Eduardo Ferreyra

Facial recognition in Latin America: Towards a human rights-based legal framework to protect public spaces from mass surveillance

Table Of Contents

Facial recognition in Latin America: Towards a human rights-based legal framework to protect public spaces from mass surveillance

Eduardo Ferreyra

EXECUTIVE SUMMARY

This policy paper addresses the challenges posed by the use of facial recognition technologies in public spaces in Latin America. It states that these systems are being deployed without strong legal safeguards, without privacy impact assessments being carried out and through low-level norms that impede a public, broad and inclusive debate. Therefore, it recommends that facial recognition systems should be banned because of their serious impact on rights such as privacy, freedom of expression, freedom of assembly and data protection.

INTRODUCTION

Facial recognition (FR) systems are increasingly used by law enforcement authorities around the world. Governments affirm this technology is very useful to prevent crime, identify fugitives or detect criminals in public spaces. Latin America is not an exception. To date, we can find that countries like Argentina,[1] Brazil,[2] Peru,[3] México[4] and Ecuador[5] have implemented FR systems. Other countries of the region – like Uruguay[6] – are also interested in acquiring this technology for public safety purposes. However, these systems are being deployed without robust safeguards to protect people's rights. Legal frameworks in Latin America are not keeping up with the risks posed by FR systems to privacy, freedom of expression or freedom of assembly. Thus, the intrusiveness of this technology may degenerate into situations of mass surveillance and social control. This lack of strong human rights standards is particularly concerning for the current political situation in Latin America. Several countries are living in a context of social unrest and citizens are protesting in the streets.[7] If widely implemented, FR systems can be used to persecute political opposition or deter individuals from engaging in protests. This scenario is serious enough to claim that the use of FR technologies for public safety should be banned or postponed.

PROBLEM DESCRIPTION

FR is a biometric technology that identifies people by mapping their facial features. Its ability to detect individuals whose footage has been captured by FR cameras has led to law enforcement agencies in Latin America to use or consider to use them for public safety purposes. However, there are various human rights concerns with this technology. Firstly, FR technology can make mistakes. It can wrongly identify a person, matching it to a database he/she is not part of. This is particularly dangerous because it can lead to the detention or arrest of innocent people. Such cases have already happened in Argentina, where the FR system used by Buenos Aires police identified incorrectly a person who was charged with a bank robbery.[8] Secondly, when FR cameras are effective in identifying people, it can be used to surveil the population, identify dissidents or inhibit social protest. Based on the above, we can argue that FR is a faulty technology

---

1   Diego Fernandez, 'Facial Recognition in the City of Buenos Aires' (*Marval, O'Farrell y Mairal*, 19 June 2019) <https://www.marval.com/publicacion/reconocimiento-facial-en-la-ciudad-de-buenos-aires-13374&lang=en> accessed 12 April 2020.

2   ANSA, 'Facial-recognition systems on the rise in Brazil' (*ANSA*, 3 April 2019) <https://www.ansa.it/english/news/2019/04/03/facial-recognition-systems-on-the-rise-in-brazil_9ec787b6-62a9-4218-9c4f-81261ac78918.html> accessed 12 April 2020.

3   El Comercio, 'Máxima vigilancia en Gamarra: así funcionan las cámaras con reconocimiento facial (Maximum surveillance in Gamarra: that's how facial recognition cameras work)' (*El Comercio*, 12 April 2019) <https://elcomercio.pe/lima/seguridad/gamarra-vigilancia-extrema-funcionan-camaras-reconocimiento-facial-george-forstyh-victoria-noticia-ecpm-625744-noticia/> accessed 12 April 2020.

4   Gerardo Jiménez, 'La Central de Abasto será la zona más vigilada de la CDMX (Central de Abasto will be México city's most surveilled zone)' (*Excelsior*, 3 January 2020) <https://www.excelsior.com.mx/comunidad/la-central-de-abasto-sera-la-zona-mas-vigilada-de-la-cdmx/1356117> accessed 8 May 2020.

5   Chris Burt, 'Ecuador tackles crime with Chinese facial recognition technology' (*Biometric Update*, 22 January 2018) <https://www.biometricupdate.com/201801/ecuador-tackles-crime-with-chinese-facial-recognition-technology> accessed 12 April 2020.

6   Guillermo Losa, 'Ministerio del Interior usará tecnología de identificación facial en la calle (Ministry of the Interior to use facial recognition technology in the streets)' (*El Observador*, 20 March 2019) <https://www.elobservador.com.uy/nota/ministerio-del-interior-usara-tecnologia-de-identificacion-facial-en-la-calle-201931916312> accessed 12 April 2020.

