identify theft, generally in a website, and is carried out by scamming a victim in order to steal their information, such as their login credentials (username and password), credit cards, etcetera. For more information please visit http://www.welivesecurity.com/la-es/2015/05/08/5-tipos-de-phishing/

[30] "They also hacked 30 e-mail accounts from the Ministry of Security", La Nación, February 2017, http://www.lanacion.com.ar/1980702-tambien-hackearon-30-correos-del-ministerio-de-seguridad

[31] "El hackeo a @PatoBullrich y al @MinSeg", January 2017, https://twitter.com/i/moments/824754207437766656

[32] "Cybersecurity in the mass surveillance age", ADC, 2016 https://adcdigital.org.ar/portfolio/cybersecurity-in-the-mass-surveillance-age/

[33] Chilling effect is a term used in common-law that describes a situation where a speech or conduct is suppressed by fear of penalization at the interests of an individual or group.

[34] Report of Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 2009, P.13. http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

[35] Indalia Ponzetti de Balbin vs. Editorial Atlántida S.A. s/Damages, National Supreme Court of Justice, December 1984 http://bit.ly/2oM7SJf

Surveillance affects the behaviour of those surveilled.[36] People tend to change their behaviour when they know or suspect they are being surveilled by third parties for fear of facing reprisals or unintended consequences. In the digital arena, this may imply censoring comments of their own they would normally post on their Facebook or Twitter accounts and refraining from searching certain topics on the internet or from consuming certain types of multimedia material on Youtube, Vimeo, Netflix and Spotify, just to name a few. The effect of surveillance is even more serious in those cases where individuals are prevented from filing claims against abuses of power and injustices. In other words, these are cases where people wish to dissent but do not feel safe fully exercising their democratic right to protest against government policies or against those retaining power.

The feeling of public exposure, of losing control over our information, interests and relationships, in other words, of losing that which makes up our image and personality may lead to self-imposed seclusion and self-censorship when expressing our ideas and thoughts. Besides, it limits the development of our relationships and those qualities that make us human.

In this sense, biometric identification may also lead to conflicts involving our freedom of speech, considering technology may be used by different actors to monitor those who wish to participate in political and religious activities or in other activities protected by freedom of speech. This gets even more problematic when protests and public demonstrations are recorded by law-enforcement agencies such as the Argentine Federal Police, a practice that has become more common throughout the years.[37]

Biometric identification technologies, and face recognition in particular, have redefined the concept of public space as we previously understood it. This change has been brought about by the arrival of surveillance cameras (CCTV) and is heightened by technologies that make it possible to delve into the public lives of individuals on the pretext of crime investigations.[38]

The fact that we carry out some actions in public doesn't mean we intend them to receive public exposure; quite the contrary, they may be considered to fall within the scope of private life. This is what the European Court of Human Rights ruled in the case Peck v. United Kingdom (2003)[39],

[36] "The Chilling Effect of Mass Surveillance Quantified", Tim Cushing, Techdirt, May 2016, https://www.techdirt.com/articles/20160429/07512934314/chilling-effect-mass-surveillance-quantified.shtml

[37] The following tweets can be consulted in relation to the protests and social movements' demonstrations recorded by the Argentine Federal Police:: caso 1; caso 2; caso 3; caso 4; caso 5; caso 6; caso 7; caso 8; caso 9

[38] At the beginning of 2013, the government of the City of Buenos Aires considered the possibility of implementing facial recognition technology in security cameras installed in the underground network in order to detect potential criminals. http://www.infobae.com/2013/01/13/691102-evaluan-un-software-identificacion-facial-ubicar-pungas-el-subte/

[39] In the case Peck v. United Kingdom, the applicant complained about disclosure in the media of material recorded by the close circuit television (CCTV), which resulted in the publication and broadcasting of images that showed him attempting suicide. The local authority running the system, Brentwood Borough Council, had passed the images to the media in order to show the effectiveness of the system in detecting and preventing crime. The Independent Television Commission (ITC) and the Broadcasting Standards Commission (BSC) considered that the

thus establishing that there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life.

On the other hand, in common law there is the reasonable expectation of privacy test[40] used ever since the case Katz v. United States (1967), the Supreme Court of the United States established that the Fourth Amendment of the Constitution protects people, rather than places, and created a two-part test: on the one hand, an individual has exhibited an actual (subjective) expectation of privacy, and, on the other hand, the expectation is one that society is prepared to recognize as reasonable.[41]

iii Argentina, the only one in the world?

The States' adoption of nationwide ID systems across the world has been controversial. The societies of many countries, such as Australia, Canada, New Zealand, United Kingdom and the United States, have successfully opposed national ID schemes designed for their citizens.[42] Meanwhile, in Argentina, the National Identity Document [DNI, for its acronym in Spanish] has a key role in the life of Argentine citizens. Designed to "identify, enrol and classify the national human potential", the DNI has become so ingrained in society throughout the years that inhabitants take it for granted in the exercise of their rights and duties. It facilitates the interaction with the State and other private individuals.

masking was inadequate as his neighbours, colleagues, friends and family recognised him from the TV programmes. The European Court of Human Rights held that releasing and broadcasting the images amounted to a serious infringement of Article 8 of the European Convention. The Court emphasised that the applicant was in a public street, but he was not there for the purposes of participating in any public event –nor was he a public figure–, and that the release of the images was uncalled for in a democratic society. Case of Peck v. United Kingdom, European Court of Human Rights, January 2003, http://merlin.obs.coe.int/iris/2003/6/article2.en.html More information available in: "CCTV and Human Rights: the Fish and the Bicycle? An Examination of Peck V. United Kingdom (2003) 36 E.H.R.R. 41", Caoilfhionn Gallagher, Surveillance & Society, 2004, http://www.surveillance-and-society.org/articles2(2)/humanrights.pdf

[40] With respect to "expectation of privacy": https://www.law.cornell.edu/wex/expectation_of_privacy

