Navigating the Complexities of Facial Recognition for Public Security in Latin America

Maria Badillo

The ongoing security crisis in Latin America has prompted governments to try new solutions to fight the problem. Major cities in the region have installed face recognition technology (FRT) cameras in public spaces.[1] Although the high rates of crime and violence have increased the general sense of insecurity, governments must deploy solutions from a human rights perspective. States should avoid the 'techno-solutonist' fever thinking technology can magically solve every problem without first assessing the consequences it might bring. Due to its massive and wide reach, FRT can enable massive and invasive surveillance that poses risks to fundamental rights, particularly privacy, data protection, and freedom of expression and association. The creation of these risks has been considered sufficient for some jurisdictions to put a full stop to its implementation. Latin American governments going forward with the deployment of FRT systems should prioritize the protection of fundamental rights and regulation of this technology.

II

Face recognition technology detects a face by its features, such as the distance between the eyes, the width of the nose, the depth of the eye sockets, and the shape of cheekbones. The facial features are used to create a face print with approximately 80 nodal points that serve as a unique template for future identification.[2] Like other biometric technologies, face recognition technology was envisioned to enhance security in multiple contexts like securing financial transactions, validating identities at airports or private buildings, and unlocking our phones.[3]

Most of these scenarios serve a verification purpose, where the algorithm simply confirms a claimed identity by verifying the facial features. When FRT is used to recognize or identify someone, the algorithm looks for a match, so the system will capture any face that is compatible with the features of another face. [4] For this to occur, FRT works with a

[1] For Argentina, see: https://www.telam.com.ar/notas/202209/604166-justicia-ciudad-buenos-aires-gobierno-porteno-reconocimiento-facial.html; for Brasil, see: https://reconocimientofacial.info/justica-de-sp-determina-que-metro-interrompa-implantacao-de-sistema-de-reconhecimento-facial/; for Chile, see: https://www.infodron.es/texto-diario/mostrar/3529913/policia-chile-incorpora-drones-reconocimiento-facial; for Colombia, see: https://digitalid.karisma.org.co/2021/07/01/SIVIT-reconocimiento-facial/; for Ecuador see: https://www.metroecuador.com.ec/ec/noticias/2020/02/19/quito-camaras-reconocimiento-facial-funcionaran-altavoces-advertir-ciudadanos.html; for Mexico, see:https://ciapem.org/c2-central-de-abasto-cdmx/

[2] Kevin Bonsor and Ryan Johnson, "How Facial Recognition Systems Work", https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm

[3] Jesse West. "21 AMAZING USES FOR FACE RECOGNITION – FACIAL RECOGNITION USE CASES", https://www.facefirst.com/blog/amazing-uses-for-face-recognition-facial-recognition-use-cases/

[4] Kevin Bowyer, "Face Recognition Technology: Security versus Privacy", IEEE Technology and Society Magazine (2004), 12. http://www.cse.nd.edu/Reports/2004/TR-2004-21.pdf

database of images of the face it wants to recognize. In a law enforcement scenario, face recognition systems will typically work under "watch lists" containing photos of suspects and offenders.[5] This is why FRT is attractive for law enforcement and security purposes since it might facilitate the recognition of a wanted person among a crowd. But this is the same reason why this technology is problematic from a human rights perspective.

Face recognition systems for public security, if implemented, should be regulated and overseen. Aside from the general human rights framework, this technology is subject, particularly, to data protection frameworks that regulate the processing of personal data held by governments and enterprises. The majority of countries in Latin America have a general data protection law in place, with a few exceptions such as Paraguay, Bolivia, Guatemala, and Honduras. Still, some of these jurisdictions have taken steps toward approving a comprehensive data protection law. As for the countries with a law already in place, most of them set out principles for data protection, rights for data subjects, and obligations for data controllers handling personal data.

Argentina, Brazil, Chile, Colombia, Ecuador, and Mexico are among the countries that have both a data protection law and active face recognition systems for law enforcement purposes. Data protection laws provide a minimum set of standards and protections to ensure personal information is processed through legal and proportional means, that the data is used solely for the purpose it was collected, and that it stays accurate, relevant, and secure. All of the laws in the study contain a similar provision regarding the legitimate basis for processing personal data. In general, each individual should give their express consent to have their data collected and processed, unless an exception applies. Similarly, most of these laws make an exception for obtaining consent when the government processes personal data to 'execute State-related activities and/or public policies' or when the processing is 'required by other laws and regulations.'[6]

However, most of the countries implementing face recognition technology lack specific regulations for video surveillance and, particularly, for face recognition systems. Most of the systems that operated in the Colombian and Argentine subway stations, in the biggest Mexican market center, or in the drones floating in Chilean skies with face recognition technology, currently do so without regulation. Governments have justified its implementation through laws that set out a wide national and public security mandate,[7] but there are no further standards or safeguards for protecting individuals. Prior regulation is important to provide transparency and protection and to avoid potential abuses of power and discrimination.