7   openDemocracy, '2019: Protests and disruptive changes in Latin America' (*openDemocracy*, 2 January 2020) <https://www.opendemocracy.net/en/democraciaabierta/2019-movilizaciones-ciudadanas-y-cambios-disruptivos-en-américa-latina-en/> accessed 12 April 2020.

8   Ella Jakubowska, 'Dangerous by design: A cautionary tale about facial recognition' (*EDRi*, 12 February 2020) <https://edri.org/dangerous-by-design-a-cautionary-tale-about-facial-recognition/> accessed 12 April 2020.

because it enables mass surveillance and opens the door for abuse. This situation has urged human rights activists to address the problem. One of the pressing issues is the need to implement controls and limitations to restrict the use of this technology to lawful ones.

RATIONALE FOR ACTION

Technologies are embedded in a certain social context, which varies from country to country or from region to region. Considering FR systems without taking into account social, political, economic and cultural conditions is a short-sighted view that is likely to lead to poor results. In this sense, we cannot overlook three main features of Latin America. The first one is the existence of societies characterised by social and economic inequalities. Latin America is one of the most unequal regions in the world and a very significant part of their population suffer basic social and economic problems.[9] The second one is the absence of effective responses to correct these inequalities by public authorities. In general, Latin American states have showed indifference or incompetence to meet the demands of their citizens. The third one is a long tradition of social protest by Latin Americans citizens. Because the state has usually not been responsive, demonstrations, marches or public occupations are forms of protest we can see every day in the region.[10]

This scenario is the reason why public space is for many people in Latin America the only place in which they can make their voice heard. By meeting in the streets, squares or stations, citizens can exchange ideas with each other, express a dissident position, denounce corruption or draw attention to a certain issue. But these activities require that people are free from state interference and mass surveillance. FR systems are particularly intrusive because they can examine unique and distinctive features of the human face to create a detailed biometric map of it.

Thus, public spaces must be friendly places for critical expressions and not an area for surveillance and control. FR impedes this goal because it may cause people to restrain from protesting publicly to avoid being identified by the government. Any widespread deployment of this technology may curtail the most productive avenue for citizens to demand.

POLICY SCENARIOS

Although the perils caused by the use of FR technologies exist for every country around the world, the risks are most pressing in Latin America for the following reasons.

Firstly, our region has a long history marked by dictatorial governments that have not hesitated to resort to tools of surveillance, control and repression of the opposition. Although Latin American countries have political systems with democratic procedures, this does not mean that the authoritarian culture has disappeared. On the contrary, current events such as the repression of social protests in Venezuela, Ecuador or Chile are a clear example of the dangers people face when protesting in public spaces. FR technologies would only aggravate that risk.

Secondly, Latin American citizens cannot trust in robust legal safeguards to prevent abuses of this technology. For instance, several countries such as Ecuador, Paraguay or Bolivia do not have data protection laws.[11] Moreover, countries with specific data protection law have not updated these norms in order to address the challenges of digital technologies nowadays, just like the European Union did when passing the General Data Protection Regulation (GDPR).[12] And countries that did enact new regulations are post-

---

9 Oxfam International, 'Latin America remains the most unequal region in the world' (*Oxfam International,* 19 December 2017) <https://blogs.oxfam.org/en/blogs/17-12-18-latin-america-remains-most-unequal-region-world/index.html> accessed 12 April 2020.

10 openDemocracy (n 7).

11 DLA Piper, 'Data Protection Laws of the World' (*DLA Piper*) <https://www.dlapiperdataprotection.com> accessed 12 April 2020.

12 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive

poning their entry into force. This is the case of Brazil, which enacted the Brazilian General Data Protection Law in 2018 but are delaying its implementation to May 2021.[13] Thus, basic requirements such as carrying out privacy impact assessments or considering biometric data as sensitive data are not part of the obligations to be met by those who use FR technologies.

Finally, in those Latin American countries that have already deployed this technology, they have done so without complying with the principles of legality, necessity and proportionality required for any interference with human rights. For instance, after his visit to Argentina in 2019, Joe Cannataci, UN Special Rapporteur on the right to privacy, speaking about the FR system to detect fugitives deployed by the city of Buenos Aires, stated that 'the justifiability of such a system, its legitimacy, necessity and proportionality should have been established by a Privacy Impact Assessment (PIA) which does not seem to have been carried out'.[14] Moreover, the system was implemented by an administrative resolution, without following the recommendation of the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, which affirmed that:

> in view of the inherent risk of abuse of any surveillance system, these measures should be based on legislation that is particularly precise, clear and detailed, and States have to ensure a plural, democratic, and open consultation prior to the adoption of the applicable regulations.[15]

Considering the preceding reasons, any scenario where FR is being used by Latin American states is a high-risk scenario for fundamental rights. Even if the system is tailored to detect only a particular group of people – eg the FR system to detect fugitives in the city of Buenos Aires – its inaccuracy will lead to the detention of innocent people and thus affect the whole population. The lack of strong legal safeguards may allow authorities to deploy this technology without transparency and accountability. And their intrusiveness and pervasiveness represent an incentive for states to rely on FR to halt social protest.