[41] In the case Katz v. United States, the petitioner used a public telephone booth to transmit wagering information without knowing that FBI agents were overhearing the call through an electronic listening and recording device they had attached to the outside of the public telephone booth, which led to his subsequent conviction. Katz appealed his conviction on the grounds that the recordings had been obtained in violation of the Fourth Amendment of the Constitution. The case reached the Supreme Court, which decided in favour of Katz, holding that an enclosed telephone booth is an area where, like a home, a person has a constitutionally protected reasonable expectation of privacy; that electronic, as well as physical, intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment, and that the invasion of a constitutionally protected area by federal authorities is presumptively unreasonable in the absence of a search warrant. In the Katz case, the Court declared that eavesdropping carried on by federal or state authorities is subject to the requirements of a search warrant under the Fourth Amendment. Katz v. United States, Supreme Court of the United States, December 1967, https://www.law.cornell.edu/supremecourt/text/389/347

[42] "Mandatory National IDs and Biometric Databases", Electronic Frontier Foundation, https://www.eff.org/issues/national-ids

In our first analysis of the evolution of biometric policies in Argentina, we noticed their shady democratic status. Regarding the massive identification of individuals, it was decree-Act 17,671 which established the National Identity Document under Juan Carlos Onganía's military dictatorship, which was a turning point for the Argentine society.

The unquestionable role of citizens' identification ingrained in Argentina thanks to the fact that the policies introduced were not implemented through legislation, but as technological updates masked under the modernisation of the State. Hence, they were justified on the grounds of a decree-Act signed during a military dictatorship, which has not only completely influenced the course taken in this kind of public policies, but has also prevented citizens from accessing any type of information or participating in debates which are, without a doubt, of public interest.

The identification of persons by means of biometric data has become an ever-growing trend across the world. Nowadays, this kind of technology is being implemented in countries such as Australia, Brazil, Canada, Gambia, Germany, Iraq, Israel, Italy, Norway, Ukraine, United Kingdom, United States and the Netherlands, to name a few.

According to the study done by Georgetown University, half of American adults are enrolled in facial-recognition databases.[43] Police departments in various states use facial-recognition software to compare surveillance images against databases of ID photos (for example, driver's license, passport), not only to confirm the identity of a suspect who has been detained, but also to analyse footage from surveillance cameras to examine certain movements made by a person.

The Centre on Privacy and Technology determined that the algorithms used to identify matches are inaccurate about 15% of the time, and are more likely to misidentify black people than white people. On top of that, the FBI, among other agencies, does not test for false positives or for racial bias on the account that the system is "race-blind". This has troubled the CPT, as it considers that the FBI ignores how often the system incorrectly identifies the wrong subject. On the other hand, according to Alvaro Bedoya, executive director of the CPT, there is no federal law controlling this technology, nor a court decision limiting it.[44]

India is one of the most paradigmatic cases when it comes to the identification of individuals. The unique identification system implemented in 2010, known as *Aadhaar*, is the largest in the world, with 1,2 billion registered users by March 2017.[45] Residents may obtain their *Aadhaar* number after submitting their demographic and biometric information (including fingerprints, iris scans, and

[43] "Half of American Adults Are in Police Facial-Recognition Databases", Kaveh Waddell, October 19, 2016, https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/

[44] "Facial recognition database used by FBI is out of control, House committee hears", Olivia Solon, March 27, 2017, https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports

[45] "State-wise Aadhaar Saturation", Unique Identification Authority of India. Consulted on March 23, 2017, available in: https://uidai.gov.in/enrolment-update/ecosystem-partners/state-wise-aadhaar-saturation.html

photographs).[46] This system has been gaining greater importance in the daily life of citizens, as it has become mandatory for recording property deeds, filing income tax returns, opening bank accounts, accessing academic scholarships as well as schools and universities, accessing state subsidies (for example, for meals and gas), obtaining passports and driving licenses, and obtaining a SIM card.

The mandatory nature of Aadhaar has excited controversy,[47] with the Supreme Court holding that it cannot be made mandatory for accessing welfare schemes.[48] On the other hand, experts from the Indian civil society have challenged the safety of the system and underlined the need for a legal reform that guarantees better rights in relation to how collected biometric data is handled.[49]

To sum up, in answer to the question raised at the beginning of this chapter, the Argentine case is part of a growing global trend regarding the adoption of technological solutions that use people's biometric data to identify and control them. The adoption of a unique document is not something necessary or unavoidable. As we have seen, there are countries with large democratic traditions which do not demand a unique ID, as the impact this type of policies may have on fundamental rights has been pondered in citizens' debates and petitions. Taking into account that the identification policies used in the Argentine society stem from de facto governments, it is clear that the reasoning behind this type of measures is linked to the State's craving for control, which is inconsistent with a completely democratic tradition, despite the fact these practices have been naturalised in society.

III The Federal Biometric Identification System for Security

The Federal Biometric Identification System for Security (SIBIOS) was introduced in 2011 by decree 1766. It is based on the logic of security and crime prevention. Before delving into the content of the decree, it is worth considering decrees per se, as an instrument used to introduce public policies in a way that curtails fundamental rights, as is the case with the right to privacy.

Based on constitutional grounds, article 18 establishes the rule of law principle, which mandates that State actions must be carried out pursuant to laws previously debated and enacted by the National Congress in an effort to avoid the arbitrariness of individual government officials in power.

When it comes to human rights, international instruments, agreements and conventions establish the states of exception in which the exercise and enjoyment of rights contemplated therein may

[46] "State of Privacy: India", Privacy International and Centre for Internet and Society, March 2017, https://privacyinternational.org/node/975

[47] "10 things you need Aadhaar for": https://www.youtube.com/watch?v=578WwTwcNyk

[48] "Aadhaar cannot be made mandatory for welfare schemes: Supreme Court", Indian Express, March 27, 2017, http://indianexpress.com/article/india/cannot-make-aadhaar-mandatory-for-welfare-schemes-supreme-court-to-centre-4587325/

[49] "Aadhaar uses fingerprints, linked to bank accounts: Is your identity safe?", Pranesh Prakash, April 2, 2017, http://www.hindustantimes.com/india-news/what-s-really-happening-when-you-swipe-your-aadhaar-card-to-make-a-payment/story-2fLTO5oNPhq1wyvZrwgNgJ.html

be restricted. In this sense, the Universal Declaration of Human Rights establishes in article 29, section 2, that "In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society"[50]; likewise, the American Convention on Human Rights establishes in article 30 that "The restrictions that, pursuant to this Convention, may be placed on the enjoyment or exercise of the rights or freedoms recognized herein may not be applied except in accordance with laws enacted for reasons of general interest and in accordance with the purpose for which such restrictions have been established."[51]

In 1999, General Comment No 27,[52] the Human Rights Committee –a body in charge of monitoring the implementation of the International Covenant on Civil and Political Rights (ICCPR)– adopted a position regarding the parameters that must be observed when limitations are imposed on the rights protected under the ICCPR by establishing a framework to analyse public policies that may impact fundamental rights.