However, the compatibility of FRT regulation with a human rights framework is questionable. On its own, the implementation of face recognition systems for law

[5] Ibidem, 10.
[6] General Data Protection Laws, for Argentina see articles 5, sec. 2(b); for Chile, article 4; for Colombia. articles 6 (a) and 10(a); for Mexico, article 10.
[7] AlSur, *Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa,* 2021, p.8. Available at: https://www.alsur.lat/sites/default/files/2021-10/ALSUR_Reconocimiento%20facial%20en%20Latam_ES_Final.pdf

enforcement clashes with personal data protection principles of proportionality, fairness, and purpose limitation, among others. Face recognition technology requires the collection and processing of biometric data, which is considered sensitive information because it reveals physical characteristics and facts related to the most intimate sphere of an individual. All countries using face recognition systems in public spaces in Latin America recognize biometric data as sensitive and some of their laws even ban its processing, unless an exception applies. The potential for abuse or discrimination if sensitive data is unlawfully disclosed or processed is the reason why this type of information is commonly subject to a higher standard of protection.

Moreover, FRT-operated systems require prior access to massive amounts of biometric information that newly captured data can be compared against. Governments usually possess biometric databases of their citizens due to the general acceptance of facial identification norms and practices in bureaucratic procedures.[8] However, as mentioned above, governments are generally not allowed to share personal information unless authorized by law or with the consent of the data subject. Importantly, the public entity receiving the personal data should also be legally authorized to process that data and have legal competence to operate the system.

The lack of regulation of FRT in this regard and noncompliance and oblivion of data protection law point towards the illegality of some of the systems implemented across Latin American cities. In Colombia, the installation of multiple FRT cameras in Bogota's *Transmilenio* subway failed after realizing the system was useless without a biometric database and that the officials lacked the competence to operate the system.[9] Setting aside the technical difficulties to implement the system, Colombia's case demonstrates the lack of preparation from a human rights and data protection approach prior to its implementation.

Moreover, while FRT works with previously stored biometric data it also collects new information. Accuracy in face recognition systems can improve with a constant collection of new, updated information since the system's performance decreases with time.[10] Indeed, high-quality databases for FRT have more than one image of the same person.[11] In this sense, FRT-operated systems can typically store almost all the information entering through video cameras as long as there is storage capacity. Some Latin American governments have already invested in systems that can gather more data at a cheaper cost.[12]

Even if biometric data is legally processed through face recognition technology, governments must take measures to collect more information than needed, delete data no

---

[8] Kelly Gates, *Our Biometric Future, Facial Recognition Technology and the Culture of Surveillance,* (New York: New York University Press, 2011), 46-47.
[9] Pilar Sáenz and Ann Spanger, *Cámaras Indiscretas: Análisis del fallido sistema de videovigilancia inteligente para Transmilenio*, (Colombia: Fundación Karisma, 2018), 4.
[10] Ibidem, 50-51.
[11] Mou Dengpan, *Machine-based Intelligent Face Recognition,* (Beijing: Higher Education Press, 2010), 46.
[12] Chris Burt, "VSBLTY to provide facial biometrics for Smart City partnership in Latin America". Available at:
https://www.biometricupdate.com/201906/vsblty-to-provide-facial-biometrics-for-smart-city-partnership-in-latin-america

longer relevant, and make sure there are no errors in the system's database. In Argentina, a recent case showed how an FRT-based system for the capture of fugitives monitoring the stations Buenos Aires subway led to several unlawful detentions because the database had erroneous information.[13] Moreover, data processing standards require fairness and transparency about surveillance activity so that citizens can be informed about when, why, and how they are being monitored. For instance, enforcement agencies should notify the purpose of the surveillance in a clear and accessible format. Common announcements with vague or general phrases such as 'you are being recorded' or 'for your safety' do not give adequate information to the individual that its biometric data is being processed. This could impact the decisions that individuals might take to protect their privacy and refuse the collection of their personal data.

But when FRT is being implemented on essential services that provide mobility and access to products and services, individuals are hardly left with a choice. Although face recognition technology may serve a legitimate state interest such as national and public security, its implementation in public spaces enables an intensified form of surveillance. The installation of cameras in places where public life occurs, such as streets, subway stations, public markets, schools, and parks, brings an intensified and automated form of surveillance with an ongoing identification-at-a-distance.[14] From a human rights perspective, FRT seems to diminish or restrain the free exercise of fundamental rights like freedom of expression, association, and mobility, aside from undermining privacy and the protection of personal information.