In conclusion, Latin American governments must avoid any use of FR technologies in public spaces. Instead of focusing their energy on deploying systems that are prone to be used for mass surveillance, they should work on modernising their legal frameworks to provide their citizens strong human rights safeguards to prevent technology from being used as a tool of control and repression.

POLICY RECOMMENDATIONS

- Governments in Latin America should ban the use of FR technologies by law enforcement authorities in public spaces. In countries like Argentina, where FR systems have already been used, their operation must be immediately stopped.
- Before considering the deployment of FR, states must implement specific legal safeguards to address the risk that digital technologies pose for the rights of their citizens. That would include the passing of data protection law in those countries that currently do not have one and the updating of the regulations in those countries that already have

95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN> accessed 5 June 2020.

13 Angelica Mari, 'Brazilian data protection regulations postponed to 2021' (*ZDNet*, 30 April 2020) <https://www.zdnet.com/article/brazilian-data-protection-regulations-postponed-to-2021/> accessed 8 May 2020.

14 Professor Joe Cannataci, 'Statement to the media by the United Nations Special Rapporteur on the right to privacy, on the conclusion of his official visit to Argentina, 6-17 May 2019' (*United Nations Human Rights Office of the High Commissioner*, 17 May 2019) <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E> accessed 12 April 2020.

15 Inter-American Commission on Human Rights and the Office of the Special Rapporteur for Freedom of Expression, *Standards for a Free, Open, and Inclusive Internet* (2017) para 217 <http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf> accessed 12 April 2020.

one. These new regulations must consider biometric data as sensitive data, demand privacy impact assessments to evaluate high risk technologies and set up independent data protection authorities with enough technical, human and financial resources to carry out their duties.

- Serious and independent analysis of necessity and proportionality must be conducted to determine the compliance of this technology with human rights standards. Privacy impact assessments are a very useful tool to achieve this end but the analysis must address other human rights that can be affected as well, like freedom of expression, freedom of assembly or the right to protest.

- States must engage in a wide-open public debate on the use of FR technology. This means that independent technologists, security experts and civil society organisations must be allowed to take part in every discussion on the issue and their analysis, feedback and suggestions be seriously considered.

- To provide a common ground for the countries in the region, the Inter-American Court of Human Rights should develop guidelines to adapt human rights to the challenges posed by these new surveillance tools. For instance, the right to privacy has received less attention than other rights in the history of the system but the perils of digital technologies should urge their organs to change their mind. An advisory opinion by the court on the impact of digital surveillance on human rights could be the most suitable option.

REFERENCES

ANSA, 'Facial-recognition systems on the rise in Brazil' (*ANSA*, 3 April 2019) <https://www.ansa.it/english/news/2019/04/03/facial-recognition-systems-on-the-rise-in-brazil_9ec787b6-62a9-4218-9c4f-81261ac78918.html> accessed 12 April 2020

Asociación por los Derechos Civiles, 'Con mi cara no. Reconocimiento facial en la ciudad de Buenos Aires (Not with my face. Facial recognition in the city of Buenos Aires)' (*ADC*) <https://conmicarano.adc.org.ar> accessed 12 April 2020

Burt C, 'Ecuador tackles crime with Chinese facial recognition technology' (*Biometric Update*, 22 January 2018) <https://www.biometricupdate.com/201801/ecuador-tackles-crime-with-chinese-facial-recognition-technology> accessed 12 April 2020

Cannataci J, 'Statement to the media by the United Nations Special Rapporteur on the right to privacy, on the conclusion of his official visit to Argentina, 6-17 May 2019' (*United Nations Human Rights Office of the High Commissioner*, 17 May 2019) <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E> accessed 12 April 2020

Derechos Digitales, 'Mal de Ojo. Reconocimiento facial en América Latina (Evil eye. Facial recognition in Latin America)' (Derechos Digitales November 2019) <https://www.derechosdigitales.org/wp-content/uploads/glimpse-cap-rec-facial.pdf> accessed 12 April 2020