Adopting this biometric system by decree means avoiding the well-deserved reflection and debate that the use of biometric data should have in Congress. For example, biometric data are a type of sensitive data under the genre of personal data, and the recognition of this particular type of data as "sensitive data" is still pending. The direct link between the lack of analysis and legal status, coupled with the impact of this type of information on fundamental rights (privacy and informational self-determination, in this case), would render the SIBIOS system at fault with the rule of law principle afforded by the Constitution and international agreements.

Pursuant to article 3 of Decree 1766/11, the Argentine Ministry of Security is the enforcement authority of the System. Meanwhile, the party responsible for the administration and maintenance of said system is the Argentine Federal Police through the Scientific Police Division.

Article 5 of Decree 1766 establishes the creation of a Coordination Unit within the Ministry of Security which must consist of representatives from said Ministry, RENAPER [Spanish acronym for National Registry of Persons] and the National Migration Office. Besides, it must follow advice from field experts such as the scientific police of the Argentine Federal Police, Gendarmerie, the Argentine Naval Prefecture and Airport Security Police. With regard to the aforementioned, given the sensitive nature of biometric data, it is necessary to highlight the absence of the National Data Protection Directorate (DNPDP, for its acronym in Spanish) as specialist experts of the Ministry of Security.

In response to the inquiry made in our request for information regarding the activities carried out

[50] http://www.un.org/es/universal-declaration-human-rights/

[51] https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

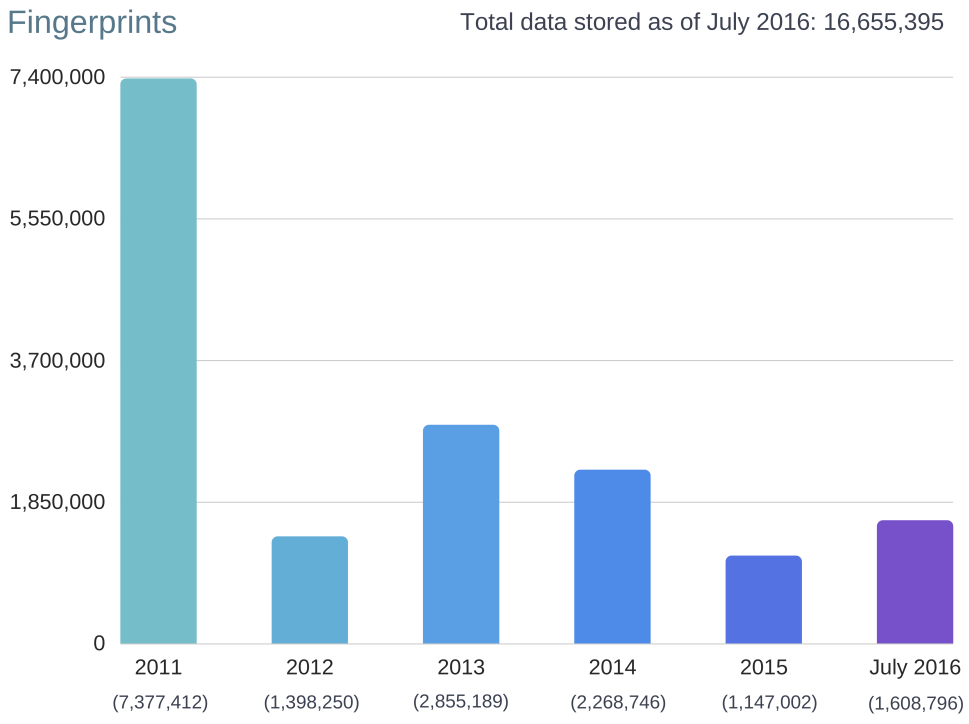
[52] http://hrlibrary.umn.edu/gencomm/hrcom27.htm

by the Coordination Unit, in terms of their tasks and actions (meetings, training, decisions taken, etcetera), the Ministry of Security established that up until September 2016, that is, almost five years after the Decree creating SIBIOS was signed, said unit had not yet been formed. In addition, it established that, in practice, the department in charge of coordinating SIBIOS is the National Scientific Police Division, under the authority of the Department of Organised and Complex Crime Investigations, within the scope of the Security Department of the Argentine Ministry of Security.

At the beginning of 2017, the Executive Power issued decree 243, which introduces modifications to articles of decree 1766.[53] Article 2 of decree 243 establishes that the Coordination and Monitoring Unit will be under the authority of the National Scientific Police Division previously mentioned, explaining in the recitals of the decree that the Unit had not been created as mandated by decree 1766. The advisory experts of the Unit were not replaced, with respect to which we insist on the absence of the DNPDP.

