Research Paper

US and the Americas Programme

November 2022

Regulating facial recognition in Latin America

Policy lessons from police surveillance in Buenos Aires and São Paulo

Carolina Caeiro

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Contents

Summary

- The use of facial recognition technology in public spaces for police surveillance has seen a swift take-up across Latin America. Its adoption appears motivated by political considerations. In a region where fighting crime is perceived as a major challenge, adopting the technology is a means for governments to signal to voters their intent to enhance public safety.
- Police rollout of the technology, however, can lend itself to abuse. Depending on how it is deployed, facial recognition may threaten an individual's right to privacy and, as a result, their rights to freedom of expression and freedom of assembly and association. The technology can also undermine the right to non-discrimination and disrupt judicial due process by challenging the principle of presumption of innocence.
- Two case studies – the deployment in the city of Buenos Aires from 2019 to 2022, and a pilot run in São Paulo in 2020 – expose common trends in the adoption of this type of biometric technology in Latin America. Facial recognition is deployed, following obscure procurement processes, on weak legal grounds, without proper human rights assessments and with inadequate transparency. Deployments rely on the use of police databases which reinforce structural discrimination, and standards for data use are poorly defined and lacking in transparency.
- While other major jurisdictions, including the US, the UK and the European Union, are enacting strict safeguards to move towards exceptional use of facial recognition in public spaces by law enforcement, Latin America may be said to be caught in a worst-case scenario.
- While arguments for banning the technology are compelling – such as facial recognition's potential role in exacerbating Latin America's existing inequalities and structural discrimination – the enactment of more robust safeguards where technology is already in use is both a preferable scenario and a more likely way forward than the continued use of facial recognition with inadequate safeguards.
- This research paper argues that policymakers in Latin America should work on building stronger safeguards around police uses of facial recognition in public spaces. To ensure that deployments remain compliant with international human rights law, policymakers should ensure that authorized uses of facial recognition steer clear of 'no-go' zones such as the indiscriminate use of live facial recognition which was, until recently, commonplace in Buenos Aires. In addition, Latin American governments should offer opportunities for public debate about the potential impacts of the technology, particularly prior to engaging in new deployments.

01 Introduction

Latin American city governments rolling out facial recognition in public spaces for law enforcement purposes are failing to properly assess potential human rights impacts and offer weak protections to citizens exposed to the technology.

When the City of Buenos Aires first deployed live facial recognition in 2019, its deputy mayor asserted that 'police forces [could] now do their job more efficiently'.[1] With the technology being initially rolled out across the city's rail networks, Argentina's minister of transport further reinforced this point, highlighting that while '82% of passengers report[ed] feeling safe on trains, this technological innovation [would] make them feel even safer'.[2]

The deployment of facial recognition technology in Latin America has been underpinned by claims about its ability to effectively identify potential criminals and enhance public safety.[3] Growing security concerns in large urban centres, astute outreach by – in many instances foreign – surveillance technology companies and a marked tendency towards techno-solutionism on the part of both politicians and technocrats have led many local governments to buy into the potential capabilities of facial recognition. Other governments – especially those of an authoritarian nature – have been enticed by the opportunity for greater social control.

---

1 Government of the City of Buenos Aires (2019), 'Se implementó el Sistema de Reconocimiento Facial en ferrocarriles' [Facial recognition system implemented on the railways], https://www.buenosaires.gob.ar/justiciayseguridad/noticias/se-implemento-el-sistema-de-reconocimiento-facial-en-ferrocarriles.
2 Ibid.
3 For example, the mayor of Mexico City, Claudia Sheinbaum Pardo, inaugurated a video monitoring centre equipped with facial recognition technologies in the city's central food market, claiming that the goal 'was to strengthen security in the market that receives 500 thousand visitors daily' (El Sol de Mexico (2020), 'Vigilan Central de Abasto con 636 cámaras conectadas a la policía' [Central Market to be surveilled with 636 cameras connected to the police], 2 January 2020, https://www.elsoldemexico.com.mx/metropoli/cdmx/vigilan-central-de-abasto-con-636-camaras-conectadas-a-la-policia-4651583.html). In Ecuador, the secretary of security and governance of the municipality of Quito, Juan Pablo Burbano, declared that the implementation of facial recognition technologies in the country's capital 'sought to prevent crime and identify the main areas with criminal activity' (See Primicias (2020), 'Reconocimiento facial, una salida contra la delincuencia en Quito' [Facial recognition, a way out to fight delinquency in Quito], 17 February 2020, https://www.primicias.ec/noticias/tecnologia/reconocimiento-facial-alternativa-contra-delincuencia-quito). In the case of Argentina, the minister of security, Patricia Bullrich, attended the launch of facial recognition systems in Buenos Aires and lauded the initiative. See Government of the City of Buenos Aires (2019), 'Se implementó el Sistema de Reconocimiento Facial en ferrocarriles' [Facial recognition system implemented on the railways].

While the adoption of facial recognition has sparked widespread debate across the US and Europe, the technology has had a swift take-up across Latin America. Argentina, Bolivia, Brazil, Colombia, Ecuador, Mexico, Paraguay and Peru have ongoing deployments or have run trials.[4] Chile, El Salvador, Guatemala and Uruguay have plans for its implementation, with Guatemala and Uruguay already running tenders for the purchase of the technology.[5] Deployments are suspected to have begun in Honduras and Nicaragua.[6]

Worldwide, multiple countries are beginning to grapple with how to regulate facial recognition. The European Union has proposed to treat biometric identification systems as a high-risk application of artificial intelligence (AI) and ban their use in public spaces, except for specific criminal investigations.[7] In 2020, a British court found that the South Wales Police – the body in charge of running facial recognition

---

4 For Bolivia, see La Razón (2020), 'Policía lanza plan 'Bolivia, destino seguro' para el Carnaval 2020' [Police launch plan 'Bolivia, a safe destination' for the 2020 Carnival], 31 January 2020, https://www.la-razon.com/sociedad/2020/01/31/policia-lanza-plan-bolivia-destino-seguro-para-el-carnaval-2020. For Colombia, see *El Tiempo* (2019), 'Helicóptero halcón de la Policía estrena identificación facial' [Police helicopter implements facial recognition], 20 November 2019, https://www.eltiempo.com/bogota/estrenan-helicoptero-halcon-con-reconocimiento-facial-en-paro-del-21-de-noviembre-435766, and Fundación Karisma (2021) 'Guía al reconocimiento facial en Colombia' [Guide to facial recognition in Colombia], 1 July 2021, https://digitalid.karisma.org.co/2021/07/01/guia-reconocimiento-facial. For Ecuador, see Metro Ecuador (2020), 'Quito: cámaras de reconocimiento facial funcionarán con altavoces para advertir a ciudadanos' [Quito: Facial recognition cameras to function alongside loudspeakers to warn citizens], 19 February 2020, https://www.metroecuador.com.ec/ec/noticias/2020/02/19/quito-camaras-reconocimiento-facial-funcionaran-altavoces-advertir-ciudadanos.html and Metro Ecuador (2020), 'Cámaras realizarán reconocimiento facial y captarán a delincuentes en tiempo real' [Cameras to use facial recognition to catch criminals in real time], 12 February 2020, https://www.metroecuador.com.ec/ec/noticias/2020/02/12/camaras-reconocimiento-facial-captaran-delincuentes-tiempo-real.html. For Mexico, see El Sol de Mexico (2020), 'Vigilan Central de Abasto con 636 cámaras conectadas a la policía' [Central Market to be surveilled with 636 cameras connected to the police] and R3D (2021), 'Descubren vulnerabilidades en Cámaras de Videovigilancia de Dahua' [Vulnerabilities discovered in Dahua video surveillance cameras], 11 October 2021, https://r3d.mx/2021/10/11/descubren-vulnerabilidades-en-camaras-de-videovigilancia-de-dahua. For Peru, see Arroyo, V. (2019), 'Cámaras con reconocimiento facial en Lima' [Cameras with facial recognition in Lima], Access Now, 14 November 2019, https://www.accessnow.org/camaras-con-reconocimiento-facial-en-lima. For Paraguay, see ABC (2019), 'Reconocimiento facial: nueva estrategia para combatir la delincuencia' [Facial recognition: new strategy to combat criminals], 11 July 2019, https://www.abc.com.py/nacionales/2019/07/11/reconocimiento-facial-nueva-estrategia-para-combatir-la-delincuencia.

5 For Chile, see InfoDefensa (2020), 'Ingesmart implementará en Chile un sistema de teleprotección con 1.000 cámaras', [Ingesmart to implement a system of teleprotection in Chile with 1,000 cameras], 8 April 2020, https://www.infodefensa.com/latam/2020/04/08/noticia-ingesmart-implementara-chile-sistema-teleproteccion-camaras.html. For El Salvador, see ReconocimientoFacial.info (2020), 'Plan Control Territorial contempla la implementación de 4,075 cámaras de videovigilancia en El Salvador', [Territorial Control Plan contemplates the implementation of 4,075 video surveillance cameras in El Salvador], 12 February 2020, https://reconocimientofacial.info/plan-control-territorial-contempla-la-implementacion-de-4075-camaras-de-videovigilancia-en-el-salvador. For Guatemala, see García, O. (2020), 'Mixco contará con cámaras de reconocimiento facial para tratar de combatir la delincuencia', [Mixco will count on facial recognition cameras to try to combat crime], Prensa Libre, 15 January 2020, https://www.prensalibre.com/ciudades/guatemala-ciudades/mixco-contara-con-camaras-de-reconocimiento-facial-para-tratar-de-combatir-la-delincuencia. Lastly, for Uruguay, see ReconocimientoFacial.Info (2021), 'Uruguay: del país de los derechos a la vigilancia del reconocimiento facial' [Uruguay: from a country that defends rights to a country with facial recognition], 6 April 2021, https://reconocimientofacial.info/uruguay-del-pais-de-los-derechos-a-la-vigilancia-del-reconocimiento-facial.

6 Bonifaz, R. (2020), *Herramientas de Vigilancia Digital Identificadas en Centroamérica* [Tools for Digital Surveillance Identified in Central America], Report, San José, Fundación Acceso, https://www.acceso.or.cr/wp-content/uploads/2021/08/2020_Art_Herramientas_Vigilancia_CA-mayo2020.pdf.

7 See Title II Prohibited Artificial Intelligence Practices Articles 5.1(d) and 5.2-4, European Commission (2021), *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, Brussels: European Commission, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206. For proposed updates to the Artificial Intelligence Act, see Council of the European Union (2021), *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Presidency compromise text*, Brussels: Council of the European Union, https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf (under the Council's Slovenian presidency) and Council of the European Union (2022), *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Progress report*, Brussels: Council of the European Union, https://artificialintelligenceact.eu/wp-content/uploads/2022/06/AIA-FRA-Progress-Report-16-May.pdf (under the Council's new French presidency).

trials in the UK – did not have sufficiently clear guidelines governing the deployment of facial recognition equipment in public places, and could have done more to assess the potentially discriminatory use of the technology.[8] In the US, widespread city-level bans throughout 2019 and 2020 sparked a debate about whether the technology is compatible with fundamental rights. To date, five states – California, Maine, Massachusetts, New York and Vermont – have either placed moratoriums on the use of facial recognition or have strictly regulated its use for policing purposes, allowing its deployment in public spaces only under specific circumstances.[9]

While Europe, the UK and the US are exploring regulatory frameworks to balance the tensions between the use of facial recognition in public spaces and the potential threats it poses to privacy and other fundamental rights, Latin America may well be described as being stuck in a worst-case scenario,[10] in that the technology is frequently being deployed or piloted on the continent despite a lack of robust regulatory frameworks to ensure proper protections, oversight and transparency. Bans on the use of the technology do not appear to be options available for debate.

This research paper will focus on the use of facial recognition technologies in public spaces and for law enforcement purposes, with reference to the city-level deployments in the Argentinian capital, Buenos Aires, between 2019 and 2022, and the technology piloting in São Paulo, Brazil's largest city, in 2020. Two potential routes emerge as alternatives to break away from the current worst-case scenario observed in the region. One route is the adoption of moratoriums on the use of facial recognition until proper safeguards are put in place and some uses of the technology possibly circumscribed. An alternative route, as proposed by human rights groups, is the enactment of comprehensive bans that prohibit the use of facial recognition for law enforcement purposes in public spaces.

Chapter 2 of the paper will set the scene, introducing the controversies surrounding the deployment of facial recognition, and the potential human rights impacts of the technology. Chapter 3 will look at trends in facial recognition deployments in Argentina and Brazil, focusing on the cases of Buenos Aires and São Paulo. Through the study of these deployments, the paper will document the underlying dynamics that are at play, as well as common trends in the adoption of this specific surveillance technology in the region. Chapter 4 will pose the question of why deployments in Latin America continue to take place despite negative human rights impacts. It suggests that politics plays a central role in motivating facial recognition rollouts. Drawing on policy developments in other jurisdictions, Chapter 5 will explore possible approaches to regulating facial recognition in Latin America, and Chapter 6 will present a concluding discussion on whether to ban or to regulate facial recognition in Latin America, offering a series of recommendations for regional policymakers.

---

8 UK Courts and Tribunal Judiciary (2020), 'Judgment R (Bridges) -v- CC South Wales', 11 August 2020, available at: https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales.
9 Ban Facial Recognition (2022), 'Ban Facial Recognition Map', https://www.banfacialrecognition.com/map (accessed 16 Aug. 2022).
10 Some countries in the Asia-Pacific region, such as China and Singapore, have also seen the widespread use of facial recognition, with seemingly ample public acceptance of the technology. Comparisons between the forms of its adoption in the Asia-Pacific and in Latin America are flagged by the author as an area for further research, but are beyond the scope of this paper.

02
The controversy surrounding facial recognition technology

How facial recognition technologies are deployed determines whether their use is compliant with international human rights law. This has rendered the technology extremely controversial.

Facial recognition is one of the most widespread – and perhaps most questionable – applications of AI.[11] Not only does its deployment risk reinforcing structural inequalities due to built-in algorithmic and data bias, but the technology can also serve as a tool for state surveillance.

The meaning of the term has become obfuscated, as it encompasses many different practices. The Electronic Frontier Foundation broadly defines face recognition as 'a method of identifying or verifying the identity of an individual using their face'.[12] The technology relies on the collection of biometric data – a type of personal data related to the physical and behavioural characteristics of an individual, which can include their facial traits, their gait or even their emotional state. Algorithms are trained using biometric databases to enable identification and verification of

11 Kind, C. (2020), 'Nowhere to hide', *The World Today*, 11 February 2020, https://www.chathamhouse.org/publications/the-world-today/2020-02/nowhere-hide.
12 Electronic Frontier Foundation (undated), 'Street-Level Surveillance', https://www.eff.org/pages/face-recognition.

individuals, and are then deployed as a software solution. In cities where video monitoring systems are already in place, the deployment of facial recognition is often a matter of adapting existing surveillance infrastructure by installing appropriate software updates.