DLA Piper, 'Data Protection Laws of the World' (*DLA Piper*) <https://www.dlapiperdataprotection.com> accessed 12 April 2020

El Comercio, 'Máxima vigilancia en Gamarra: así funcionan las cámaras con reconocimiento facial (Maximum surveillance in Gamarra: that's how facial recognition cameras work)' (*El Comercio*, 12 April 2019) <https://elcomercio.pe/lima/seguridad/gamarra-vigilancia-extrema-funcionan-camaras-reconocimiento-facial-george-forstyh-victoria-noticia-ecpm-625744-noticia/> accessed 12 April 2020

Electronic Frontier Foundation, 'Street-level surveillance. Facial recognition' (*EFF*, 24 October 2017) <https://www.eff.org/es/pages/face-recognition> accessed 12 April 2020

Fernandez D, 'Facial Recognition in the City of Buenos Aires' (*Marval, O'Farrell y Mairal*, 19 June 2019) <https://www.marval.com/publicacion/reconocimiento-facial-en-la-ciudad-de-buenos-aires-13374&lang=en> accessed 12 April 2020

Inter-American Commission on Human Rights and the Office of the Special Rapporteur for Freedom of Expression, *Standards for a Free, Open, and Inclusive Internet* (Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights 2017) para 217 <http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf> accessed 12 April 2020

Jakubowska E, 'Dangerous by design: A cautionary tale about facial recognition' (*EDRi*, 12 February 2020) <https://edri.org/dangerous-by-design-a-cautionary-tale-about-facial-recognition/> accessed 12 April 2020

Jiménez G, 'La Central de Abasto será la zona más vigilada de la CDMX (Central de Abasto will be México city's most surveilled zone)' (*Excelsior*, 3 January 2020) <https://www.excelsior.com.mx/comunidad/la-central-de-abasto-sera-la-zona-mas-vigilada-de-la-cdmx/1356117> accessed 8 May 2020

Losa G, 'Ministerio del Interior usará tecnología de identificación facial en la calle (Ministry of the Interior to use facial recognition technology in the streets)' (*El Observador*, 20 March 2019) <https://www.elobservador.com.uy/nota/ministerio-del-interior-usara-tecnologia-de-identificacion-facial-en-la-calle-201931916312> accessed 12 April 2020

Mari A, 'Brazilian data protection regulations postponed to 2021' (*ZDNet*, 30 April 2020) <https://www.zdnet.com/article/brazilian-data-protection-regulations-postponed-to-2021/> accessed 8 May 2020

openDemocracy, '2019: Protests and disruptive changes in Latin America' (*openDemocracy*, 2 January 2020) <https://www.opendemocracy.net/en/democraciaabierta/2019-movilizaciones-ciudadanas-y-cambios-disruptivos-en-américa-latina-en/> accessed 12 April 2020

Oxfam International, 'Latin America remains the most unequal region in the world' (*Oxfam International*, 19 December 2017) <https://blogs.oxfam.org/en/blogs/17-12-18-latin-america-remains-most-unequal-region-world/index.html> accessed 12 April 2020

Privacy International, 'Protecting civic spaces' (*Privacy International*, 1 May 2019) <https://privacyinternational.org/long-read/2852/protecting-civic-spaces> accessed 12 April 2020

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (*General Data Protection Regulation*) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>accessed 5 June 2020

UN News, 'Moratorium call on surveillance technology to end "free-for-all" abuses: UN expert' (*UN News*, 25 June 2019) <https://news.un.org/en/story/2019/06/1041231> accessed 12 April 2020

The Public Voice, 'Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance' (*The Public Voice*, October 2019) <https://thepublicvoice.org/ban-facial-recognition/> accessed 12 April 2020

Global Campus of Human Rights

Monastery of San Nicolò
Riviera San Nicolò, 26
I-30126 Venice Lido (Italy)

gchumanrights.org

Global Campus of Human Rights

The Global Campus of Human Rights is a unique network of more than one hundred participating universities around the world, seeking to advance human rights and democracy through regional and global cooperation for education and research. This global network is promoted through seven Regional Programmes which are based in Venice for Europe, in Sarajevo/Bologna for South East Europe, in Yerevan for the Caucasus, in Pretoria for Africa, in Bangkok for Asia-Pacific, in Buenos Aires for Latin America and the Caribbean, and in Beirut for the Arab World.

The Global Campus Policy Observatory

The Observatory is a 'virtual hub' which comprehends a team of seven researches from the regional programmes to produce, publish and publicly present seven different policy analyses in form of policy briefs, with the aim of making of each regional programme a solid focal point for policy expert advisory in human rights issues.