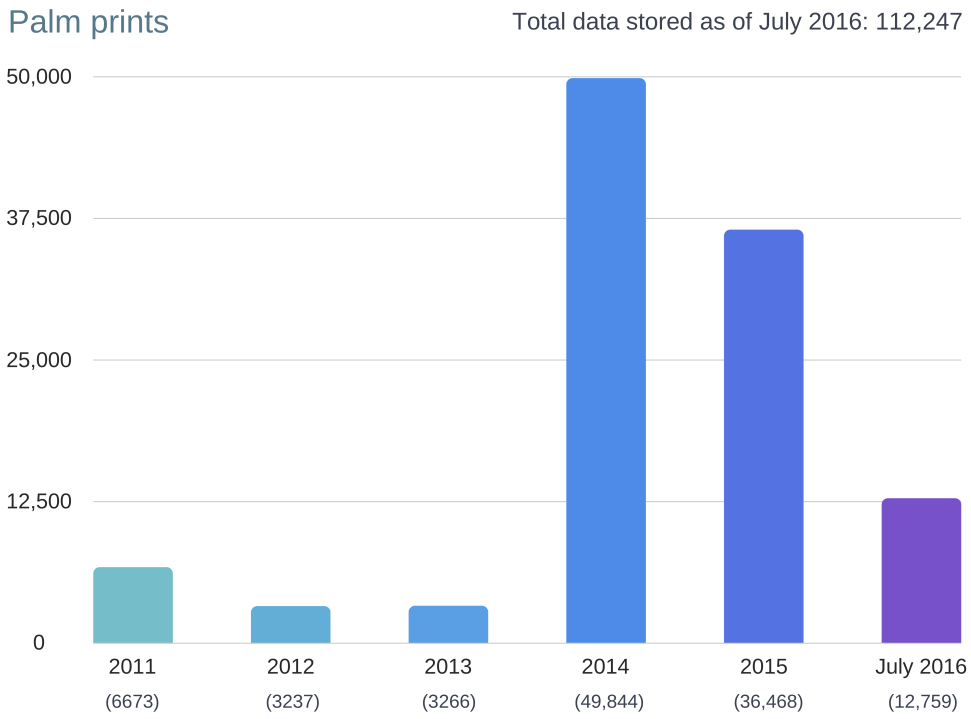
Based on the answer we received from the Ministry of Security upon ADC's request for information, the SIBIOS database is made up of two types of data: Biometric and demographic (that is, the name and surname used to identify a person).

The Ministry of Security establishes that the biometric data stored by SIBIOS are: fingerprints, palm prints and facial records (facial recognition). Below there follows three graphs done by ADC based on the information provided by the Ministry in relation to the total amount of data stored in SIBIOS per type of datum.

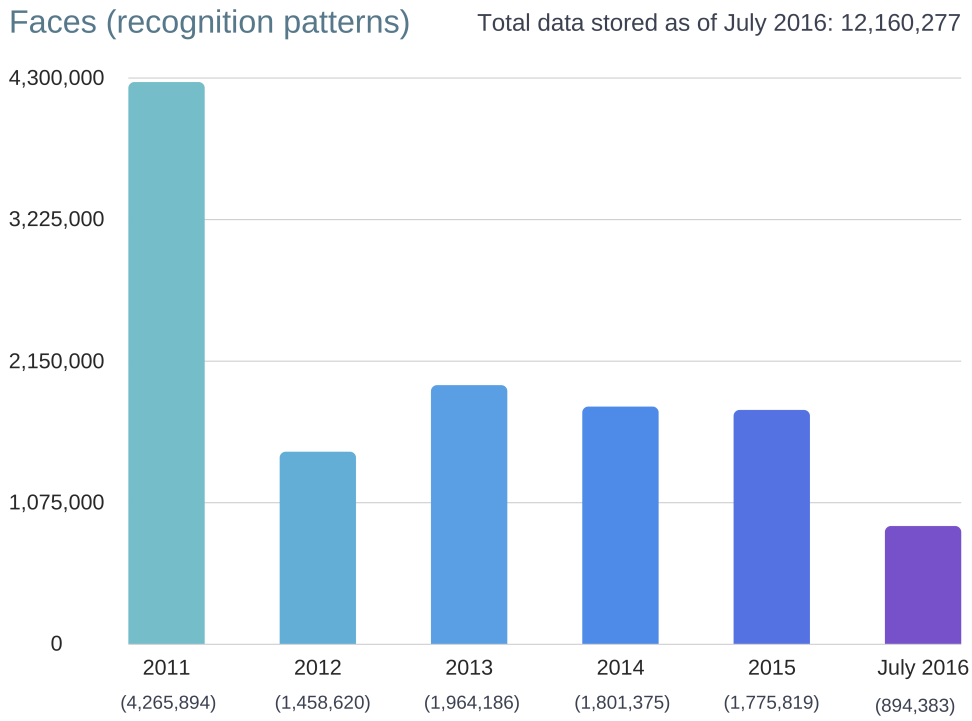


[53] Decree 243/2017, Official Gazette, https://www.boletinoficial.gob.ar/#!DetalleNorma/161771/20170410

Graph 1 prepared by the author, September 2016.



Graph 2 prepared by the author, September 2016.



Graph 3 prepared by the author, September 2016.

The decree seems to justify the implementation of biometric technology in two specific paragraphs, underlining "the importance of biometric identification for the purposes of verifying the identity of a person by means of a face recognition system used to contrast and analyse the information stored in a database designed for that end", and that for this reason, "it is indispensable to profit as much as possible from the technological devices available, considering that the use of biometric techniques is a fundamental contribution to the role of public security in crime prevention matters as well as in investigation and scientific police competences (...)."

Therefore, based on the abovementioned, the decree defending the implementation of SIBIOS seems to be incompatible with the test of admissible limitations established by international agreements, given that it fails to account for the need of the System in a democratic society and, even more seriously, to meet the goal proposed.

Considering that biometrics is not an infallible technology, as we saw in the chapter dealing with the various vulnerabilities that may affect biometric identification systems, and that the SIBIOS decree does not mention specifically the needs for implementing the system but only mentions vaguely the "essential protection of the right to security", and avoids explaining the concrete threats and including a factual, qualitative and quantitative analysis on the advantages/disadvantages of its implementation compared to the former system, the decree seems to be based on the logic of identifying individuals effectively and easily through biometric technology, not because it is the best solution for the concrete security need, but because it is available. When the legislative debate is bypassed, one loses perspective about the safeguards that must be in place to guarantee the exercise of human rights.

i How is data transferred to SIBIOS?

For SIBIOS to work as a centralised database, it is essential for it to centralise information from different state and law-enforcements agencies which, to a greater or lesser extent, used to have their own databases. The arrival of SIBIOS led all these independent databases to be digitalised (if they had not been digitalised previously) and uploaded to the System.

Since the databases in place before Decree 1766/11 were incomplete, and in order to enrol more than 40 million citizens, the main source to feed the SIBIOS database is the National Registry of Persons (RENAPER) of the Ministry of Interior, Public Works and Housing, which has since 2009 the power to "utilise digital technologies for the identification of national and foreign citizens."[54]

RENAPER is responsible for remitting biometric and demographic information collected through

[54] Decree 1501/2009, http://servicios.infoleg.gob.ar/infolegInternet/anexos/155000-159999/159070/norma.htm

the National Identity Document and National Passport. In 2012 both the digital DNI[55] and the electronic passport, which stores the holder's data and biometric information on a RFID chip [56] in order to identify them through their fingerprints, iris and/or face.[57]

On the other hand, given that SIBIOS wants to be a federal database, a scheme was established which allows each province to use the System and provide their own records. This way, Provincial States can sign the Act of Accession with the National State, after which the Scientific Police Division of the Argentine Federal Police proceeds to load the fingerprint cards (which show the full 10 fingers), faces, print palms and demographic data provided by the provincial Police in question. Later, the Province may request that the relevant records be introduced directly in order to keep the System updated.