Facial recognition gained momentum in the early 2010s, when AI deep-learning methodologies significantly improved its accuracy rates.[13] Despite these performance improvements, facial recognition was found to reinforce gender and racial discrimination. This was well documented in Joy Buolamwini and Timnit Gebru's 'Gender Shades', a study published in 2018 which showed how women of colour were most often misclassified by commercial AI systems.[14] The study shed light on how algorithmic bias – which can derive both from design decisions and from bias in the databases used to train algorithms – can give inaccurate results when attempting to identify women, people of colour and gender-nonconforming individuals. Since then, several companies have worked to reduce bias in their AI systems, though it still represents a significant limitation of the technology.[15]

Facial recognition is especially problematic when used in public spaces, for law enforcement purposes. Deployments connected to public safety are often designed to single out an individual from a crowd or database.[16] This is why the technology is mostly deployed in public spaces with high levels of circulation, such as in public transport networks or mass events. Identification differs from verification procedures which are used to corroborate the identity of a specific person – for example, to unlock a smartphone.[17] To identify a person, facial recognition systems deployed in public spaces analyse the biometric data of several individuals, including those who are not suspected of any crime. The right to privacy of all these individuals is compromised. The overtly invasive and potentially disproportionate nature of identification procedures render the use of facial recognition a problematic practice which, without the proper safeguards to prevent abuse, can easily be misused for surveillance.

The risk of misidentifying individuals also poses an important limiting factor when employing facial recognition for law enforcement purposes. Facial recognition systems estimate the probability of having a match, meaning that they have a margin of error that may result in false positives or false negatives. Being misidentified through false positives can have severe consequences, such as wrongful detentions. False positives also tend to echo gender, racial, class, age or able-bodied biases built into the technology. Additionally, false negatives

---

13 OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, Paris, https://www.oecd.org/publications/artificial-intelligence-in-society-eedfee77-en.htm.
14 Buolamwini, J. and Gebru, T. (2018), 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', Proceedings of Machine Learning Research, 81, pp. 1–15, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
15 Gloria, K. (2021), *Power and Progress in Algorithmic Bias*, Washington, DC: Aspen Digital, a programme of the Aspen Institute, https://www.aspeninstitute.org/wp-content/uploads/2021/07/Power-Progress-in-Algorithmic-Bias-July-2021.pdf.
16 Asociación por los Derechos Civiles (2022), 'Con mi cara no' [Not with my face], https://conmicarano.adc.org.ar.
17 When facial recognition is used for identification purposes, systems compare one face to many (1:n), whereas for verification purposes the comparison is one-to-one (1:1).

mean facial recognition systems might fail to identify persons of interest in criminal and national security investigations, therefore interfering with important individual rights while falling short in the delivery of purported benefits.

Evaluating facial recognition deployments in public spaces for law enforcement purposes calls for a thorough assessment of how each specific implementation may affect human rights. An important factor is whether identification of individuals occurs in real time or ex post. Live facial recognition deployed in public spaces, as defined by the College of Policing for England and Wales, entails the comparison of live camera feeds of faces against a predetermined 'watch list'.[18] According to the analysis put forth in the EU's Artificial Intelligence Act, this is especially intrusive for affected individuals, as it can disrupt the sphere of privacy of large segments of the population, evoke a sense of surveillance and potentially dissuade citizens from exercising other rights, such as the right to peaceful assembly.[19] Whenever a deployment relies on capturing images of non-wanted individuals – as opposed to solely capturing images of those who are indeed suspects – special attention is required to assess whether the deployment meets proportionality requirements and which measures are being put in place to prevent abusive use for surveillance purposes.

Evaluating facial recognition deployments in public spaces for law enforcement purposes calls for a thorough assessment of how each specific implementation may affect human rights.

Data use and retention practices are another important feature to consider when assessing human rights. The questionable retention, use or transfer of images obtained during identification procedures for purposes other than originally intended would raise red flags about the potential risks of surveillance. Similarly, the ways in which entities deploying facial recognition source biometric data, and whether they have legitimate access to use specific public databases that contain biometric data, will also determine whether a deployment is indeed compliant with human rights standards.

18 College of Policing (2022), 'Live facial recognition: Authorised professional practice', https://www.college.police.uk/app/live-facial-recognition.
19 See recital 18, Council of the European Union (2021), *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Presidency compromise text.*

Box 1. Law enforcement use of facial recognition in public spaces: the human rights impact

The deployment of facial recognition systems in public spaces, for law enforcement purposes, has chilling effects on multiple human rights.

First, facial recognition systems have an impact on the right to privacy. Privacy can be understood as the presumption that individuals should enjoy a private sphere that is free from state intervention.[20] This concept applies not only to secluded spaces, but also to public spaces, where facial recognition systems are often deployed.[21] In other words, when facial traits are scanned, facial recognition systems violate people's presumption of privacy in public spaces.

The indiscriminate amount of data processed by facial recognition systems renders it especially difficult for such systems to meet the principles of necessity and proportionality. Facial recognition deployments can also constitute a form of mass surveillance if they fail to meet the standards for permissible surveillance: being limited in scope and duration, targeted, and subject to independent authorization and oversight.[22] This type of mass surveillance also infringes on the right to privacy.

Facial recognition also has chilling effects on civil and political rights that are essential for democracy: the rights to freedom of opinion and expression, as well as of peaceful assembly and association. The threat of surveillance sets off a 'panopticon' effect which can lead to self-censorship, deter dissident voices and curtail freedom of expression.[23] Similarly, facial recognition systems can enhance the ability of governments to surveil protesters, discouraging and endangering those who seek to engage in peaceful protest.

The risk of being misidentified – aggravated primarily by racial, gender and class bias built into both algorithms and police databases – also undermines the right to non-discrimination, which requires states to treat individuals equally before the law and protect them against any form of discrimination.[24] It also places vulnerable communities at risk of being further marginalized.

Facial recognition systems can also have an impact on the right to due process and the principle of presumption of innocence, which are the cornerstones of fair judicial processes. Facial recognition systems used in public spaces to identify wanted criminals from a crowd treat all individuals in the public space as potential

---

20 UN General Assembly, Human Rights Council (2018), *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*, https://undocs.org/A/HRC/39/29.
21 Ibid.
22 Ibid.
23 Bernal, P. (2016), 'Data gathering, surveillance and human rights: recasting the debate', *Journal of Cyber Policy*, 1 (2), pp. 243–64, https://doi.org/10.1080/23738871.2016.1228990.
24 The rights to non-discrimination and to equality before the law are enshrined in Articles 2.1 and 26 of the International Covenant on Civil and Political Rights (ICCPR) respectively. Article 2.2 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) further stipulates that states parties to the covenant must guarantee access to economic, social and cultural rights without discrimination.

suspects. As highlighted by several human rights activists in Latin America and documented in a number of wrongful detentions,[25] the burden of proof is sometimes inverted when the onus to prove one's innocence is placed on the individual identified by facial recognition systems – as opposed to being placed on the state, which would normally have the responsibility to prove an individual's guilt.[26]

25 For argumentation on inverted burden of proof, see the civil society communiqué against the legalization for security uses of facial recognition systems in Buenos Aires signed by Access Now, Argentina's Asociación por los Derechos Civiles [Association for Civil Rights], Amnesty International Argentina, the Centro de Estudios Legales y Sociales (CELS) [Centre for Legal and Social Studies], DATAS, Fundación Vía Libre and the Observatorio de Derecho Informático Argentino (ODIA) [Observatory of Argentine Computer Law]. Access Now, Amnesty International, ADC, CELS, DATAS, Vía Libre and ODIA (2020), 'La Legislatura porteña debe rechazar el uso de la tecnología de reconocimiento facial para la vigilancia del espacio público' [The Buenos Aires legislature must reject the use of facial recognition for surveillance in the public space], Amnistia.org.ar, 22 October 2020, https://amnistia.org.ar/wp-content/uploads/delightful-downloads/2020/10/Comunicado-conjunto-reconocimiento-facial.pdf. For wrongful detentions see, for example, the cases of Guillermo Ibarola in Buenos Aires, who was wrongfully detained for six days following his misidentification by the Buenos Aires facial recognition system and of Leo Colombo, another individual misidentified by the local facial recognition system, who reportedly spent hours convincing officers he was not the wanted criminal in question. Brief case descriptions available at Infobae (2019), 'Un hombre estuvo seis días preso por un error policial' [Man imprisoned for six days for a police error], 2 August 2019, https://www.infobae.com/sociedad/policiales/2019/08/02/un-hombre-estuvo-seis-dias-preso-por-un-error-del-sistema-de-reconocimiento-facial and Gershgorn, D. (2020), 'The U.S. Fears Live Facial Recognition. In Buenos Aires, It's a Fact of Life', OneZero, 4 March 2020, https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d.
26 Please note that where the burden of proof lies may vary by jurisdiction.

03
Facial recognition rollouts: trends in Buenos Aires and São Paulo

The deployment of facial recognition in Argentina and Brazil reveals common patterns and shortcomings in the rollout of the technology.

The adoption of facial recognition technologies in multiple spheres of life has been rapidly embraced in two of the largest countries in Latin America – Argentina and Brazil.

Live facial recognition – which is widely feared by detractors of the technology – was regularly used in Argentina's capital city, Buenos Aires, between 2019 and 2022.[27] Security forces in the city employed live footage to vet passers-by against the country's national fugitive database, in order to identify potential criminals who had evaded justice.[28] The system worked through video monitoring systems

27 Gershgorn (2020), 'The U.S. Fears Live Facial Recognition', and Ombudsman of the City of Buenos Aires (2022), 'La Justicia Porteña Suspendió el Sistema de Vigilancia y Reconocimiento Facial' [The Buenos Aires judiciary suspends the surveillance and facial recognition system], https://defensoria.org.ar/noticias/la-justicia-portena-suspendio-el-sistema-de-vigilancia-y-reconocimiento-facial.

28 While the city government claims the system use was discontinued during the pandemic due to the use of face masks, the 2022 court investigation that imposed the suspension of the system maintains that facial recognition systems were still in use. See Clarin (2022) 'Otro fallo judicial polémico: suspenden el sistema de reconocimiento facial en la Ciudad de Buenos Aires' [Another controversial judicial resolution: facial recognition system suspended in the City of Buenos Aires], 14 June 2022, https://www.clarin.com/politica/fallo-judicial-polemico-suspenden-sistema-reconocimiento-facial-ciudad-buenos-aires_0_pxFjXMiM40.html; and Bertoia, L. (2022), 'Espionaje ilegal en CABA: se usó el sistema de reconocimiento facial con políticos, periodistas y jueces' [Illegal surveillance in Buenos Aires: Facial recognition used with politicians, journalists and judges], Página 12, 13 April 2022, https://www.pagina12.com.ar/414933-espionaje-ilegal-en-caba-se-uso-el-sistema-de-reconocimiento.

set up throughout the city, including in the three main railway stations and on the underground transport network, which is used by more than 1.3 million passengers per day.[29] The use of the technology was temporarily suspended in April 2022 by a court order which alleged that the system had been misused to run unauthorized searches.[30] Shortly afterwards, in September 2022 a city court declared the current conditions under which the system was operating to be unconstitutional.[31] The ruling, against which an appeal is likely to be lodged, is expected to further extend the suspension of the facial recognition system.

Facial recognition has been deployed for marketing purposes, with highly controversial emotion detection techniques having been used to place advertisements in front of passengers in the São Paulo Metro.

While implementation is most highly consolidated in the capital, Argentina's Association for Civil Rights (Asociación por los Derechos Civiles – ADC) reports that as at early 2021 facial recognition had also been deployed or piloted in the provinces of Córdoba, Salta and Mendoza, as well as in the county of Tigre in the province of Buenos Aires.[32] There are also programmed deployments in the province of Santa Fe.

In the case of Brazil, the use of facial recognition is far more widespread, with deployments identified in 30 cities as of 2019.[33] The technology is used for diverse purposes. Facial recognition has been adopted purportedly to prevent fraud in the distribution of social benefits: it has been used to verify the identities of beneficiaries of public transport subsidies in multiple Brazilian cities, and to track school attendance requirements for cash transfer programmes in the state of Pernambuco.[34] The technology has also been deployed for marketing purposes, with highly controversial emotion detection techniques having been used to place advertisements in front of passengers in the São Paulo Metro.[35]

---

29 Buenos Aires Ciudad (2022), 'Subte cada 3 minutos y WIFI', [Subway every 3 minutes and with WiFi] https://www.buenosaires.gob.ar/compromisos/subte-cada-3-minutos-y-wifi.
30 See additional information below, under 'Weak legal grounds and a lack of human rights assessments'.
31 Rosende, L. (2022), 'La justicia declaró inconstitucional el modo en que la Ciudad usa el sistema de reconocimiento facial' [The judiciary declared unconstitutional the way in which the Buenos Aires City uses the system of facial recognition], *Tiempo Argentino*, https://www.tiempoar.com.ar/informacion-general/la-justicia-declaro-inconstitucional-el-modo-en-que-la-ciudad-usa-el-sistema-de-reconocimiento-facial.
32 Asociación por los Derechos Civiles (2022), 'Con mi cara no' [Not with my face] (accessed 16 Aug. 2022).
33 Instituto Igarapé (undated), 'Infográfico reconhecimento facial no Brasil' [Infographic: Facial recognition in Brazil], https://igarape.org.br/infografico-reconhecimento-facial-no-brasil (accessed 13 Apr. 2022).
34 Ventura, F. (2015), 'Ônibus adotam biometria facial em todo o Brasil para evitar fraudes' [Buses adopt facial biometrics in all of Brazil to prevent fraud], Gizmodo Brazil, 18 December 2015, https://gizmodo.uol.com.br/onibus-e-biometria-facial; and Canto, M. (2019), *We don't need no observation: The use and regulation of facial recognition in Brazilian public schools*, Global Information Society Watch, https://www.giswatch.org/pt-br/node/6159.
35 Arroyo, V. and Leufer, D. (2020), 'Facial recognition on trial: emotion and gender "detection" under scrutiny in a court case in Brazil', Access Now Blog, 29 June 2020, https://www.accessnow.org/facial-recognition-on-trial-emotion-and-gender-detection-under-scrutiny-in-a-court-case-in-brazil.

The latter project was eventually rolled back, after a local court declared that data collection on Metro passengers did not meet minimum consent requirements.[36]

Perhaps the most controversial application of facial recognition is in the context of public safety. Widespread crime and high murder rates in Brazil have rendered average citizens amenable to embracing the promises of new surveillance technologies.[37] The ascent to the presidency in 2019 of the far-right Jair Bolsonaro was itself facilitated by his controversial promises to crack down on domestic insecurity, relying on the increased involvement of military forces to deal with public safety issues. In 2022, public safety continued to be a central theme in the presidential campaign, along with the state of the Brazilian economy. Specific examples of facial recognition applied to public safety in the country include the deployment of live monitoring during the Carnival celebrations in São Paulo, the use of cameras mounted on police uniforms in Rio de Janeiro, and the establishment of facial recognition systems in the cities of Salvador de Bahía and Campinas.[38]

Common trends: the cases of Buenos Aires and São Paulo

Deployments in the cities of Buenos Aires and São Paulo offer some compelling insights into the adoption of facial recognition in the Latin American region. This section of the paper will focus closely on two distinct implementations in public spaces, for law enforcement purposes: the adoption by the Buenos Aires city police, starting in 2019, of live facial recognition technology to study passengers on the public transport network; and a pilot deployment conducted during the 2020 Carnival by the Civil Police of the State of São Paulo.[39]

---

36 Altman, G. (2018), 'Em liminar, Justiça impede o uso de câmeras de reconhecimento facial no metrô' [In an injunction, Court prevents the use of facial recognition cameras in the Metro], Jota, 14 September 2018, https://www.jota.info/justica/mp-cancele-cameras-metro-14092018. For specificities on the case, please see arguments presented by the plaintiff, Brazil's Institute of Consumer Protection: Instituto Brasileiro de Defesa do Consumidor (2021), 'Em ação do Idec, Justiça condena ViaQuatro por reconhecimento facial não consentido no Metrô de SP' [Through legal action by IDEC, the judiciary finds ViaQuatro guilty for non-consensual facial recognition in the São Paulo Metro], press release, 10 May 2021, https://idec.org.br/release/em-acao-do-idec-justica-condena-viaquatro-por-reconhecimento-facial-nao-consentido-no-metro.