III

Nevertheless, governments in Latin America seem to be going forward with FRT surveillance to aid law enforcement and provide a general sense of security in their cities. The assignment of contracts to private entities for the deployment of these type of systems implicate multi-million investments and contractual duties for both governments and companies. This context is important because current operations are unlikely to stop unless voluntarily taken down by the administration –and compensating for it– or if a court orders it –which might take years of litigation–. In that sense, governments should consider regulating FRT systems for law enforcement purposes, provide more guidance and safeguards for the protection of biometric data, and be more transparent about their functioning overall.

Moreover, governments should also be aware of the practical and technical complexities of these systems. Different from other biometric technologies, FRT was designed for effective, accurate, and real-time results.[15] But even when it relies on machine learning, FRT needs human intervention. A major challenge of FRT is the false positives and false negatives error rates. A false positive error means the system matches the face of an innocent person with the face of an offender, while a false negative means the face of the offender is not

[13] Diario Judicial, *La Constitución no reconoce ese reconocimiento,* 2022. https://www.diariojudicial.com/nota/93028. For a detailed analysis of the judicial decision, see: https://fpf.org/blog/judge-declares-buenos-aires-fugitive-facial-recognition-system-unconstitutional/
[14] Kelly Gates, *Our Biometric Future…*, 27.
[15] Idem.

matched with its own. The question for those running the systems should be whether the algorithms are configured to cast more false positives or false negatives. There is no easy decision since this implies a tradeoff between detaining more innocent or more guilty people.[16] In a "pro-innocence or pro-guilt" dilemma governments are likely to choose the latter since they are, allegedly, looking out for criminals. Choosing a fewer false acceptance rate can make the technology useless. In this sense, if governments decide to use the FRT they must also count on trained human personnel capable of detecting false alarms and preventing unlawful detentions.

Importantly, some argue that machine-based systems like FRT surveillance can be privacy friendly.[17] Governments should privilege privacy by design systems, which may collect and process biometric data only for specific purposes and assuring the data processing also complies with existing normative frameworks.[18] More importantly, privacy by design in FRT could be developed with procedures to "respect the dignity of people who could have been wrongly identified and to avoid transferring onto them the burden of system faults".[19] Finally, Latin American governments using these systems also need to face the challenges that come with the technology. This is a space with multiple questions and few answers for the moment. Some of the principal concerns about FRT are related to the necessity to regulate its results as trial evidence. For instance, governments should regulate matters regarding the use of face recognition results as evidence of identification or establishing a probable cause of an offense.[20] Additionally, citizens should have the right to question the validity of such evidence considering FRT may never be completely reliable since algorithms can be gender and race-biased.[21]

IV

Even when FRT was conceived as a non-invasive technology, it has been strongly questioned for its potential for abuse. What makes face recognition so controversial is the processing of biometric data in such a "passive way", as individuals are not aware they are constantly being identified. In general, Latin American governments will face challenges in the implementation of FRT, especially related to data protection, technology reliability, and the use of its results for law enforcement purposes.

Given the general situation of violence in the region, face recognition has been considered a viable resource to aid law enforcement. Nonetheless, the lack of strong normative frameworks regarding both surveillance and data protection raises concerns about its

[16] Mou Dengpan, *Machine-based Intelligent…,* 45.
[17] Ibidem, 2.
[18] J. Pedraza, et al, *Privacy-by-design rules in face recognition system. Neurocomputing* (Madrid: Elsevier, 2013), 51.
[19] Idem.
[20] Kristine Hamann and Rachel Smith, "Facial Recognition Technology: Where Will It Take Us?", American Bar Association Organization. Available at: https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/
[21] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", (Conference on Fairness, Accountability, and Transparency, 2018), 3. Available at: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

potential for abuse. As a matter of fact, the Latin American region is usually below adequate standards of data protection and privacy laws.[22] If there are no limits for the collection and storage of biometric data by enforcement agencies, security policies can be just an excuse for the creation of a 'police State'. There are many human rights issues related to FRT implementation for national or security purposes and clear dilemmas between security and privacy. In that sense, governments need to create or reform their surveillance and data protection frameworks in order to grant broader protection to their citizens. This might only be achieved by a human-centered regulation of FRT with high standards for data protection, privacy, and other fundamental rights. Governments and policymakers must prioritize the protection of fundamental rights when deploying FRT-operated systems.

[22] DLA PIPER, "Data protection laws of the world". Available at: https://www.dlapiperdataprotection.com/