In the request for information made before the Ministry of Security, we sought to determine the nature of the security measures and guarantees afforded by the infrastructure under which SIBIOS and the database feeding the system work. In relation to this, the Ministry answered that "the Electronic System of Registries and Identification Division of the Argentine Federal Police keeps a detailed track of the logins made by authorised users to access the System (...), through regular audits."

On the other hand, they added that "the various Agencies using the System (...), are subject to security measures, authenticity requirements, integrity, the duty of confidentiality, availability and compatible technical standards, all consistent with the provisions set forth in Article 23 and relevant articles of Act 25,326 of Personal Data Protection"; failing to describe the technical details underlying the security of the servers and system that feed SIBIOS, which was inquired by ADC in the request for information.

ADC also inquired whether there have been cases of non-authorised information extraction from SIBIOS and the Ministry of Security replied that "No registered cases of this nature have been notified to this Argentine Ministry of Security or the Argentine Federal Police."

ii What agencies are part of SIBIOS?

Pursuant to article 3 of Decree 1766, the main users of the System include: the Argentine Federal Police, the National Gendarmerie, the Argentine Naval Prefecture, the Airport Security Police, the National Registry of Persons and the National Migration Office. Other users include provincial police departments which have signed the Act of Accession.

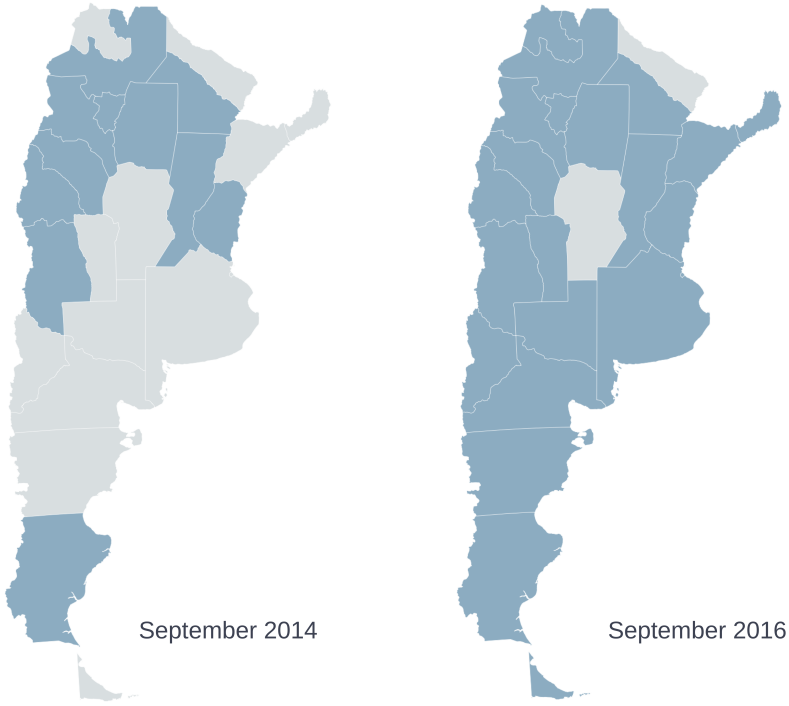
[55] Resolution 585/2012, National Registry of Persons, http://servicios.infoleg.gob.ar/infolegInternet/anexos/195000-199999/195199/norma.htm

[56] Radio Frequency Identification, https://es.wikipedia.org/wiki/RFID

[57] Resolution 1474/2012, National Department of the National Registry of Persons, http://servicios.infoleg.gob.ar/infolegInternet/anexos/195000-199999/198662/texact.htm

Decree 243/2017, signed at the beginning of April, establishes in article 1 that invitations to join SIBIOS should also be made available to "(...) all those agencies under the Executive or Judicial Power both at national and provincial levels as well as of the City of Buenos Aires (...)" so that they may submit biometric queries in real time, thus modifying article 4 of decree 1766.

In our previous report we found that out of the 23 provinces and the autonomous city, 11 provinces had joined SIBIOS by September 2014, namely: Chaco, Mendoza, San Juan, Tucumán, Catamarca, Santiago del Estero, Santa Fe, Santa Cruz, Entre Ríos, Salta, and La Rioja. The latest report provided by the Ministry of Security establishes that by September 2016, as shown in graphic 4, almost the entire number of provinces had joined SIBIOS, except for Córdoba and Formosa. However, there are some inconsistencies in the answer given by the Ministry of Security suggesting that SIBIOS, in fact, has already been implemented across the national territory, which we intend to clarify in our next request for information.



Graph 4 prepared by the author, September 2016.

Each SIBIOS user has a computer in their office that is set in such a way as to afford them access to the System and servers, where the database is located, through a Virtual Private Network.[58] Apart from the authorization required by the Ministry of Security for both the agency appearing as the

[58] A Virtual Private Network or VPN, for its acronym is English, "is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection, such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee." http://www.cisco.com/cisco/web/support/LA/7/74/74718_how_vpn_works.pdf

SIBIOS user and the individual responsible for it in the division, it is required that users take the System Operator Course, which is a training module provided by said Ministry.

The Ministry of Security states that the reasons for accessing the System include:

- Data queries
- Loading prints (fingerprints, palm prints, face images)
- Storing partial or complete fingerprints
- Storing partial or complete palm prints
- Storing face images
- Data comparison
- Uploading biometric data
- Uploading demographic data

iii The technology behind SIBIOS

Given that SIBIOS is a database used for identifying persons based on their biological information, apart from data itself (prints, face recognition, iris), the other fundamental part of the equation is the technology used for processing such information and for effectively running the System in the various state departments. After all, biometrics consists of the technology and processes which allow us to read the human body.