37 Ionova, A. (2020), 'Brazil takes a page from China, taps facial recognition to solve crime', The Christian Science Monitor, 11 February 2020, https://www.csmonitor.com/World/Americas/2020/0211/Brazil-takes-a-page-from-China-taps-facial-recognition-to-solve-crime.

38 For São Paulo, see Mari, A. (2020), 'Brazilian police introduces live facial recognition for Carnival', ZDNet, 25 February 2020, https://www.zdnet.com/article/brazilian-police-introduces-live-facial-recognition-for-carnival; for Rio de Janeiro, see GloboNews (2020), 'PMs do RJ usarão microcâmeras nos uniformes' [Military police in Rio de Janeiro will use micro-cameras on their uniforms], 13 January 2020, https://g1.globo.com/rj/rio-de-janeiro/noticia/2020/01/13/uniforme-da-pm-do-rj-vai-ganhar-microcameras.ghtml; for Bahia, see Palma, A. and Pacheco, C. (2020), 'Presos pela cara: polêmico sistema de reconhecimento facial identificou 109 foragidos na BA' [Imprisoned by the face: Controversial facial recognition system identified 109 outlaws in Bahia], Correio, 5 January 2020, https://www.correio24horas.com.br/noticia/nid/presos-pela-cara-polemico-sistema-de-reconhecimento-facial-identificou-109-foragidos-na-ba; and for Campinas, see Campinas Municipal Town Hall (2018), 'Prefeitura apresenta "Cidade Segura" com câmeras de reconhecimento facial' [Town Hall presents 'Safe City' with facial recognition cameras], http://www.campinas.sp.gov.br/noticias-integra.php?id=35530.

39 In the case of Brazil, there have been multiple attempts to deploy facial recognition in public transport; in 2021, the state legislature approved a bill that would have required the São Paulo Metro and metropolitan train system to deploy facial recognition. This law would lay the foundations for the establishment of partnerships with security forces, but was vetoed by the governor of the state of São Paulo following a successful advocacy campaign by rights groups. In June 2021, the São Paulo Metro rolled out the use of facial recognition technologies on the Red line: by 2023, the deployment is expected to have extended to all stations on each of four metro lines, out of an overall total of six lines, including the monorail. (See domtotal.com (2021) 'Metrô de São Paulo terá câmeras com reconhecimento facial' [São Paulo metro will have cameras with facial recognition], 24 June 2021, https://domtotal.com/noticias/index.jsp?id=1523868.) While it has been profoundly problematic, this case is intentionally excluded from this paper as the deployment is handled by the public–private consortium commissioned to run the São Paulo Metro, and therefore is not strictly a deployment by law enforcement agencies.

Six common trends are identified: (1) a justification of the use of facial recognition in the name of public safety; (2) the adoption of facial recognition systems through obscure procurement processes, and amid growing efforts to place surveillance technologies in Latin American markets; (3) the deployment of facial recognition systems on weak legal grounds, and without proper human rights assessments; (4) the establishment of inadequate transparency and oversight mechanisms; (5) a reliance on the use of police databases that reinforce structural discrimination; and (6) poorly defined standards in data use and retention.

Public safety as the justification for deployment

Security is a central concern across Latin American cities, and Buenos Aires and São Paulo are no exception. In both cities, government officials and law enforcement agencies have leveraged public safety as the leading justification for deploying facial recognition in public spaces.

In the case of São Paulo, the biometric identification laboratory at the Instituto de Identificação Ricardo Gumbleton Daunt (Ricardo Gumbleton Daunt Identification Institute – IIRGD), under the purview of the state's Civil Police, ran a live facial recognition trial during the celebrations for the 2020 Carnival. During the inauguration of what was referred to in the press as 'the facial recognition lab', São Paulo's state governor asserted that statewide security forces would find the technology to be an 'important ally to fight against criminals and search for missing persons'.[40] However, the use of facial recognition to curb crime appears to be disproportionate. Overall, in 2018 Brazil ranked as the country with the 16th highest murder rate in the world, with 27.38 murders per 100,000 inhabitants.[41] The wealthy state of São Paulo, however, is significantly safer, boasting one of the lowest murder rates in the country, at 8.2 per 100,000 in 2018.[42] Searching for missing persons also features prominently as a justification for the deployment of the technology, this proposed use being less likely to draw criticism from the public.

In the case of Buenos Aires, similar arguments have been invoked to justify the deployment of facial recognition across the public transport network. The system, operated by the Urban Monitoring Centre of the Buenos Aires City Police, was set up in April 2019. During its launch, the city's mayor Horacio Rodríguez Larreta asserted that the government's 'sole purpose was to ensure the residents of Buenos are safer and not walking among criminals in the streets'.[43] At a time when 'smart city' projects are booming across Latin America, the adoption of facial recognition has also been portrayed as a sign of state modernization. Reinforcing

---

40 Tomaz, K. (2020), 'Carnaval de SP vai ter sistema de reconhecimento facial para identificar criminosos e desaparecidos, diz Doria' [The São Paulo Carnival will have facial recognition to identify criminals and missing persons, says Doria], Globo, 28 January 2020, https://g1.globo.com/sp/sao-paulo/carnaval/2020/noticia/2020/01/28/carnaval-de-sp-vai-ter-sistema-de-reconhecimento-facial-para-identificar-criminosos-e-desaparecidos-diz-doria.ghtml.
41 World Population Review (2022), 'Murder Rate by Country 2022', https://worldpopulationreview.com/country-rankings/murder-rate-by-country (accessed 15 Sep. 2022).
42 Instituto de Pesquisa Econômica Aplicada (2020), *Atlas da Violência 2020* [Violence Atlas 2020], Brasília, IPEA, https://www.ipea.gov.br/atlasviolencia/download/24/atlas-da-violencia-2020.
43 Rodríguez Larreta, who initiated the use of facial recognition in the city of Buenos Aires, remains in office. His second mandate is due to expire on 9 December 2023.

this view, Rodríguez Larreta described the adoption of facial recognition as an 'additional step in incorporating the use of technology to protect the population'.[44]

Security concerns carry a significant weight in Argentina, despite indications that public safety is not as severe a challenge as in other Latin American countries. For example, Argentina has a murder rate comparable to that of the US.[45] The Economist Intelligence Unit's *Safe Cities Index 2019*, which among other indicators measures the prevalence of violent and petty crime, ranked Buenos Aires as having an acceptable level of personal safety.[46] Average citizens, however, are highly concerned about public safety. A 2020 poll found that seven out of 10 Argentinians identified insecurity as one of the most pressing policy concerns in the country.[47]

Obscure procurement and a growing market for surveillance technology

Transparent procurement processes allow the public to independently assess a government's acquisition of technology; to know what specific companies and countries are serving as technology providers; and to learn about important features of the systems acquired, such as the efficacy rates of different facial recognition systems or efforts to address issues of bias in AI-based technologies.[48]

In both Buenos Aires and São Paulo, procurement processes to acquire facial recognition systems have been opaque, with little information having been made available to the public on the technologies employed. This is not unusual in either Argentina or Brazil where, in spite of existing regulation, procurement processes tend to be marred by questionable transparency practices and documented instances of rigged bidding.[49] Available information is pieced together from ad hoc statements to the press, freedom-of-information access requests and investigative reporting by local civil society organizations.

---

44 Government of the City of Buenos Aires (2019), 'Rodríguez Larreta presentó el Sistema de Reconocimiento Facial De Prófugos: 'El objetivo es que los vecinos estén más seguros" [Rodríguez Larreta presented the Facial Recognition System for Fugitives: 'The goal is for the community to be safer'], https://www.buenosaires.gob.ar/jefedegobierno/noticias/rodriguez-larreta-presento-el-sistema-de-reconocimiento-facial-de-profugos.
45 According to the latest available data for both countries, in 2018 the US had a murder rate of 4.96 and Argentina of 5.32 murders per 100,000 people. See World Population Review (2022), 'Murder Rate by Country 2022', https://worldpopulationreview.com/country-rankings/murder-rate-by-country (accessed 15 Sep. 2022).
46 Economist Intelligence Unit (2019), *Safe Cities Index 2019: Urban security and resilience in an interconnected world*, https://safecities.economist.com/wp-content/uploads/2019/08/Aug-5-ENG-NEC-Safe-Cities-2019-270x210-19-screen.pdf.
47 Observatorio de Psicología Aplicada (2020), 'Monitor de Inseguridad No. 2 – Diciembre 2020' [Insecurity Monitor No. 2, December 2020], http://www.psi.uba.ar/opsa/informes/monitor_inseguridad_pais_2.pdf.
48 There is growing awareness about the importance of ensuring government transparency in technology acquisition. The World Economic Forum, for example, has issued an AI procurement kit that offers valuable transparency recommendations, and the UK government launched AI procurement guidelines in 2020. See World Economic Forum (2020), *AI Procurement in a Box: AI Government Procurement Guidelines*, toolkit, https://www3.weforum.org/docs/WEF_AI_Procurement_in_a_Box_AI_Government_Procurement_Guidelines_2020.pdf; and HM Government, (2020), *Guidelines for AI procurement*, 8 June 2020, https://www.gov.uk/government/publications/guidelines-for-ai-procurement/guidelines-for-ai-procurement#top-10-considerations.
49 See OECD (2021), *Fighting Bid Rigging in Brazil: A Review of Federal Public Procurement*, https://www.oecd.org/competition/fighting-bid-rigging-in-brazil-a-review-of-federal-publicprocurement.htm; and OECD (2019), *Fighting Bid Rigging in the Procurement of Public Works in Argentina*, https://www.oecd.org/competition/fighting-bid-rigging-in-public-procurement-in-argentina.htm.

The surveillance technologies employed across Latin America have been purchased from a varied ecosystem of sources which includes but is not limited to countries such as China, Israel and Russia, all of which have a strong trade presence in the region as providers of surveillance technology. The technology piloted in São Paulo, for example, is supplied by Western companies. The facial recognition system employed by the State of São Paulo and deployed at the IIRGD's biometric identification laboratory was provided by the Brazilian subsidiary of Gemalto, a Dutch company which was subsequently acquired by France's Thales Group.[50] No information is available about the specific technology employed, or its accuracy rates in identifying individuals. For the live trials run during the carnival in São Paulo, the biometric laboratory relied on live footage collected through the 'City Cameras' project – a city-wide video distribution network based on closed-circuit television (CCTV) technology developed by Microsoft.[51]

The surveillance technologies employed across Latin America have been purchased from a varied ecosystem of sources which includes countries such as China, Israel and Russia, all of which have a strong trade presence in the region as providers of surveillance technology.

In the case of Buenos Aires, the city government engaged the locally based Danaide SA, a provider which commercializes in the domestic market surveillance technologies that are developed overseas. Through a freedom-of-information access request submitted in 2019, the ADC confirmed that the facial recognition system provided by Danaide is of Russian origin.[52] The firm that developed the software claims it has an accuracy rate of 80 per cent.[53]

The Latin American market has been increasingly targeted by a range of overseas surveillance technology companies seeking to place their products on the continent. For example, São Paulo's City Cameras project incorporated additional cameras donated by Chinese firms, evidencing both the intention of such firms to encourage the adoption of surveillance technologies by authorities in Latin America, and those authorities' own interest in expanding surveillance

50 Silva, V. H. (2020), 'Polícia de SP inaugura laboratório de reconhecimento facial' [São Paulo Police inaugurates facial recognition lab], Tecnoblog, 29 January 2020, https://tecnoblog.net/323082/policia-civil-sao-paulo-inaugura-laboratorio-reconhecimento-facial.
51 Carvalho, J. (2017), 'Microsoft participa de projeto "City Câmeras" para monitorar cidade de SP' [Microsoft participates in "City Cameras" project to monitor the city of São Paulo], IPNews, 17 March 2017, https://ipnews.com.br/microsoft-participara-de-projeto-city-cameras-da-prefeitura-de-sp.
52 Government of the City of Buenos Aires (2019), *Response to Access Information Request by ADC*, File NO-2019-21065074-GCABA-DGAYCSE, 2 July 2019, https://adc.org.ar/wp-content/uploads/2019/07/Respuesta-PAIP-reconocimiento-facial-GCBA-V2.pdf.
53 Gershgorn (2020), 'The U.S. Fears Live Facial Recognition'.

networks.[54] A 2021 report by Access Now on surveillance technology providers in Latin America has also drawn attention to a lack of transparency in acquisition processes across the region and a failure on the part of local governments to enable a proper public dialogue about the potential impacts of this type of technology.[55]

Countries which export surveillance technology also hold responsibility for the use of these products in developing countries. In 2019 David Kaye, the UN Special Rapporteur on freedom of opinion and expression, called for a moratorium on the sale of surveillance equipment, particularly across the Global South, until 'rigorous human rights safeguards are put in place' for both governments and non-state actors.[56] Most recently, in 2021, the UN Human Rights Council issued a resolution to revisit the UN Guiding Principles on Business and Human Rights to explore the role of the private sector in the development and spread of emerging technologies that threaten human rights.[57]

Weak legal grounds and a lack of human rights assessments

Both Argentina and Brazil have federal systems of government where municipal, state and federal legislations coexist and, in some cases, contradict one another. This generates complex, patchwork-style regulatory frameworks with varying standards and safeguards.

This dynamic has played out in the ways local governments have sought to justify the legality of facial recognition deployments. Argentina and Brazil have seen a combination of city legislation and state-level regulatory proposals that fall short of standards enshrined in their respective constitutions, international human rights treaties and federal laws.