Based on the responses ADC obtained in reply to the requests for information made before the Ministry of Security and the Ministry of Interior, we were able to verify the technology developers that support SIBIOS. In this sense, we collected information from each ministry separately, as they use different technology providers.

i Ministry of Security

Up until 2012, the website *"biometría.gov.ar"*[59] stated on a footnote that they received support from agencies, mainly American, such as the National Institute of Standards and Technology, FBI Biometrics Centre of Intelligence and *"biometrics.gov"* (a website providing information on activities related to biometrics from the government of the United States), apart from INTERPOL.

[59] Please visit https://web-beta.archive.org/web/20121001201359/http://www.biometria.gov.ar for a version of the website to 1/10/2012

After uncovering this situation and consulting specifically what individuals or agencies and/or companies were collaborating in the development and implementation of SIBIOS, the Ministry of Security determined that the intervening company is "Morpho Safran", which installed and set up the equipment for the Automatic Fingerprint Identification System (AFIS, for its acronym in English), without giving further explanations.

SAGEM was a French company founded in 1924 and majorly involved in the development of defence electronics, consumer electronics and communication systems. In 2005, SAGEM and Snecma (Safran Aircraft Engines),[60] also of French origin, merged to form Safran Group[61], a company involved in the development of aircraft and rocket engines, aerospace-component and defence and security electronics.

Formerly known as Sagem Sécurité in 2007 and later changing its name to Morpho in 2010, today it is known as Safran Identity and Security. It operates as a subsidiary of Safran group and is involved in the development of biometric technology, with more than 8,400 employees in more than 40 countries around the world and revenues estimated at 1,5 billion euros.[62]

Product development includes solutions for the identification of individuals,[63] such as voter and citizen registration, National ID, travel documents (passports), vehicle and driver registration, healthcare and social benefits; for public security,[64] such as research tools (biometric identification of suspects, DNA, video analysis), migration controls and explosives and drug detection; and for the commercial sector,[65] where the focus lies on technology for telecoms and financial institutions.

Safran is the main provider of the FBI,[66] INTERPOL[67] and the New York Police Department (NYPD)[68], apart from the Transport Security Administration (TSA), an agency of the U.S. De-

[60] https://en.wikipedia.org/wiki/Snecma

[61] Official website: http://www.safran-electronics-defense.com

[62] Morpho official website, information from August 2014: https://web-beta.archive.org/web/20150526044815/http://www.morpho.com/qui-sommes-nous

[63] http://www.morpho.com/en/government-id-solutions-facilitate-and-secure-identity-management

[64] https://www.morpho.com/en/mobile-and-automated-systems-improve-public-security

[65] http://www.morpho.com/en/ensuring-trusted-authentication-and-transactions-online

[66] "Morpho Trak Technology Goes Operational for the FBI", Morpho press release, 2011, http://www.morpho.com/en/media/morphotrak-technology-goes-operational-fbi-20110418 (also available in: http://web.archive.org/web/20150607084516/http://www.morpho.com/actualites-et-evenements/presse/morphotrak-technology-goes-operational-for-the-fbi?lang=en)

[67] "Sagem Sécurité to provide Interpol and its 186 member states with latest AFIS, Automated Fingerprint Identification System", Morpho press release, 2008: http://www.morpho.com/en/media/sagem-securite-provide-interpol-and-its-186-member-states-latest-afis-automated-fingerprint-identification-system-20080204 (also available in: http://web.archive.org/web/20150607090048/http://www.morpho.com/news-events-348/press/sagem-securite-to-provide-interpol-and-its-186-member-states-with-latest-afis-automated-fingerprint-identification-system?lang=en) "Safran Identity & Security is the exclusive partner of INTERPOL for facial recognition", press release, 2016: http://www.morpho.com/en/media/safran-identity-security-exclusive-partner-interpol-facial-recognition-20161123

[68] "Morpho Trak Deploys Morpho Biometric Identification System at NYPD", Morpho press release, 2012:

partment of Homeland Security, the Ministry of Interior of the United Arab Emirates, the police and the French Ministry of Interior, among others. Recently the company announced it was awarded a five-year contract with the National Electoral Institute in Mexico to implement its multi-biometric identification systems.[69]

Even though the Ministry of Security did not provide more details as to the product specifications of the products acquired from Safran, information from 2013 from a source close to the Argentine Federal Police gave us more insight into the specifics of the technology used by this law-enforcement agency, which is one of SIBIOS main users.

Apart from the AFIS system used to identify fingerprints, the Argentine Federal Police also carries out facial identification using Safran technology, specifically the product "Morpho Face Investigate Pilot" (MFIP).

Thanks to the documents published by WikiLeaks, known as The Spy Files,[70] a series of documents released between 2011 and 2014 with the view of exposing the global industry of massive surveillance, we were able to access a PDF from Safran devoted to describing the product mentioned in the presentation of the Argentine Federal Police, labelled "An Introduction to Morpho Face Investigate Pilot".[71]

Based on this document, its main features are:

- "Load and manage a database of up to 350,000 portraits, with an option for an extension to 2,000,000 portraits;
- Search one or more images against the portrait database using the Morpho face recognition technology;
- Acquire face images from files, or using a camera or a scanner;
- Extract face images from video files and search them against the database;
- Extract faces from images showing multiple people;
- Check the result of face recognition searches and report on the decision made;

http://www.morpho.com/en/media/morphotrak-deploys-morpho-biometric-identification-system-nypd-20120919 (also available in: http://web.archive.org/web/20150607084015/http://www.morpho.com/news-events-348/press/morphotrak-deploys-morpho-biometric-identification-system-at-nypd?lang=en)

[69] "Safran Identity & Security to modernize Mexico's multi-biometric identification system", press release from Safran Identity and Security, 2016: http://www.morpho.com/en/media/safran-identity-security-modernize-mexicos-multi-biometric-identification-system-20161221

[70] https://wikileaks.org/spyfiles/

[71] "An Introduction to Morpho Face Investigate Pilot", 2011: https://wikileaks.org/spyfiles/document/safran/SAFRAN-2011-AnIntrto-en/ Also available in: https://sii.transparencytoolkit.org/docs/Morpho_MorphoFace_Product-Descriptionsii_documents

- Manage subsets of the portrait database - called watch lists - to enable search scope restriction."[72]

It also explains that MFIP "can be deployed and used with minimal effort even for users with no or very limited knowledge of face recognition."[73]

The process for MFIP face recognition develops as follows:[74] the first step consists in acquiring the face image, which can be done from live or file sources (e.g. from a camera or a .JPG file); the second step aims at finding where the face is located in the image, and pinpointing the eye centres, based on which a template is obtained. A template is a representation of the image that is suitable for image comparison (a template may represent either visible features of a portrait, such as nose or eyebrows location, or purely mathematical data). As the image is analysed, a quality control is performed, which determines whether the template is reliable or not, and whether the image is of high or low quality. A low quality score may require that an operator manually confirm the location of some face feature in order to enhance the overall accuracy of the system.