In the case of Buenos Aires, the deployment of facial recognition technologies initially took place on weak legal grounds, being introduced through a resolution of the city government rather than an actual law.[58] However, in October 2020, the city legislature legalized the use of facial recognition technologies through the modification of Law 5688 of 2016, which regulates the city's security systems.[59] The amendment was strongly opposed by civil society organizations, which highlighted the government's failure to conduct proper human rights assessments,

---

54 Ribeiro, B. (2017), 'Doações de chineses a Doria somam R$8,5 mi' [Donations by the Chinese to Doria add up to R$8.5 million], Estadão, 29 July 2017, https://sao-paulo.estadao.com.br/noticias/geral,doacoes-de-chineses-a-sp-somam-r-8-5-mi,70001912058; and Schwartz, L. (2021), 'Major surveillance firms are 'gifting' tools to find a foothold in Latin America', Rest of World, 12 August 2021, https://restofworld.org/2021/surveillance-latin-america-access-now.
55 Access Now (2021), *Surveillance Tech in Latin America: Made Abroad, Deployed at Home*, Access Now, https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.
56 United Nations General Assembly, Human Rights Council, *Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/41/35, 28 May 2019, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement.
57 United Nations General Assembly, Human Rights Council, 'New and emerging digital technologies and human rights', A/HRC/47/L.12/Rev.1, 13 July 2021, https://undocs.org/A/HRC/47/L.12/Rev.1.
58 The city of Buenos Aires is an autonomous federal district with the capacity to sanction its own legislation. See Legislature of the City of Buenos Aires (2019), '25 años de autonomía de la Ciudad de Buenos Aires' [25 years of autonomy for the City of Buenos Aires], https://www.legislatura.gov.ar/posts/25-anos-de-autonomia-de-la-ciudad-de-buenos-aires147.html.
59 Legislature of the City of Buenos Aires (2016), 'Ley 5688: Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires' [Law 5688: Integral System of Public Safety for the Autonomous City of Buenos Aires].

particularly around the right to privacy. [60] This point was reinforced firstly in 2019 and again in 2021 by the UN Special Rapporteur on the right to privacy, who expressed concern about how facial recognition was deployed in Buenos Aires 'without the necessary privacy impact assessment or the desirable consultation and strong safeguards'.[61]

The existence of a city-level regulation does not mean that facial recognition in Buenos Aires meets the principle of legality.[62] The impact of the technology on the right to privacy – enshrined in Articles 18 and 19 of Argentina's national constitution – remains to be properly assessed. In addition, Argentina has not only ratified international human rights treaties but has also granted constitutional status to the rights set out in the International Covenant on Civil and Political Rights (ICCPR), and the American Convention on Human Rights (ACHR).[63] Beyond privacy assessments, the Buenos Aires city government has not evaluated how facial recognition impacts other fundamental rights, including the rights to freedom of expression, freedom of assembly and association, and the right to non-discrimination.

The existence of a city-level regulation does not mean that facial recognition in Buenos Aires meets the principle of legality. The impact of the technology on the right to privacy remains to be properly assessed.

Civil society in Argentina has played an active role in questioning the legality of facial recognition deployments. ADC, the local civil society organization, presented a legal action in 2019 to declare the use of the technology in Buenos Aires unconstitutional: after being on hold for almost three years, the request was eventually rejected.[64] In 2020 the Observatory of Argentine Computer Law (Observatorio de Derecho Informático Argentino – ODIA) presented a writ of amparo before the judiciary to halt the use of facial recognition in Buenos Aires.[65] The legal action led to an investigation in 2022 by a city judge, who found that the city government had used special permits granted for its facial recognition system to run unauthorized searches for individuals who did not feature in any

---

60 For civil society joint communiqué, see Diario Judicial (2020), 'Sonría, lo estamos filmando' [Smile, you are on camera], Diario Judicial, 22 October 2020, https://www.diariojudicial.com/nota/87691.
61 United Nations General Assembly, Human Rights Council, *Visit to Argentina: Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci*, A/HRC/46/37/Add.5, 27 January 2021, https://undocs.org/A/HRC/46/37/Add.5.
62 In addition, at the national level, Resolution 238/20212 of the Ministry of Security establishes a protocol for the use of video monitoring in public spaces. According to the protocol, video monitoring must respect individuals' privacy and uphold standards set forth in Argentina's data protection law. The sheer scale of video monitoring for facial recognition – which surveils citizens en masse – indicates that the deployment may be in direct conflict with the standards established in the protocol.
63 Levit, J. K. (1999), *The Constitutionalization of Human Rights in Argentina: Problem or Promise?*, Columbia Journal of Translational Law, 37, pp. 281–355. Available at: https://digitalcommons.law.utulsa.edu/cgi/viewcontent.cgi?article=1239&context=fac_pub.
64 Asociación por los Derechos Civiles (2019), 'El reconocimiento facial para vigilancia no pertenece a nuestro espacio público' [Facial recognition for surveillance does not belong in our public space], 6 November 2019, https://adc.org.ar/2019/11/06/el-reconocimiento-facial-para-vigilancia-no-pertenece-a-nuestro-espacio-publico.
65 Commonly used in Spanish-speaking legal systems, the writ of amparo is a mechanism to seek remedy for the protection of constitutional rights. For further information, see Observatorio de Derecho Informático Argentino (ODIA) [Observatory of Argentine Computer Law], 'Nuestro Trabajo: Reconocimiento facial' [Our Work: Facial recognition], https://odia.legal.

criminal or missing persons watch lists.[66] The local judge ordered the suspension of the facial recognition system, in what became the first active involvement of an Argentine court in the facial recognition debate.[67] Shortly afterwards, in September 2022, ODIA's pending writ of amparo was resolved with a city-level court finding that the facial recognition system – as currently deployed – is unconstitutional.[68] While the resolution is likely to be contested, it highlighted blind spots in the legal framework underpinning the use of facial recognition in the city of Buenos Aires.

Argentina's outdated data protection law has also been another point of contention around facial recognition deployments. The law, established in 2000, is widely considered as no longer fit to properly address the challenges that have emerged through the adoption of new technologies and the growth of the internet.[69] As biometric technologies are increasingly deployed in the country, civil society actors have called for the immediate update of this piece of legislation, asking for clear guidelines and protections to be applied to the collection of sensitive personal data through technologies such as facial recognition.[70] Efforts to have Argentina's data protection law updated have not yet borne fruit.[71]

Facial recognition deployments in Brazil have also rested on weak legal grounds. In the case of São Paulo, the local city government has steered clear from attempting to regulate facial recognition through city-level legislation. This appears to be a trend across the country, where city legislatures have refrained from pronouncements on the use of facial recognition. However, the state of São Paulo came close to passing regulation on the subject. During his tenure as governor (2019–22), João Doria – who had otherwise been an avid supporter of the deployment of surveillance technologies – vetoed a bill approved by the state legislature following a successful advocacy campaign from civil society. The law would have required the São Paulo Metro and metropolitan train system to deploy facial recognition, preparing the ground for later partnerships with

---

66 Ombudsman of the City of Buenos Aires (2022), 'La Justicia Porteña Suspendió el Sistema de Vigilancia y Reconocimiento Facial' [The Buenos Aires judiciary suspends the surveillance and facial recognition system].
67 The government of the City of Buenos Aires attempted to recuse the judge from the investigation, though the request was denied. The resolution to halt the use of the facial recognition system in Buenos Aires had been reinstated at the time of this paper's publication, although it is likely to be contested again before the Supreme Court of Justice. See Espósito, N. (2022), 'La justicia sostuvo la suspensión del sistema de reconocimiento facial de la Ciudad por uso indebido' [The judiciary upheld the suspension of the facial recognition system in the city due to misuse], *Tiempo Argentino*, 1 June 2022, https://www.tiempoar.com.ar/politica/la-justicia-sostuvo-la-suspension-del-sistema-de-reconocimiento-facial-de-la-ciudad-por-uso-indebido.
68 Rosende (2022), 'La justicia declaró inconstitucional el modo en que la Ciudad usa el sistema de reconocimiento facial' [The judiciary declared unconstitutional the way in which the Buenos Aires City uses the system of facial recognition].
69 Argentine Congress, *Ley 25.326: Protección de los Datos Personales*, [Law 25.326: Protection of Personal Data], available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm.
70 Ferreyra, E. (2020), 'Facial recognition in Latin America: Towards a human rights-based legal framework to protect public spaces from mass surveillance', Global Campus of Human Rights, https://repository.gchumanrights.org/items/b6fb1ba9-95d2-436a-a4ef-a2471b54a9cf.
71 Bio, D. (2019), 'Expertos en protección de datos piden modificar la ley: "Corremos el riesgo de ser manipulados por empresas o gobiernos"' [Experts in data protection ask to modify the law: "We run the risk of being manipulated by companies or governments"], Infobae, 21 September 2019, https://www.infobae.com/politica/2019/09/21/expertos-en-proteccion-de-datos-piden-modificar-la-ley-corremos-el-riesgo-de-ser-manipulados-por-empresas-o-gobiernos. A new bill proposal was presented in November 2020, though it failed to become law. See Chamber of Deputies of Argentina (2020), 'Bill Proposal: Personal Data Protection Law', available at: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2020/PDF2020/TP2020/6234-D-2020.pdf.

security forces.[72] At least four further bill proposals were made at the state and federal levels between 2019 and 2020, indicating a growing intention to regulate facial recognition technology.[73] As in Argentina, many of these proposals sought to provide a 'green light' for the adoption of facial recognition in Brazil, with little attention being paid to building in adequate safeguards.

This situation may soon change, however. In March 2022 the Brazilian federal senate created a commission of legal experts to advise on the drafting of a proposed bill for the regulation of AI.[74] Following a series of public audiences to incorporate contributions from subject-matter experts across a wide range of backgrounds – from academia to local think-tanks, civil society organizations and legal experts – the commission's rapporteur expressed concern about algorithmic biases in the technology and the impact on the rights of children, hinting that the commission may consider banning the use of facial recognition for law enforcement purposes.[75] In June 2022, a civil society-driven campaign entitled #SaiDaMinhaCara [which translates as 'Get out of my face'] encouraged 50 state and municipal legislators to introduce proposals to ban facial recognition from being used in public spaces.[76]

Discussions around the use of facial recognition in Brazil are strongly underpinned by existing national regulation and the right to privacy as enshrined in the country's constitution. In addition, the country has ratified both the ICCPR and the ACHR. In sum, this means that facial recognition deployments must uphold privacy standards and their impacts on rights to freedom of expression, peaceful assembly and non-discrimination must be considered.[77]

Brazil also boasts one of the most progressive data protection laws in the wider Latin American region: the General Personal Data Protection Law (Lei Geral de Proteção de Dados Pessoais – LGPD). Likened to the European Union (EU)'s General Data Protection Regulation (GDPR), Brazil's LGPD offers strong protections but sets explicit exceptions for activities related to public safety, national defence, state security, and the investigation and prosecution of

---

72 Mello, D. (2021), 'Doria veta projeto para instalação de reconhecimento facial no Metrô' [Doria vetoes project for the deployment of facial recognition in the metro], Agência Brasil, 13 March 2021, https://agenciabrasil.ebc.com.br/politica/noticia/2021-03/doria-veta-projeto-para-instalacao-de-reconhecimento-facial-no-metro.
73 As identified in Access Now (2021), *Surveillance Tech in Latin America*, these include: at the state level, Bill No. 391/2019 (Minas Gerais); Bill No. 318/2019 (Rio de Janeiro); Bill No. 148/2019 (Paraná); and Bill No. 865/2019 (São Paulo). Another related legislative proposal is Bill No. 42/2020 (Ceará) which does not focus exclusively on facial recognition, but proposes to enable police to conduct video monitoring in public areas. At the federal level, there are additional proposals, including Bill No. 4.612/2019, Bill 5694/2019 and Bill No. 4.858/2020.
74 Agência Senado (2022), 'Brasil poderá ter marco regulatório para a inteligência artificial' [Brazil might have a regulatory framework for AI], 30 March 2022, https://www12.senado.leg.br/noticias/materias/2022/03/30/brasil-podera-ter-marco-regulatorio-para-a-inteligencia-artificial.
75 Convergência Digital (2022), 'Marco Legal de IA: Comissão admite banir o uso do reconhecimento facial' [AI Legal Framework: commission considers banning the use of facial recognition], 18 May 2022, https://www.convergenciadigital.com.br/Inovacao/Marco-Legal-de-IA%3A-Comissao-admite-banir-o-uso-do-reconhecimento-facial-60339.html.
76 Coding Rights (2022), 'Legislators from all regions of Brazil present bills to ban facial recognition in public spaces', 22 June 2022, https://medium.com/codingrights/legislators-from-all-regions-of-brazil-present-bills-to-ban-facial-recognition-in-public-spaces-31d8da0d3822.
77 Law 1/2005 – which regulates video surveillance by security forces in public spaces – also provides additional safeguards for individual privacy. The law establishes that the use of video surveillance must meet standards of proportionality, and should safeguard individuals' intimacy and private communications; and that security forces must demonstrate it is the most adequate means of protecting citizens. The lack of information on the use of facial recognition technology, and on its effectiveness, render independent proportionality assessments non-viable in spite of the clear risks that the technology poses on individuals' privacy. In spite of these robust safeguards, public security policies related to facial recognition do not appear to meet these established standards.

criminal offences.[78] This means that uses of facial recognition by public security forces, such as the deployment by the São Paulo civil police during the 2020 São Paulo Carnival, are beyond the protections of the LGPD.[79] An expert committee has put forward a bill proposal to regulate data protection in law enforcement, but it is uncertain whether this will come into force in the near future.[80] The research undertaken for this paper has been unable to identify any proof that human rights assessments were conducted in connection with this specific pilot.

Inadequate transparency and oversight

The use of facial recognition in both Buenos Aires and São Paulo has been marked by inadequate transparency and oversight.

Transparency in the use of facial recognition systems is crucial for the proper assessment of the effectiveness and proportionality of deployments. This entails making information available to the public in adequate measure: for example, this might include details about the technology providers and the key technology features, where the technology is deployed, how data is collected and kept secure, and whether any data is retained.

In both instances, such information as has been made available on the performance of facial recognition systems has come either from official statements to the press or from responses to freedom-of-information access requests submitted by civil society representatives. No verification mechanisms exist to corroborate performance data, and information rarely offers longitudinal data, preventing the continuous assessment of deployments over time.

In a response to a freedom-of-information access request presented by ADC in April 2019, the Buenos Aires city government reported that facial recognition deployments in the city had an effectiveness rate of 90 per cent in identifying missing criminals; no access was provided to databases to independently verify such a claim or help understand the methodology employed to arrive at such a result.[81] This reported performance is unusually high when compared, for example, to a deployment in 2018 in Cardiff, UK, where the police reported a 92 per cent 'false positive' rate.[82]

---

78 See Article 4, III of the Lei Geral de Proteção de Dados Pessoais (LGPD, General Personal Data Protection Law), available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
79 This is not the case when private companies are involved – such as in the repeated attempts to deploy facial recognition in São Paulo's privately-run public transport system – where the protections of the LGPD and the provisions of the Marco Civil da Internet [Civil Rights Framework for the Internet] and Consumer Protection Code apply. See Santana, A. (2019), 'Reconhecimento facial para coleta de dados para fins comerciais sem o consentimento pessoal. Ilegalidade', [Facial recognition to collect data for commercial purposes without consent: illegal], Jusbrasil, https://andreluizdarochasantana.jusbrasil.com.br/artigos/665452011/reconhecimento-facial-para-coleta-de-dados-para-fins-comerciais-sem-o-consentimento-pessoal-ilegalidade.
80 Chamber of Deputies of Brazil (2020), 'Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal' [Draft Bill Proposal: Data Protection Law for Public Safety and Criminal Prosecution], https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf.
81 Ucciferri, L. (2019), '#ConMiCaraNo: Reconocimiento facial en la Ciudad de Buenos Aires' [#NotWithMyFace: Facial Recognition in the City of Buenos Aires], ADC, 23 May 2019, https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires.
82 Note that the deployments in Buenos Aires and Wales are unlikely to have used the same methodology. Press Association (2018), 'Welsh police wrongly identify thousands as potential criminals', *Guardian*, 5 May 2018, https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals.

In the case of Brazil, access to performance indicators for surveillance technologies is also inconsistent, and relies on ad hoc public statements by authorities to the press.[83] During the live facial recognition pilot during the 2020 São Paulo Carnival, no statistical results were reported. In other areas of the country where data has been made available, false positive rates appear high. For instance, facial recognition techniques employed during the 2019 Salvador de Bahía Carnival identified 903 potential suspects but led to only 33 confirmed identifications and arrests.[84]

Oversight mechanisms, on the other hand, are crucial to ensure accountability and build safeguards. They allow for the monitoring of those in charge of deploying facial recognition technologies, so that abuses can be prevented and opportunities for contesting misidentification can be offered (and redress sought). They also provide a means of assessing the application of data protection standards, and of ensuring compliance with transparency requirements.

In Buenos Aires and São Paulo, government authorities have provided little information regarding the existence of oversight mechanisms. The City of Buenos Aires has reported having disciplinary procedures in place for individuals within the police force that make inappropriate use of the system. However, no oversight mechanism exists to monitor institutional abuses.[85] A wave of wrongful detentions triggered a review by the Buenos Aires Ombudsman in February 2022, though this has been an ad hoc assessment rather than a systematic review.[86] The judicial resolution that declared the system unconstitutional in September 2022 identified the failure by the Buenos Aires city government to set up an oversight body as one of the existing irregularities within the system.[87]

In the case of the São Paulo biometric identification laboratory, it is not clear whether any specific oversight mechanisms apply. While it is likely that the protocols of the regular security forces are enforced, the research conducted for this paper was unable to find whether these protocols are robust enough or are conducted by an independent body.

Reliance on police databases and reinforcement of structural discrimination

Live facial recognition techniques like those employed in Buenos Aires and São Paulo rely on police databases to identify potential suspects. Police regulation specialists Barry Friedman and Andrew Guthrie Ferguson have highlighted how 'mugshot' databases in the US are the product of decades of discriminatory

83 Canto, M. (2019), *We don't need no observation*.
84 Rede de Observatórios da Segurança/Centro de Estudos de Segurança e Cidadania (2019), *Retratos da Violência: Cinco meses de monitoramento, análises e descobertas* [Portraits of Violence: Five Months of Monitoring, Analysis and Findings], http://observatorioseguranca.com.br/wordpress/wp-content/uploads/2019/11/1relatoriorede.pdf.
85 Ucciferri (2019), '#ConMiCaraNo: Reconocimiento facial en la Ciudad de Buenos Aires' [#NotWithMyFace: Facial Recognition in the City of Buenos Aires].
86 Ombudsman of the City of Buenos Aires (2022), 'La Justicia Porteña Suspendió el Sistema de Vigilancia y Reconocimiento Facial' [The Buenos Aires judiciary suspends the surveillance and facial recognition system].
87 Rosende (2022), 'La justicia declaró inconstitucional el modo en que la Ciudad usa el sistema de reconocimiento facial' [The judiciary declared unconstitutional the way in which the Buenos Aires City uses the system of facial recognition].

policing; this also holds true for countries such as Argentina and Brazil, where police records similarly reflect the disproportionate criminalization of individuals based on race and income level.[88] Just as algorithmic bias can reinforce inequalities, police databases can further contribute to the replication of structural discrimination.

In the case of Buenos Aires, police forces employ the National Inquiry System on Default and Detention Orders (Consulta Nacional de Rebeldías y Capturas – CoNaRC) database. Following a visit to the country in 2019, the UN Human Rights Council's Special Rapporteur on the right to privacy expressed concern about the CoNaRC database which, despite being described as a list of 'most wanted' criminals, includes individuals who are sought for committing petty crimes. When used in tandem with facial recognition systems, this type of police database can reinforce the criminalization of minor offenders.[89]

The Special Rapporteur also highlighted that the CoNaRC database is plagued by errors. Some 29.5 per cent of the more than 46,000 entries do not specify the offence for which the person is wanted.[90] The wrongful detention of computer science professor Leo Colombo Viña in 2020, after his identification details were erroneously entered into the database, exposed the fact that the information listed could contain serious errors.[91] The UN report additionally highlighted that 61 children were listed on the database.[92] Human Rights Watch publicly criticized the Argentinian and Buenos Aires governments for failing to meet 'international obligations to respect children's privacy in criminal proceedings' and asserting that the national authorities should remove these records.[93] (The records in question have reportedly since been removed.)

Little concrete information is available about the composition of the criminal databases used in São Paulo. The live facial recognition pilot that was conducted during the 2020 Carnival compared facial images captured through live camera feeds against databases of wanted criminals and missing persons, with an estimated 30,000 and 10,000 entries each.[94] In the case of wanted criminals,

---

88 Friedman, B. and Guthrie Ferguson, A. (2019), 'Here's a Way Forward on Facial Recognition', *New York Times*, 31 October 2019, https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html.
89 There is a growing body of literature on criminalization of poverty and policing practices that reinforces racial inequalities, and how these manifest through the prosecution of petty offenders. See, for example, Campaign to Decriminalise Poverty & Status (https://pettyoffences.org/) and work by the Organization of American States' Inter-American Commission on Human Rights (2018), *Police Violence Against Afro-descendants in the United States*, OAS, https://www.oas.org/en/iachr/reports/pdfs/PoliceUseOfForceAfrosUSA.pdf. The US, in particular, has a developing body of literature on racial bias on police databases (see Angwin, J., Larson, J., Mattu, S. and Kirchner, L. (2016) 'Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks', *ProPublica*, 23 May 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing and Douglas Heaven, W. (2020), 'Predictive policing algorithms are racist. They need to be dismantled', MIT Technology Review, 17 July 2020, https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/). Further research, however, may be required to explore the impact of bias in police and government databases beyond the US, particularly as the use of AI-based technology becomes increasingly popular in the public sector across Latin America and the Global South.
90 United Nations General Assembly, Human Rights Council, *Visit to Argentina*, p. 12.
91 European Digital Rights (2020), 'Dangerous by design: A cautionary tale about facial recognition,' EDRi, 12 February 2020, https://edri.org/our-work/dangerous-by-design-a-cautionary-tale-about-facial-recognition.
92 Ibid.
93 Human Rights Watch (2020), 'Argentina: Child Suspects' Private Data Published Online', 9 October 2020, https://www.hrw.org/news/2020/10/09/argentina-child-suspects-private-data-published-online.
94 Simões Gomes, H. (2020), 'Pela 1ª vez, SP tem monitoramento facial em tempo real no Carnaval' [For the first time, São Paulo has real-time facial monitoring for Carnival], Tilt Uol, 19 February 2020, https://www.uol.com.br/tilt/noticias/redacao/2020/02/19/folia-vigiada-sp-tera-reconhecimento-facial-ao-vivo-no-carnaval-entenda.htm.

the database only contains details on suspects who have evaded justice starting from 2015, one year after criminal records began to be digitized. Both databases are reported to be maintained, secured and accessed only by the IIRGD.[95]

The criminal database, however, is likely to reflect discriminatory biases within Brazil's police system. A 2019 report by the country's Rede de Observatórios da Segurança (Network of Security Observatories) indicated that 90 per cent of arrests resulting from the use of facial recognition in the states of Bahia, Ceará, Rio de Janeiro, Paraíba and Santa Catarina involved black Brazilians.[96] This corresponds to the demographic composition of the Brazilian prison population, which is disproportionately black, suggesting that police databases in the country tend to reinforce forms of structural discrimination.

While no information is available about whether the police databases in Brazil include minors who have committed criminal offences, the commission in charge of drafting the proposed AI regulation bill (see above) has expressed concern as to how facial recognition may affect the rights of Brazilian children and has listed this as an important consideration in their deliberations about whether to ban the use of the technology for law enforcement purposes.[97]

Poorly defined standards in data use and retention

Facial recognition systems rely on the processing of large amounts of personal and sensitive data. In the deployments in Buenos Aires and São Paulo, there has been little transparency about what data use and retention practices apply, and whether these meet minimum standards.

The government of the City of Buenos Aires has only reported on its data processing practices following the 2019 submission by the ADC of a freedom-of-information access request (see above). According to the city government's response, the data generated by the facial recognition system is managed by police authorities and is subject to security, privacy and confidentiality protocols prohibiting data transfers to other administrative authorities in the city of Buenos Aires. Furthermore, the response stated that data is destroyed when judicial orders are withdrawn or lines of inquiry exhausted.[98] The mere inclusion of an individual's data on the CoNaRC database appears to be sufficient grounds to trigger searches aimed at locating wanted individuals – including those wanted for petty crime –

---

95 Ibid.
96 See Rede de Observatórios da Segurança/Centro de Estudos de Segurança e Cidadania (2019), *Retratos da Violência* [Portraits of Violence]; Barbon, J. (2019), '151 pessoas são presas por reconhecimento facial no país; 90% são negras' [151 people imprisoned by facial recognition in the country: 90% are black], *Folha de São Paulo*, 22 November 2019, https://www1.folha.uol.com.br/cotidiano/2019/11/151-pessoas-sao-presas-por-reconhecimento-facial-no-pais-90-sao-negras.shtml; and Sousa, B. (2021), 'Panóptico: reconhecimento facial renova velhas táticas racistas de encarceramento' [Panopticon: facial recognition renews old racist incarceration tactics], Rede de Observatórios de Segurança (2021), 22 April 2021, http://observatorioseguranca.com.br/panoptico-reconhecimento-facial-renova-velhas-taticas-racistas-de-encarceramento.
97 Convergência Digital (2022), 'Marco Legal de IA: Comissão admite banir o uso do reconhecimento facial' [AI Legal Framework: commission considers banning the use of facial recognition].
98 Ucciferri (2019), '#ConMiCaraNo: Reconocimiento facial en la Ciudad de Buenos Aires' [#NotWithMyFace: Facial Recognition in the City of Buenos Aires].

without requiring a specific court order. Lack of sufficient clarity about data use and retention render proper human rights assessments of the technology unviable.

In the case of São Paulo, authorities have provided little information about how personal and sensitive data is processed, retained and kept secure. As mentioned above, IIRGD's biometric identification laboratory reports that the databases are maintained, protected and accessed only by the IIRGD itself, although no specific procedural information has been made available.[99] If held to the standards laid down by the LGPD, the laboratory would be required to demonstrate that it has an adequate reason for processing data; prove that the data is kept secure; abide by transparency requirements; and respond to data access requests from the public. Authorities would also be required to ensure that data is not utilized for discriminatory purposes.

Lack of sufficient clarity about data use and retention render proper human rights assessments of the technology unviable.

Facial recognition systems require data collected through live footage to be cross-referenced with police watch lists. In the case of Buenos Aires, given that the CoNaRC database does not contain photographs, biometric information is pulled from the national population registry, RENAPER (Registro Nacional de las Personas), with which the ministry of justice and security of Buenos Aires has an agreement for running queries.[100] This process allows the CoNaRC database to be cross-referenced with the biometric data of wanted individuals.

Argentina is known to have one of the most intrusive data collection systems in Latin America.[101] The court ruling of April 2022 that suspended the use of facial recognition in Buenos Aires was based on the claim that the Buenos Aires city government abused its access to RENAPER, to search for individuals – including political figures, human rights activists and social leaders – whose data was not held in the criminal database.[102] On the other hand, the city government claims that the agreement with RENAPER authorizes other uses, beyond the comparison of live data from the facial recognition system.[103] However, the staggering number of searches run – reportedly nine million between April 2019 and

99 Simões Gomes (2020), 'Pela 1ª vez, SP tem monitoramento facial em tempo real no Carnaval' [For the first time, São Paulo has real-time facial monitoring for Carnival].
100 See details provided in the initial resolution through which the Buenos Aires city government introduced the facial recognition system: Government of the City of Buenos Aires (2019), 'Resolution N° 398/MJYSGC/19 – Annex', https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-RES-MJYSGC-MJYSGC-398-19-ANX.pdf.
101 Ucciferri, L. and Ferreyra, E. (2017), *Cuantificando identidades en América Latina* [Quantifying identities in Latin America], Buenos Aires: Asociación por los Derechos Civiles, https://adc.org.ar/wp-content/uploads/2019/06/029-cuantificando-identidades-en-america-latina-05-2017.pdf.
102 Bertoia (2022), 'Espionaje ilegal en CABA'.
103 At a public conference, the Argentinian minister of justice and human rights declared that the numerous system queries correspond to identity checks done by the city government so that it is able to provide a range of government services: these checks include seeking proof of address, and running queries related to COVID-19 tests and vaccines. See Martínez, L. (2022), 'Por qué se suspendió el sistema de reconocimiento facial de la Ciudad de Buenos Aires' [Why the facial recognition system of the city of Buenos Aires was suspended], Chequeado, 21 April 2022, https://chequeado.com/el-explicador/porque-se-suspendio-el-sistema-de-reconocimiento-facial-de-la-ciudad-de-buenos-aires.

March 2022[104] – speaks of the potential for abuse in the absence of clear policies for the use of this data.

Similar arrangements are reported to exist in relation to São Paulo's biometric identification laboratory, with security forces likewise having access to existing citizen databases for cross-referencing purposes. For example, beyond live facial recognition pilots, the laboratory regularly runs searches using static images of wanted persons. These static images are compared with a citizens' database which contains 32 million entries, with data derived from identity documents issued by the state of São Paulo.[105] The database includes biometric information on São Paulo residents, such as digital fingerprints and photographs.

Across Latin America, governments have a poor track record in preventing data breaches, which raises serious concerns about the ability of local governments to secure the sensitive data that is collected through facial recognition systems.[106] In 2019, hackers leaked 700 gigabytes (GB) of data they had obtained from Argentina's federal security forces and the Buenos Aires police; the leak included 'confidential documents, wiretaps and personal information of police officers themselves'.[107] More recently, in October 2021, the RENAPER database was hacked following a security breach at Argentina's federal ministry of health; the data was subsequently reported to be available for purchase online.[108] Brazil recorded its largest personal data leak in January 2021, when a massive database containing the records of 223 million Brazilians, including deceased individuals, was detected on the 'Dark Web'. The leak included personal data such as facial images, names, addresses and unique taxpayer identification codes, among other sensitive information.[109] Many other breaches have been reported: in 2016, the São Paulo city administration accidentally leaked the personal data of 365,000 patients, including some medical records, and in 2018, the tax identification numbers of some 120 million Brazilians were made available online due to a misconfigured server.[110]

---

104 Telam (2022), 'La Justicia detectó el uso irregular de datos biométricos en CABA y suspendió el sistema de vigilancia facial,' [The judiciary detected the irregular use of biometric data in the autonomous city of Buenos Aires and suspended the facial recognition system], 12 April 2022, https://www.telam.com.ar/notas/202204/589313-gobierno-ciudad-buenos-aires-denuncia-uso-reconocimiento-facial-datos.html.
105 Simões Gomes (2020), 'Pela 1ª vez, SP tem monitoramento facial em tempo real no Carnaval' [For the first time, São Paulo has real-time facial monitoring for Carnival].
106 Kemeny, R. (2020), 'Brazil is sliding into techno-authoritarianism', MIT Technology Review, 19 August 2020, https://www.technologyreview.com/2020/08/19/1007094/brazil-bolsonaro-data-privacy-cadastro-base.
107 Lostri, E. (2019), 'Hackers Leaked Sensitive Government Data in Argentina – and Nobody Cares', Lawfare blog, 21 August 2019, https://www.lawfareblog.com/hackers-leaked-sensitive-government-data-argentina%E2%80%94and-nobody-cares.
108 Cimpanu, C. (2021), 'Hacker steals government ID database for Argentina's entire population', The Record, 28 October 2021, https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population.
109 Belli, L. (2021), 'The largest personal data leakage in Brazilian history', Open Democracy, 3 February 2021, https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history.
110 See Kemeny (2020), 'Brazil is sliding into techno-authoritarianism' and Paganini, P. (2018), 'ID Numbers for 120 Million Brazilians taxpayers exposed online', Security Affairs, 18 December 2018, https://securityaffairs.co/wordpress/78874/data-breach/brazilian-taxpayers-data-leak.html.