Once the images are loaded onto the database feeding MFIP, faces can be compared. Each comparison produces a score: the higher the score, the more likely the two compared faces are similar.

ii Ministry of Interior

"We would like to specially thank the Republic of Cuba for their collaboration in developing this system, a low-cost software that will be integrated into AFIS and which will make it possible to know in real time who is the person in front of a law-enforcement officer or in any other place, if it is the person in question or, if it's not, who they really are."[75] This is how Argentina's former president, Cristina Fernández de Kirchner, presented SIBIOS in the first speech that introduced it to society in 2011.

As a result, the newspaper Página12 confirmed again with the Ministry of Interior that Cuba played a role in developing the technology behind the System, stating that "Cuba's support was crucial, because it is the only country in the Latin American region that utilises biometric identification for its citizens."[76]

In October 2015, the Ministry of Interior announced once again that they were working with Cuba to continue implementing biometric technology. According to the former Ministry of Interior, Florencio

[72] Ibid, p.2

[73] Ibid, p.2

[74] Ibid, p. 3-4

[75] Creation of Federal Biometric Identification System (SIBIOS)", November 7, 2011, Cristina Fernández de Kirchner, minute 2:27: https://www.youtube.com/watch?v=GcKrHKqBzwo

[76] [Ya nunca más habrá que tocar el pianito", Página12, November 8, 2011: https://www.pagina12.com.ar/diario/sociedad/3-180795-2011-11-08.html

Randazzo, "this agreement will open the door to a new stage of biometric technology implementation in our country, as we will be able to identify a person by contrasting a clear image against an entire [data]base from ReNaPer [National Registry of Persons] and obtain their identity with a single photo", and he added that "In the case of photographs, in the past, identifying an individual required comparing a photo against another photo of a concrete person, (. . .) but now we will also be able to identify a person using a single image, as it will be possible to contrast the photo against ReNaPer's entire database."[77]

Thanks to this data, in the request for information sent to the Ministry of Interior for the purposes of this report, we explicitly inquired about the terms of collaboration of Cuba's government, the company or entity that participated in the development of this technology and the terms and conditions of the agreement.

The Cuban company in question is DATYS. With its main office in La Habana, it was founded in 2005 and has facilities in the provinces of Matanzas, Villa Clara, Holguín and Santiago de Cuba. Based on the information on its website, it has more than 700 employees.[78]

DATYS classifies its business lines into five categories: biometrics, identity, security technology, management and data mining.

In the reply to our request for information, the Ministry of Interior did not specify which software it was; the Technology Department of RENAPER just mentioned that "The tool provided by the government of Cuba facilitates working with face images. The tool is designed to strengthen the automatic system of identification. The main method of automatic identification using the AFIS system is that of fingerprint comparison. Face comparison of the same person is used as a secondary method."[79]

According to DATYS' official website, there are three biometric products available: BIOMESYS, a multi-biometric identification platform; PMAIC, a Criminal Investigation Multi-biometric Platform; and BIOMESYS framework Bioapi, the framework for the biometric deployment.

BIOMESYS' main features are:

- "Enrolment of persons from biographical and biometric data capturing, particularly fingerprints, face, and signature.
- Identification of persons included in the system.

[77] Randazzo announced that 'Argentina will incorporate biometric technology that will help the Justice system identify individuals based on images'", October 13, 2015, Ministry of Interior: http://www.mininterior.gov.ar/prensa/prensa.php?i=4594

[78] Official website: http://datys.cu/, a version of the website in file on 24/11/2016 can be accessed in: https://web-beta.archive.org/web/20161124082804/http://datys.cu/spa/site/index

[79] Reply from the Ministry of Interior to the request for information made in July 2016, filed in ADC

- Among identification and biometric verification services are:
  - Fingerprints vs. Fingerprints.
  - Latent Fingerprints vs. Fingerprints.
  - Latent Fingerprints vs. Latent Fingerprints of unsolved cases.
  - Palm prints vs. Palm prints.
  - Latent Palm Prints vs. Palm Prints.
  - Latent Palm Prints vs. Latent Palm Prints of unsolved cases.
  - Face vs. Face.
  - Edited Faces vs. Face, Identikit picture vs. Face.
  - Voice vs. Voice, DNA vs. DNA.
- The Exchange of information with other systems".[80]

In their reply to our request for information, the Ministry of Interior also provided information on the agreement previously mentioned, signed in October 2015, specifically addenda 6 and 7 of the original International Cooperation Agreement, signed on June 17, 2011.

These addenda provide for the updating of the biometric system supplied by DATYS and used by the Ministry of Interior and its various departments. Addendum 6 establishes that the updating of the biometric platform licensed from the Cuban government consists in "(...) the incorporation of new web services under BIAS standards[81], which facilitate 1:N face identification and improvements to verification and quality control tools for identification through 1:1 face recognition (...)."

In biometrics, a "1:N" system is used for identification, where "N" generally stands for the total number of enrolments stored in a database and looks at the question "Who's that person?"; while a "1:1" system is used for verification, looking at "Is that the person they say they are?".

On the other hand, addendum 7 revolves around contracted services such as technical support and maintenance for the tools used in biometric identification, as well as training on troubleshooting targeted at the technical staff working in the Ministry of Interior.

Pursuant to addendum 6, the updating of the biometric system had a total cost of one million eighty thousand US dollars (U$D 1,080,000), while the technical support hired under addendum 7 had a cost of one hundred eighty thousand US dollars (U$D 180,000) for each applicable year of the addendum, which shall extend for a period of five years as of 2016, with the possibility to review the terms and conditions of the agreement at the end of each year.