04
A question of politics? Deployment in spite of the human rights risks

Cities across Latin America are deploying facial recognition despite potential human rights impacts. This suggests that rollouts are motivated by politics and unconcerned with legal implications.

Facial recognition technologies threaten an individual's right to privacy, and, as a result, their rights to freedom of expression and freedom of assembly and association. The technologies also undermine the right to non-discrimination and can disrupt judicial due process by challenging the principle of presumption of innocence. Despite these potential infringements on personal rights, a combination of political will and public acceptance, underpinned by an inadequate and peripheral public debate, have facilitated the deployment of facial recognition technologies in Argentina and Brazil, and may be driving adoption across other Latin American nations as well.

The political dimension behind facial recognition deployments tends to be lost when discussions are solely centred on a legal and human rights analysis. The adoption of facial recognition technologies, however, is proving to be just as much a question of politics as it is a question of law. In both Argentina and Brazil, for example, political considerations would appear to be driving the deployment of the technology.

A pragmatic approach to contain the potential harms of facial recognition technologies in Latin America calls for sincere conversations about the political drivers behind its adoption. Public safety concerns and apparent voter acceptance of heavy-handed security policies are playing an important role in driving adoption forward.

The public safety argument invoked by government officials in the deployment of facial recognition appears to have buy-in among the general public, and it is indeed a compelling argument. Latin America is described by regional analysts as having a 'chronic public security crisis', with crime and victimization rates on the rise.[111] While cities such as Buenos Aires and São Paulo boast low per head murder rates, public concerns around security tend to carry special weight across the continent's urban centres – which were home to some 81 per cent of the continent's population in 2021.[112] Security concerns are legitimate. Anti-crime policies have been an essential tool in containing both everyday criminality – emanating from the marked inequality observed across Latin American cities – and the more severe forms of violence and conflict that are associated with the presence of organized crime.[113]

Public perceptions around personal safety appear to play a significant role in encouraging governments to adopt heavy-handed security policies, such as the deployment of surveillance technologies. In deploying strict security policies, local politicians find a means to cater to voters' concerns around crime. The adoption of facial recognition has also played well alongside the push by many public officials to transform Latin American urban centres into 'smart cities', as state modernization makes for attractive political platforms. This was discernible, for example, in the 2019 mayoral election in Buenos Aires: the incumbent, Rodríguez Larreta, who was re-elected, promised during his campaign to expand the use of facial recognition technologies across the city's neighbourhoods.[114]

Security concerns feature prominently in opinion polls as a central matter of concern to voters. The Latin America Public Opinion Project (LAPOP) at Vanderbilt University reports that in 2017 nearly half of the region's population considered crime to be the most pressing problem.[115] This suggests that anti-crime policies are likely to be met with strong public support. In Argentina, for example, in spite of a marked political polarization, public security has been identified as one of the top four issues affecting the country by voters across the political spectrum.[116] In Brazil, not only was Bolsonaro's 2018 presidential campaign boosted by

---

111 Muggah, R. and Aguirre Tobón, K. (2018), *Citizen security in Latin America: Facts and Figures*, Igarapé Institute, Strategic Paper 33, https://igarape.org.br/wp-content/uploads/2018/04/Citizen-Security-in-Latin-America-Facts-and-Figures.pdf.
112 World Bank (2022), 'Urban population (% of total population) – Latin America & Caribbean', https://data.worldbank.org/indicator/SP.URB.TOTL.IN.ZS?locations=ZJ (accessed 15 Aug. 2022).
113 Melgaço, L. and Arteaga Botello, N. (2015), 'Introduction: the securitization of Latin American cities', *Revista Brasileira de Gestão Urbana*, 7, pp. 149–53, https://doi.org/10.1590/2175-3369.007.002.IT01.
114 Página 12 (2019), 'Cámaras de reconocimiento facial: Larreta prometió 10.000 más' [Facial recognition cameras: Larreta promised an additional 10,000], 4 October 2019, https://www.pagina12.com.ar/223372-camaras-de-reconocimiento-facial-larreta-prometio-10-000-mas.
115 Cafferata, F. G. and Scartascini, C. (2021), 'Combating Crime in Latin America and the Caribbean: What Public Policies Do Citizens Want?', Washington, DC: Interamerican Development Bank, https://publications.iadb.org/publications/english/document/Combating-Crime-in-Latin-America-and-the-Caribbean-What-Public-Policies-Do-Citizens-Want.pdf.
116 Observatorio de Psicología Aplicada (2020), 'Monitor de Inseguridad No. 2 – Diciembre 2020' [Insecurity Monitor No. 2, December 2020].

the candidate's promises to crack down on insecurity (see above), but Bruno Covas also committed to increase the use of surveillance technologies during his successful 2020 campaign to be re-elected as mayor of São Paulo, with the use of drones and the incorporation of 4,240 new cameras across the city for urban monitoring.[117]

Concerns around crime are known to have shifted the 'Overton window' in Latin America – that is, the range of policies that the public is willing to accept, even if they infringe the rights of individuals.[118] Starting in the 1980s, the region went through a process of securitization by which the state was empowered 'to legitimately resort to extraordinary means to guarantee the security of its citizens'.[119] In the early 2000s, several Latin American governments attempted to promote a paradigm shift in anti-crime policies, seeking to place human rights and democracy at the heart of new policy development, and addressing social inequalities to bolster public safety. This shift, however, failed to take hold in the region, and several national security policies still fall short in terms of complying with human rights.[120] On the contrary, Latin America's widened Overton window seems to support the steady incorporation of surveillance technologies such as facial recognition.

Concerns around crime are known to have shifted the 'Overton window' in Latin America – that is, the range of policies that the public is willing to accept, even if they infringe the rights of individuals.

Assessing public perceptions around the use of facial recognition in Argentina and Brazil remains challenging, as there have been no specific polls on the subject in either country. Other than actions initiated by local and international civil society organizations, the lack of mobilization or social protest around the adoption of this technology speaks of the apathy with which the deployments have been met.[121] This inaction suggests a degree of acceptance – or at the very least, ambivalence – about the use of facial recognition technologies. Apathy is likely to be a reflection of the 'nothing to hide' mentality, a public position documented by various human rights groups in which individuals are willing to tolerate infringements on privacy guided by the belief that they personally

---

117 Faustine, L. (2020), 'Drones, mais guardas, olhar para as minorias: os planos para segurança de Covas e Boulos' [Drones, more guards, looking out for minorities: plans for security in Covas and Boulos], Ponte, 28 November 2020, https://ponte.org/drones-mais-guardas-olhar-para-as-minorias-os-planos-para-seguranca-de-covas-e-boulos.
118 Kind (2020), 'Nowhere to hide'.
119 Lopez, D. (2017), 'Securitisation and its impact on human rights in Latin America', *Global Campus Human Rights Journal*, 1(2), pp. 463–78, https://repository.gchumanrights.org/server/api/core/bitstreams/bad7c417-bc6b-4b43-a6f1-be6bf8165b5a/content.
120 Chinchilla M., L. and Vorndran, D. (2018), *Citizen Security in Latin America and the Caribbean: Challenges and Innovation in Management and Public Policies over the Last 10 Years*, Interamerican Development Bank, https://publications.iadb.org/en/citizen-security-latin-america-and-caribbean-challenges-and-innovation-management-and-public.
121 For example, in the case of Buenos Aires, it was civil society organizations that contested the legalization of the system. See Access Now et al. (2020), 'La Legislatura porteña debe rechazar el uso de la tecnología de reconocimiento facial para la vigilancia del espacio público' [The Buenos Aires legislature must reject the use of facial recognition for surveillance in the public space], joint communiqué, available at: https://amnistia.org.ar/wp-content/uploads/delightful-downloads/2020/10/Comunicado-conjunto-reconocimiento-facial.pdf.

will not be subject to wrongful suspicion.[122] While human rights activists have provided strong arguments about why the 'nothing to hide' argument is flawed, it still features prominently in public debates about privacy infringements.

However, the debate is more nuanced. Public opinion on the adoption of technologies such as facial recognition is influenced not only by perceptions around security, but also by citizens' perceptions around privacy itself. High-profile surveillance cases have had an impact in swaying public opinion against practices that violate the right to privacy. For example, following the disclosures made in 2013 by the US intelligence consultant Edward Snowden, who revealed that the US National Security Agency had placed Brazilian President Dilma Rousseff and millions of the country's citizens under surveillance,[123] an opinion poll conducted by Amnesty International documented a strong opposition to surveillance practices in Brazil. The survey also found that there was a higher tolerance towards surveillance practices when the latter were targeted by the host country at foreign nationals, indicating a higher acceptance of surveillance when related to national security concerns.[124] Specialists on Brazilian politics point out that while there may be public support for strict security policies, as shown by Bolsonaro's ascent to power in 2019 and the importance assigned to public safety debate during the 2022 election cycle, there is a strong public expectation that human rights be respected in the implementation of such policies.[125] This is indicative of public opinion being both aware of, and reactive to, the trade-offs between privacy and safety.

The key to public acceptance in Latin America appears to hinge on whether technologies such as facial recognition – and related privacy infringements – are perceived to generate benefits for the public and are therefore deemed both necessary and proportionate. A national survey on the use of facial recognition technologies conducted in 2019 by the UK-based Ada Lovelace Institute found that the majority of the UK population (55 per cent) would support government restrictions on the police using facial recognition technology, but nearly half (49 per cent) was prepared to accept it if associated with a clear public benefit, assuming appropriate safeguards were in place.[126]

To develop this level of critical thinking, it is important for countries to engage in a public debate about the use of these technologies, as well as the purported benefits and potential harms which they generate. These conversations require deep consideration about how to craft deployments in a manner that is consistent with human rights standards, striking a balance between the potential benefits

---

122 Coustick, R. (2015), 'Responding to "nothing to hide, nothing to fear"', Open Rights Group, 4 December 2015, https://www.openrightsgroup.org/blog/responding-to-nothing-to-hide-nothing-to-fear.
123 Owen, P. and Watts, J. (2013), 'Edward Snowden offers to help Brazil over US spying in return for asylum', *Guardian*, 17 December 2013, https://www.theguardian.com/world/2013/dec/17/edward-snowden-brazil-spying-asylum.
124 See Amnesty International (2015), 'Global opposition to USA big brother mass surveillance', 18 March 2015, https://www.amnesty.org/en/latest/news/2015/03/global-opposition-to-usa-big-brother-mass-surveillance; and Chambers, C. (2015), 'The psychology of mass government surveillance: How do the public respond and is it changing our behaviour?' *Guardian*, 18 March 2015, https://www.theguardian.com/science/head-quarters/2015/mar/18/the-psychology-of-mass-government-surveillance-how-do-the-public-respond-and-is-it-changing-our-behaviour.
125 As documented in the author's private exchange with Latin American specialist Elena Lazarou.
126 Ada Lovelace Institute (2019), *Beyond face value: public attitudes to facial recognition technology*, Report, London: Ada Lovelace Institute, https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology.

for public security and against crime, and the impacts on individual and collective rights. For example, this could entail rolling out facial recognition programmes that minimize data collection on individuals or that guarantee that, whenever data is legitimately collected, it is properly handled to reduce its impact on individual rights.

Public dialogue needs to involve relevant stakeholders, such as policymakers, security forces, legal experts, civil society and academics, but, above all, the general public and those who may be affected by pilots or ongoing developments. In countries where technologies are already in use, transparency and access to information are essential to enable an evidence-based public debate on the effectiveness of public security practices and their impacts on human rights.

Box 2. Argentina and Brazil: the depth of the public debate on facial recognition

Public debate on the adoption of facial recognition technologies has been limited in the case of Argentina, whereas in Brazil it has received greater attention at the National Congress and state courts.

In Buenos Aires, public dialogue on facial recognition peaked when the city legislature debated the amendment to the security regulation that legalized the use of the technology. Beyond the capital city's legislature, no debate has ensued at the level of provincial legislatures or the National Congress to frame the use of facial recognition as a problem to be solved.

Civil society organizations have pointed out that the government of the City of Buenos Aires tends to favour the implementation of surveillance technologies without proper assessments or adequate forms of public debate that engages average citizens potentially affected by their deployment.[127] Local NGOs also report an inadequate understanding among security forces of the potential human rights impacts of some of the measures adopted.

Brazil, on the other hand, has hosted a more sophisticated debate. The country has seen the emergence of multiple regulatory efforts at state and federal levels. The adoption of facial recognition throughout the country triggered two public audiences in 2019, organized by the National Congress and the federal public ministry, the national agency tasked with protecting the public interest.[128] Analysts from the Igarapé Institute think-tank indicate that a general consensus emerged in these public audiences around the need for a balanced regulation to govern the use of facial recognition technologies in a way that upholds fundamental rights such as privacy

127 Asociación por los Derechos Civiles (2019), 'El reconocimiento facial para vigilancia no pertenece a nuestro espacio público' [Facial recognition for surveillance does not belong in our public space].
128 See Chamber of Deputies of Brazil (2019), 'A questão das tecnologias de reconhecimento facial para aplicação em segurança pública no Brasil' [The issue of applying facial recognition technologies to public safety in Brazil], Audiências interativas [Interactive audiences], 3 April 2019, https://edemocracia.camara.leg.br/audiencias/sala/840; and Public Ministry of Federal Districts and Territories (MPDFT) (2019), 'MPDFT: Audiência pública debate uso de ferramentas de reconhecimento facial' [MPDFT: Public audience debates use of facial recognition tools], 16 April 2019, https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10779-mpdft-audiencia-publica-debate-uso-ferramentas-de-reconhecimento-facial.

and access to information.[129] Most recently, the federal senate's efforts to produce a draft bill to regulate AI has triggered a new round of public consultations, inspired by collaborative regulatory design efforts that shaped Brazil's GDPR equivalent, the LGPD. Once the consultation is finalized, the commission of legal experts is expected to present a draft proposal to the Brazilian Senate before the end of 2022.

In April 2022, Argentina saw the conversation on the use of facial recognition systems resurface with the first active involvement of a city-level court that temporarily suspended the technology's use in the city of Buenos Aires, and the subsequent resolution from September 2022 that found unconstitutional the way in which the current system is deployed. The debate has been tainted by political tensions, with the Buenos Aires city government officials claiming that the judicial intervention is politically motivated.

Brazil's judiciary, on the contrary, has been very responsive in analysing controversial facial recognition deployments. The case against ViaQuatro, a private firm operating segments of the São Paulo Metro, was widely discussed in Brazil. ViaQuatro placed an advertisement in front of passengers exiting the Metro, using emotion detection techniques. Following a class action suit coordinated by the Instituto Brasileiro de Defesa do Consumidor (Brazilian Consumer Protection Institute), a local court fined ViaQuatro and ruled that the system it had used was illegal, as the deployment collected passengers' biometric data without their consent.[130] The ruling also highlighted the potential discriminatory impact of the technology.[131]

In both countries, while civil society has been widely active in monitoring deployments and denouncing the potential rights impacts of facial recognition deployments, further public involvement is still needed to engage broader audiences in the conversation about the potential societal impacts of the technology.

129 Francisco, P., Hurel, L. M. and Marques Riell, M. (2020), *Regulação do Reconhecimento Facial No Setor Público: avaliação de experiências internacionais* [Regulation of facial recognition in the public sector: evaluation of international experiences], Igarapé Institute and Data Privacy BR, https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf.
130 See Soprana, P. and Amâncio, T. (2021), 'ViaQuatro é condenada por reconhecimento facial sem autorização no Metrô de SP' [ViaQuatro is convicted of unauthorized facial recognition in the São Paulo Metro], *Folha de São Paulo*, 11 March 2021, https://www1.folha.uol.com.br/cotidiano/2021/05/viaquatro-e-condenada-por-reconhecimento-facil-sem-autorizacao-no-metro-de-sp.shtml; Becker, S., Lara, J. C. and Canales, M. P. (2018), *La construcción de estándares legales para la vigilancia en América Latina – Parte I: Algunos ejemplos de regulación actual en América Latina* [Building legal standards for surveillance in Latin America – Part I: Some examples of current regulation in Latin America], Derechos Digitales and Global Partners Digital, https://www.derechosdigitales.org/wp-content/uploads/construccion-estandares-legales-vigilancia-I.pdf.
131 Ibid.

05
The way forward: insights from other jurisdictions

The ways in which other major jurisdictions approach facial recognition deployments offers valuable insights for policymakers in Latin America.

Facial recognition deployments in Buenos Aires and São Paulo are mirrored in other countries across Latin America. Similar technology has been brought into use in Colombia, Mexico and Paraguay. The region appears to be 'stuck' in a worst-case scenario, where facial recognition is being used by security forces in public spaces despite potential human rights infringements, and with inadequate safeguards to contain potential abuses or provide avenues for redress.

With these deployments already in place, the use of the technology for law enforcement purposes has been normalized and even legitimized.

Where does Latin America go from here? While the region has unique characteristics that call for local solutions, an examination of evolving regulatory responses in jurisdictions such as the US, EU and UK – all of which are also exploring how to deploy AI and biometric technologies in a manner that is respectful of fundamental rights – provides some pointers as to how Latin America may move away from this scenario.

Facial recognition in the US

The US offers an interesting opportunity to study the regulation of facial recognition technologies, since the country – like Argentina and Brazil – is organized as a federal system where national, state or provincial and city-level authorities and legislation coexist.

US regulatory approaches to police use of facial recognition made international headlines when a number of cities began to ban the technology. The first city to take such action, in May 2019, was San Francisco, at the heart of the Silicon Valley technology hub. Somerville, Massachusetts, and Oakland, California, quickly followed suit, giving rise to a 'domino effect' which led to ordinances banning facial recognition being passed in another dozen US cities in the period to October 2020.[132] At federal level, law enforcement agencies are known to make extensive use of the technology for national security purposes.[133] However, except for a bill proposal in mid-2021 to ban the federal government from using facial recognition,[134] national authorities in the US had steered clear of actively regulating facial recognition and biometric technologies.

State governments, on the other hand, have been left to self-regulate. In Massachusetts, policymakers at city and state levels are dealing with simultaneous efforts to regulate the technology. In June 2020, following an exhaustive campaign by local civil rights and community leaders, the city of Boston pronounced itself against the use of facial recognition by city police. The American Civil Liberties Union of Massachusetts, which participated in the pro-ban campaign, maintained that facial recognition is a risky technology that should not be regulated at city level.

In June 2020, following an exhaustive campaign by local civil rights and community leaders, the city of Boston pronounced itself against the use of facial recognition by city police.

Regulation was indeed taken up at the state level through the Police Reform Bill which, among other aspects, touched upon police use of facial recognition technologies. The bill originally sought to ban the use of biometric surveillance systems by Massachusetts state government agencies, but was vetoed by the state executive, which claimed that the technology was needed for criminal investigations. A renegotiated version of the bill was approved in December 2020, establishing that police may resort to facial recognition when in possession of a court order, or, in emergencies only, without a judicial warrant. In addition, the legislation established transparency requirements and created a commission to assess whether more stringent regulation might become necessary in the future.[135] By contrast, Maine – the state with the strictest statewide regulation

---

132 Feathers, T. (2021), 'Facial Recognition Is Racist. Why Aren't More Cities Banning It?', Vice Motherboard, 25 May 2021, https://www.vice.com/en/article/4avx3m/facial-recognition-is-racist-why-arent-more-cities-banning-it.
133 Brandom, R. (2021), 'Most US government agencies are using facial recognition', The Verge, 25 August 2021, https://www.theverge.com/2021/8/25/22641216/facial-recognition-gao-report-agency-dhs-cbp-fbi.
134 Ed Markey, United States Senator for Massachusetts (website) (2021), 'Senators Markey, Merkley Lead Colleagues on Legislation to Ban Government Use of Facial Recognition, other Biometric Technology', press release, 15 June 2021, https://www.markey.senate.gov/news/press-releases/senators-markey-merkley-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology.
135 See The 192nd General Court of the Commonwealth of Massachusetts (2020), 'Bill S.2963: An Act relative to justice, equity and accountability in law enforcement in the Commonwealth', available at: https://malegislature.gov/Bills/191/S2963/BillHistory?pageNumber=2 and American Civil Liberties Union of Massachusetts (2020), 'Massachusetts Passes Police Reform', 31 December 2020, https://www.aclum.org/en/news/massachusetts-passes-police-reform.

of facial recognition – requires government agencies to have 'probable cause'.[136] This means that facial recognition may be used in criminal investigations, but only when law enforcement has sufficient grounds to believe that a particular person has committed a crime.

In October 2022, the Biden administration – through the White House's Office of Science and Technology Policy – introduced its Blueprint for an AI Bill of Rights, which offers more straightforward, though non-binding, guidelines for the use of automated technologies. The blueprint includes a series of principles to protect civil rights, including privacy, in the deployment of AI-based systems.[137] For example, the application of these guidelines to police use of facial recognition would require the enactment of protections against algorithmic discrimination.

Facial recognition in the EU

The European Union has set out to regulate the use of facial recognition technology through its proposed Artificial Intelligence Act, which is currently going through the final stages of the EU's legislative process. Within this framework, real-time biometric identification is classified as a high-risk application of AI and must therefore comply with certain mandatory requirements if it is to be put into service. More specifically, real-time biometric identification systems deployed in publicly accessible spaces for law enforcement purposes are prohibited, unless used for specific exceptions connected to public safety such as the search for missing persons and the localization of criminals and suspects.[138] Similar to the regulation put in place by the US state of Massachusetts (see above), law enforcement would need to secure authorization to use the technology from either a judicial or an independent administrative authority designated by a member state, unless dealing with emergencies or life-threatening circumstances such as terrorist attacks. Member states would retain the discretion to draw up national laws that extend or limit law enforcement uses of the technology.

Precisely how facial recognition is to be regulated across the EU is, however, far from settled. Both the European Data Protection Board and the European Data Protection Supervisor, Europe's privacy 'watchdogs', believe that these

---

136 American Civil Liberties Union (2021) 'Maine enacts strongest statewide facial recognition regulation in the country', 30 June 2021, https://www.aclu.org/press-releases/maine-enacts-strongest-statewide-facial-recognition-regulations-country.

137 The White House (2022), 'Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People', Office of Science and Technology Policy, 5 October 2022, https://www.whitehouse.gov/ostp/ai-bill-of-rights.

138 See Louradour, S. (2021), 'What to know about the EU's facial recognition regulation – and how to comply', Word Economic Forum, 22 April 2021, https://www.weforum.org/agenda/2021/04/facial-recognition-regulation-eu-european-union-ec-ai-artificial-intelligence-machine-learning-risk-management-compliance-technology-providers. As per the partial compromise text published by the Presidency of the Council of the European Union on 29 November 2021, 'real-time' remote biometric identification systems could also be used by other actors, acting on behalf of law enforcement authorities, and the list of objectives for which law enforcement is allowed to use such systems is expanded to include, for example, attacks on critical infrastructure, or acting on behalf of the health of natural persons. See Council of the European Union (2021), *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Presidency compromise text*, Note from the Presidency to Delegations, 29 November 2021, https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf.

exceptions are too broad and could still lead to mass surveillance.[139] Civil society organizations across Europe have welcomed this criticism, which is likely to prove a central point of contention in upcoming debates over this new component of the EU regulatory framework (one that, like the GDPR, is expected to generate a worldwide 'ripple effect').

Among the provisions of the AI Act is the adoption of a risks-assessment approach to better gauge the implications of specific AI deployments. This entails targeting applications of AI that pose greater threats to the public good, and lowering the burden for less risky applications of the technology.[140] This approach offers a valuable proposition and an interesting model for Latin American countries to consider, as they design their national AI strategies: identifying which AI applications are particularly risky, and enabling national debates about those which pose significant challenges to fundamental rights. These conversations will be important to foster innovation and provide predictability for entrepreneurs and investors in the AI sector. Whether they are operating in the EU or Latin America, regulators must consider state capacities to enforce safeguards and potential political intent to abuse exceptions.

Facial recognition in the UK

The extensive use of CCTV by the UK's law enforcement agencies is well documented, as are those agencies' exploratory deployments of facial recognition. London's Metropolitan Police and the South Wales Police have made the most extensive use of the technology, although Big Brother Watch, a civil liberties campaign group, was reporting in August 2022 that pilot projects and deployments were confirmed or believed to have taken place in at least another eight UK cities.[141] The Metropolitan Police has run facial recognition trials in the UK capital since 2016, with two live pilots having taken place as recently as January and July 2022.[142] Londoners are not unaccustomed to the use of technology for monitoring streets, with their city having the most extensive CCTV network of any, outside China.[143] This prolific use of networked CCTV in London has prompted the development of robust legislation to regulate video surveillance that seeks to minimize its potential impact on individual rights and liberties. The South Wales Police, on the other hand, is the national lead on testing automated facial

139 See Meyer, D. (2021), 'Europe's privacy regulators call for a ban on facial recognition in publicly accessible spaces', *Fortune*, 21 June 2021, https://fortune.com/2021/06/21/ban-facial-recognition-in-all-publicly-accessible-spaces-europe-privacy-regulators-urge-edps-edpb-ai-regulation/; Burt, C. (2021), 'Public surveillance biometrics in Europe could be crushed between the EDPS and AI Act', BiometricUpdate.com, 16 November 2021, https://www.biometricupdate.com/202111/public-surveillance-biometrics-in-europe-could-be-crushed-between-the-edps-and-ai-act.
140 Louradour (2021), 'What to know about the EU's facial recognition regulation – and how to comply'.
141 According to Big Brother Watch, cities and counties where facial recognition surveillance is currently in use in the UK include Birmingham, Bradford, Brighton, Cardiff, Hull, Leicestershire, Liverpool, London, Manchester and Sheffield. See Big Brother Watch (2022), 'Facial Recognition Map', https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition (accessed 15 Aug. 2022).
142 Klovig Skelton, S. (2022), 'Met police deploy facial-recognition technology in Oxford Circus', ComputerWeekly.com, 13 July 2022, https://www.computerweekly.com/news/252522694/Met-police-deploy-facial-recognition-technology-in-Oxford-Circus.
143 Carlo, S. (2019), 'Britain Has More Surveillance Cameras Per Person Than Any Country Except China. That's a Massive Risk to Our Free Society', *Time*, 17 May 2019, https://time.com/5590343/uk-facial-recognition-cameras-china.

recognition.[144] It is reported to have run 50 facial recognition trials between 2017 and 2019 at mass events, including concerts and sports matches.[145]

The use of facial recognition technologies in the UK is currently governed by a complex regulatory framework: supervision of existing deployments falls under the purview of a range of government entities commissioned with overseeing video surveillance and biometric technology systems.[146]

Beyond existing regulation, the weight of case law has also been very important in shaping the use of facial recognition. *Edward Bridges vs South Wales Police (2018–20)* has been a seminal case. Following a legal complaint by a resident of Cardiff, who challenged the legality of having his face analysed by the South Wales Police after his image was captured by facial recognition systems during a trial of the technology, the Cardiff Court of Appeal found irregularities with the way the facial recognition was implemented.[147] This included a lack of clarity about the rules that determined whether the police could use facial recognition, and how the police force had compiled the watch list of individuals to monitor. The court ruling also found that the police had not thoroughly studied the potential discriminatory impact of the technology.[148] The South Wales Police had won the case at first instance, before losing in the Court of Appeal, indicating that the breach of rights was not self-evident.[149]

This UK ruling does not render all uses of facial recognition technologies unlawful, but it highlights the importance of crafting detailed guidelines with robust standards in relation to potential interferences with the right to privacy.[150] Since the ruling was made, the South Wales Police has resumed facial recognition trials, making a concerted effort to ensure the deployments are legitimate and proportionate, and avoid breaching equality requirements through bias or discrimination.[151] This measured approach indicates that police forces

---

144 See South Wales Police's use of automated facial recognition technology: UK Courts and Tribunal Judiciary (2020), 'Judgment R (Bridges) -v- CC South Wales', paragraph 10.
145 See South Wales Police's use of automated facial recognition technology: UK Courts and Tribunal Judiciary (2020), 'Judgment R (Bridges) -v- CC South Wales', paragraph 11.
146 According to a parliamentary report on the work of the Biometrics Commissioner, there is a comprehensive legal framework for the management of facial recognition which includes 'police common law powers to prevent and detect crime, the Data Protection Act 2018 (DPA), the Human Rights Act 1998, the Equality Act 2010, the Police and Criminal Evidence Act 1984 (PACE), the Protection of Freedoms Act 2012 (POFA), and police forces' own published policies'. In terms of oversight, the report explains that: 'the Information Commissioner's Office (ICO) regulates compliance with the DPA, including police use and retention of biometrics and POFA created the Surveillance Camera Commissioner and Biometrics Commissioner roles, and the Forensic Information Databases Service strategy board'. Lastly, the College of Policing's Authorised Professional Practice (APP) offers guidelines for 'the retention, review and deletion of custody images' by the police. See UK Parliament (2021), 'Work of the Biometrics Commissioner and the Forensic Science Regulator: Government Response to the Committee's Nineteenth Report of Session 2017–19', https://publications.parliament.uk/pa/cm5801/cmselect/cmsctech/1319/131902.htm.
147 The appellant, Edward Bridges, was supported and represented by Liberty, a civil rights group.
148 See UK Courts and Tribunal Judiciary (2020), 'Judgment R (Bridges) -v- CC South Wales' and UK Courts and Tribunal Judiciary (2020), 'Judgment R (Bridges) -v- CC South Wales Press Summary', 11 August 2020, https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Press-Summary-1.pdf.
149 For judgment won at first instance, see High Court of Justice, Queen's Bench Division, Divisional Court sitting at Cardiff Civil Justice Centre (2019), 'Judgement R (Bridges) v Chief Constable of the South Wales Police,' EWHC 2341 (Admin) available at: https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf.
150 Stokel-Walker, C. (2020), 'Is police use of face recognition now illegal in the UK?', *New Scientist*, 11 August 2020, https://www.newscientist.com/article/2251508-is-police-use-of-face-recognition-now-illegal-in-the-uk/#ixzz76Ro2woHe.
151 South Wales Police (2022), 'Keeping South Wales safe with facial recognition technology', 14 March 2022, https://www.south-wales.police.uk/news/south-wales/news/2022/maw-mar/keeping-south-wales-safe-with-facial-recognition-technology.

across the UK are incorporating the lessons learned from the Bridges case. The College of Policing for England and Wales has also issued guidelines for police authorities to use live facial recognition in a manner that is ethical and respectful of human rights.[152]

While debates on how to regulate facial recognition are still not fully settled in any of these three jurisdictions, regulation in the US and EU appears to be moving towards the authorized use of the technology in public spaces only under specific circumstances related to public safety. Civil society and watchdog organizations continue to challenge whether these limitations are sufficiently robust to prevent mass surveillance. They have persisted in calling for comprehensive bans, while continuing to expose the potentially discriminatory biases of the technology. In the UK, in addition to civil society, the judiciary has contributed to the debate and raised the bar by calling for more robust privacy protections which have encouraged the incorporation of additional human rights safeguards and oversight mechanisms.