[80] Official website, DATYS, file from November 28, 2016: https://web-beta.archive.org/web/20160428071558/http://www.datys.cu/spa/site/product/5

[81] For its acronym in English, "Biometric Identity Assurance Services (BIAS)"

iv SIBIOS in use

To sum up the abovementioned, we saw that the journey of the information feeding SIBIOS first begins when the digital National ID and the new biometric Passport are issued by RENAPER, and, on the other hand, when the national and provincial law-enforcement agencies previously load the enrolments. Once the information is stored in the database, it can be utilised by the various users authorised by the relevant act and the agreements made with the provinces.

In this manner, the National Migration Office uses SIBIOS to control internal and external migration checkpoints in Argentina. Both Argentine and foreign citizens are enrolled in SIBIOS database when they traverse the international airports of the country or Buquebus' port terminal.

Even though the public information available with regard to how law-enforcement agencies –Argentine Federal Police, Gendarmerie, Argentine Naval Prefecture and Airport Security Police– use SIBIOS is almost null, information from 2013 from a source close to the Federal Police allowed us to learn about some cases in which the system was actually used. Apparently, the Argentine Federal Police uses SIBIOS during natural disasters in order to identify the victims, as was the case with the floods in the city of La Plata,[82] and the Castelar rail accident on the Sarmiento line[83] and the Once tragedy.[84] In order to identify the victims, the Argentine Federal Police is said to have used a device from Safran group, the "Morpho RapID" model, a wireless device for capturing and identifying fingerprints.[85]

Given SIBIOS' origin and current structure, law-enforcement agencies require no court order (in other words, there is no need for a judge to authorise the carrying out of certain duties under a criminal process) to use the database and identify the persons enrolled therein. This undermines the compliance of the System with the legal principle of due process, and in particular, the presumption of innocence.

Granting federal and provincial police (and recently any agency under the Executive and/or Judicial Power) unrestricted access to the biometric identification of individuals permanently or temporarily living in the country seems to follow a logic under which all citizens enrolled in SIBIOS database are presumed guilty until proven innocent. This is a clear illustration of how technology has reshaped criminal investigations to such an extent that it must be addressed very carefully in order to avoid a potential violation of rights.

[82] "Over 48 people killed by the storm in La Plata", La Nación, April 4, 2013, http://www.lanacion.com.ar/1569096-inundacion-en-la-plata; "89 persons confirmed dead as a result of the floods on April 2 in La Plata", Télam, July 4, 2014, http://www.telam.com.ar/notas/201407/69935-la-plata-justicia-89-muertos-inundacion.html

[83] "Government confirms 3 dead and 315 injured as a result of Sarmiento train crash", Clarín, June 13, 2013, http://www.clarin.com/ciudades/chocaron-trenes-sarmiento-castelar_0_HkvPcVDsvXg.html

[84] "Once train crash: 50 dead and 676 injured", Clarín, February 22, 2012, http://www.clarin.com/sociedad/descarrilo-tren-sarmiento-llegaba-once_0_Syp-jfDhwmx.html

[85] More information on Safran mobile terminals available on its website: http://www.morpho.com/en/biometric-terminals/mobile-terminals

Another concern resulting from the use of SIBIOS by law-enforcement agencies in the criminal field is related to the total discretion with which the System is utilised, taking into account that the applicable laws do not establish specific guidelines for its use in criminal investigations. Is it used for any type of crime investigation, regardless of its magnitude or legally-protected rights involved? Is it the first investigation measure utilised? ADC is currently examining these aspects and will be dealing with them in another work.

IV Conflicts involving fundamental rights

After the analysis carried out in this document, it is worth considering the key aspects and questions based on which we can –and must– study the impact of biometric identification technologies introduced as public policies on people's rights:

- The implementation of SIBIOS through a decree issued by the Executive Power calls its legitimacy into question under the legality principle enshrined in the Constitution and international human rights instruments.
- Access to SIBIOS by law-enforcements agencies without a court order. While these new technologies pose new challenges regarding their use for prosecuting crimes, they also jeopardise traditional interpretations of defence rights in criminal proceedings, which makes us ponder: Under what criteria do users utilise SIBIOS? Must there be an actual criminal investigation for law-enforcement agencies to use the database or can they use it under normal circumstances too?
- Given the sensitive nature of biometric data, they represent people's most intimate characteristics. In this sense, it is worth considering the following questions: What are the new challenges posed by the identification of individuals based on this data when it comes to avoiding discriminatory practices? As we saw previously, technology may reproduce the biases of those who implement it, then, what is the protection afforded by the State to prevent these systems from becoming discriminatory tools or being used exclusively against certain social groups?
- Regarding the purposes for which SIBIOS was created, what is the reasoning behind its implementation? How effective has the System been in preventing and prosecuting crime? Can we affirm SIBIOS has been useful for solving the problems referred to by the State in terms of security?
- Going back to the analysis of biometric identification from the perspective of technology, not only did we find problems in terms of how to exploit this type of technologies, but we also

reached the conclusion that biometric data collection in itself poses a serious risk. Systems such as SIBIOS confer the State enormous power to the detriment of individual freedom, but given the case, what happens when new governments are elected? What safeguards must be afforded to avoid a potential abuse on the part of the governments in power?

The biometric identification systems used, particularly SIBIOS in Argentina, have a lack of transparency that is characteristic of traditional institutions in the intelligence and military fields, which is rooted in the emergence of citizens' identification policies. This lack of transparency in terms of how the State uses these systems, how the information and biometric data stored in databases is protected; and in terms of the studies carried out to justify the adoption of this technology or the parameters considered for the acquisition of technological solutions are all concerns the answer of which is pending.

The answers to these questions will have to consider the elements established in the Constitution and the main international human rights instruments: the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the American Convention on Human Rights. All these instruments recognize that privacy, freedom of speech, thought and opinion, freedom of association and assembly, freedom of worship, as much as the freedom to request and receive information, are essential rights of human beings as they are part of our dignity. Hence, any interference on the part of the State must be based on solid grounds, supported by hard data and serious and independent diagnoses, in order to comply with all the necessity and proportionality conditions required for any measure limiting fundamental rights to be considered legitimate.


por los Derechos Civiles