The case of the US provides relevant lessons for Latin American countries which have federal systems of government and where city-level legislation has served to enact more stringent rules in the use of the technology than those offered by state or national legislation. In the few US states that have regulated facial recognition, legislation has provided macro-level frameworks that contemplate exceptions and outline the various levels of authorization required to use the technology. In the US, where federal legislation tends to be less prescriptive, regulation is likely to be shaped at the state level whereas in Latin American countries, regulatory frameworks are more likely to be developed by policymakers at the national level. In either case, city-level regulation should not provide lesser protections than those upheld by state and national regulation.

Lastly, the EU's AI Act offers a potential model for Latin American countries to follow in terms of integrating facial recognition regulation within their AI strategies to develop coherent, overarching frameworks. Indeed, the risk-assessment approach adopted by the EU may serve as a valuable methodology to countries beyond Europe, enabling them to identify AI applications that challenge fundamental rights and either limit or ban their deployment.

152 College of Policing (2022), 'Live facial recognition'.

06
To ban or to regulate facial recognition in Latin America? The debate

If robust policies are to be developed for the use of facial recognition technology across Latin America, concerns around human rights must be addressed and safeguards built against potential abuses.

While there is widespread agreement on the shortfalls and perils that the use of facial recognition poses, there are two distinctive positions on how the technology should be handled.

First, there are those who side with authorizing the use of the technology in public places for law enforcement purposes, provided that strong safeguards are in place. At state level in the US, and in the debate around the forthcoming AI Act in the EU, policymakers have worked to legislate based on the notion that facial recognition is a valuable tool when used to protect public security, and, as such, have sought to regulate the technology by allowing its exceptional use in public places, requiring judicial or third-party authorization except in cases of specific emergencies. For Latin America, where the technology is already deployed, such an approach could

be set in motion through the establishment of moratoriums that allowed the use of the technology to be paused until proper safeguards are put in place.

On the other side of the debate, privacy and data protection watchdogs and civil society organizations maintain that facial recognition is inherently at odds with fundamental rights such as privacy, and that its use for law enforcement in publicly accessible spaces is unacceptable in democratic societies. This view has been epitomized by the city-level bans rolled out across the US. It echoes the stance taken in Latin America by human rights groups and digital rights activists, who are calling for outright bans throughout the region.[153]

In Latin America, where the technology is largely deployed without proper safeguards, both policymakers and human rights advocates must ask themselves what the most realistic routes might be to move beyond the current worst-case scenario. As regulation in Western jurisdictions appears to be headed towards exceptional, authorized use with strict safeguards on that use, placing a moratorium on the technology while those precautions are put in place seems a feasible alternative for Latin America. However, this is not a bullet-proof approach, and may not be easily applicable to non-consolidated democracies and nations with governments tending to authoritarianism.

Indeed, proponents of facial recognition bans in Latin America have strong and valid arguments about why the region may be unprepared for 'middle-of-the-road' solutions. First, they highlight that state institutions have often performed poorly when enforcing safeguards around surveillance practices. Brazil is one such example: its wiretapping law (Law No. 9,296, enacted in 1996) has been lauded for meeting international standards and safeguards. Yet, far from being an instrument for exceptional use, security forces are regularly and easily granted wiretap permits, as evidenced by the authorization of an extraordinary 21,925 phone tapping cases during protests against Brazil's staging of the football World Cup in 2014.[154] Enforcement capacity may also be challenging for smaller Latin American states, where institutions are relatively fragile and may not have the resources or political leverage to properly monitor the adequate deployment of facial recognition technologies.

Another point of concern among supporters of a comprehensive ban is the potential amplification effect, inherent to facial recognition technologies, of algorithmic and data bias, which is likely to exacerbate existing inequalities and reinforce structural discrimination. Pro-ban activists suggest that marked racial, gender and income inequalities across the Latin American region would render the deployment of facial recognition particularly risky for vulnerable populations. For example, some of the limited data available in Brazil indicates that people of colour are disproportionately targeted, as compared to white Brazilians.[155] While available data on the Buenos Aires deployment is not disaggregated by race,

---

153 See, for example, ReconocimientoFacial.info by Derechos Digitales (in coalition with 12 civil society organizations), ReconocimientoFacial.info (undated), 'El reconocimiento facial no nos protege, nos vulnera' [Facial recognition does not protect us, it violates us], https://reconocimientofacial.info and ADC's #NotWithMyFace campaign: Asociación por los Derechos Civiles (2022), 'Con mi cara no' [Not with my face].
154 Privacy International (2019), 'State of Privacy Brazil', https://privacyinternational.org/state-privacy/42/state-privacy-brazil#:~:text=Interception%20of%20communications%20in%20Brazil,instructing%20criminal%20procedures%20or%20investigations.
155 Rede de Observatórios da Segurança (2019), *Retratos da Violência* [Portraits of Violence].

gender or income level, the use of facial recognition to tackle petty crime clearly sets out to criminalize vulnerable populations in Argentina, where poverty rates stood at 40 per cent in 2021.[156]

Pro-ban groups also point to the history of military dictatorships in Argentina, Brazil and other Latin American countries. These regimes share a regrettable track record of incarcerating political dissidents and engaging in political assassinations and kidnappings –a sobering reminder that civil society must stand for the protection of open public spaces that are free of surveillance. The human rights abuses experienced under military rule are a fresh example of how the potential misuse of facial recognition for state surveillance can incur significant human and political costs. While Latin America has not yet seen major attempts to abuse the technology, China's alleged use of facial recognition to track Uighur populations in the Xinjiang region is a worrying example of such misuse.[157]

The value of moratoriums has also been questioned by civil society actors. Representatives from European Digital Rights (EDRi), an association of European civil and human rights organizations, claim that waiting for facial recognition systems to improve performance and tackle bias will still not address potential infringements of privacy. The technology would continue to erode anonymity, transform the public space and undermine the very foundations of open and free societies. Offering strong safeguards to limit the use of facial recognition in publicly accessible spaces would only normalize some degree of mass surveillance. This could be manageable in Western jurisdictions with strong institutions and robust enforcement capacities: however, it may not be an acceptable standard across either the region or the Global South, where normative safeguards may be weak from the outset.

As multiple countries are exploring how to approach the use of biometric and AI technologies, this is the right time – in Argentina, Brazil and Latin America more broadly – for an open debate about how to move forward with regulating facial recognition. A central challenge will revolve around whether to attempt to put 'the genie back in the bottle' through the imposition of outright bans (as framed by Carly Kind, Director of the Ada Lovelace Institute)[158] or to focus on building the proper safeguards to prevent abuses deriving from ongoing uses of this technology. But could such protections prove sufficiently robust in Latin America?

While arguments in favour of a ban are compelling, it is also clear that no safeguards would be a worse outcome than some safeguards. Constructing adequate protections – such as having strict internal and external oversight mechanisms over the institutions in charge of conducting facial recognition; offering proper avenues for redress in cases of discriminatory uses of the technology, or false positives; and opening data on the performance of facial recognition systems to assess effectiveness and bias – may test local institutions

156 Poverty rate as of the first trimester of 2021. See Chequeado (2021), 'La pobreza bajó en relación con 2020, pero aún se ubica por encima de los niveles prepandemia' [Poverty down in relation to 2020, but still above pre-pandemic levels], 30 September 2021, https://chequeado.com/hilando-fino/la-pobreza-bajo-en-relacion-con-2020-pero-aun-se-ubica-por-encima-de-los-niveles-prepandemia.
157 Ng, A. (2020), 'How China uses facial recognition to control human behavior', CNET, 11 August 2020, https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand.
158 Kind (2020), 'Nowhere to hide'.

in Latin America, but these would constitute important steps in moving regional regulation and facial recognition implementations in the right direction.

In the case of Buenos Aires, where the use of live facial recognition was fully operational until April 2022, policymakers need to urgently reassess the potential human rights impacts of such practices and acknowledge the extent to which current safeguards offered in Argentina are far behind acceptable, minimum standards in the EU, UK and US. In the case of Brazil, where the public debate around the use of biometric technologies has been more sophisticated, the need for regulation to guide facial recognition deployments and pilot projects is becoming ever more pressing. Beyond law enforcement-driven uses of the technology, regulation must extend to other problematic applications of facial recognition within Brazil, such as in the distribution of social benefits.

Recommendations

Some additional recommendations can be drawn for other Latin American policymakers exploring strategies to regulate facial recognition technologies:

Facial recognition regulation should be anchored on human rights. Latin American countries share a strong tradition of engagement with regional and international human rights processes, and human rights standards are widely accepted in the continent. As the region continues to explore how human rights standards apply to emerging technologies and digital environments, the regulation of facial recognition technologies must be anchored in these guiding principles and must uphold regional commitments to the protection of individuals' rights to privacy, to freedom of opinion and expression, and to freedom of peaceful assembly and association, as well as rights to non-discrimination and due process. In particular, any regulation designed to enable exceptional law enforcement-driven uses of facial recognition in public spaces must build robust safeguards to protect said human rights. There are some internationally agreed standards on what constitute proper safeguards. These include: (a) ensuring transparency around the deployment and use of facial recognition technologies, with the regular reporting of performance data – as validated by external oversight – and putting mechanisms in place for a swift response to freedom-of-information access requests; (b) rendering procurement procedures for the acquisition of surveillance technology more transparent, with proper disclosure of information on technology providers and the features of the technologies employed; (c) guaranteeing data security and adequate data handling procedures, ideally as guided by national data protection legislation, if in place, or following international standards; and (d) guaranteeing internal and external oversight of specific technology deployments, including mechanisms for redress for those affected by wrongful identifications. In addition, private companies engaged to provide the technology or run the software on behalf of governments should abide by human rights guidelines as specified in the UN Guiding Principles on Business and Human

Rights.[159] The establishment of specific safeguards and mechanisms for oversight that adjust to local realities may be discussed and agreed by joint working groups coordinated by implementing authorities, with the participation of policymakers, security forces, technical specialists, civil society, privacy watchdogs and ombudsman agencies.

Authorized uses of facial recognition must steer clear of 'no-go' zones. International debates on the use of facial recognition and emerging regulation in Western jurisdictions are beginning to generate some valuable guidelines to deal with the technology. Strong agreement has emerged around what can be considered as no-go zones for law enforcement uses of the technology, which are those where potential drawbacks to human rights exceed potential benefits. This translates into enabling the exceptional use of facial recognition technologies in public spaces only in the case of serious criminal offences or life-threatening emergencies, and excluding what is currently authorized in the case of Buenos Aires: the use of the technology for persecution of petty crime. The regular use of live recognition – which until April 2022 was a regular practice in Buenos Aires – is also emerging as a no-go zone, with regulatory frameworks only allowing its deployment under exceptional circumstances. Requiring judicial or third-party authorization from applicable government agencies is also becoming established as a widely accepted standard, serving as a crucial safeguard to prevent abuses in the use of the technology.[160] This has been seen, for example, in legislation in parts of the US and in the EU's proposed AI Act. Different standards emerge when it comes to judicial or external authorizations. In the US, the debate has split between those who favour the application of probable cause as the required standard and those who favour more broad uses of facial recognition when relevant for the investigation. While more stringent standards make for more robust safeguards, what is clear is that the indiscriminate use of facial recognition in public spaces and its authorized use to identify minor offenders are both unacceptable, disproportionate applications of the technology – with the negative human rights impact of applying the technology outstripping any potential benefits or gains.

Facial recognition regulation should be sensitive to the local context. While regulatory frameworks from other jurisdictions may provide guidelines and innovative methodologies--such as Europe's AI risk-assessment approach – the adoption of 'copycat' legislation should be avoided, and the design of domestic laws should take into consideration local contexts and limitations. Particular attention is required around enforcement capacities to devise feasible regulatory frameworks that are applicable to the local context and the consideration of the potential impacts of algorithm bias in reinforcing structural discrimination along racial or class lines in Latin America.

---

159 See United Nations (2011), *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*, New York and Geneva: United Nations, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

160 According to existing regulation in parts of the US and under the proposed EU regulation on AI, facial recognition may be deployed without authorization in emergency situations. The EU's proposed AI Act establishes the need for law enforcement to request ex-post authorization when deploying facial recognition in emergencies and to present 'the reasons for not having been able to request it earlier'; these provisions are meant to prevent abuse and further strengthen safeguards. See point 21 in Council of the European Union (2021), *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Presidency compromise text*.

States need to engage in thorough public conversations about the use of facial recognition. Policymakers and regulators, particularly those dealing more closely with the application of technologies for public safety, must become more conversant with the potential human rights impacts of emerging technologies. They should also strive to generate open opportunities for debate prior to any type of technology deployment. The two public audiences organized in 2019 by Brazil's National Congress and the federal public ministry, and the current consultations in the country's federal senate, on the drafting of an AI regulatory framework, are examples of how such debate may be accomplished. The EU's multiple public and expert consultations on the AI Act also provide a model for how this level of public dialogue may be enabled with relevant stakeholders.[161] In addition to formal consultation processes, debates should also extend to the general public, and in particular, to populations that may be affected by specific technologies. Civil society and human rights groups have contributed to such efforts and need to be actively engaged. This may be accomplished, for example, through town-hall meetings, which are uncommon but not unprecedented in modern Latin America.

Latin American governments still have a long road ahead of them if they are to move towards the establishment of adequate regulation to deal with the use of facial recognition technologies. This will require regional policymakers to actively engage with security forces in devising adequate normative guidelines and to explore the adoption of technologies that effectively serve the public interest, while protecting fundamental rights that are essential to democratic societies. More in-depth policy analysis will be required if the use of biometric and AI-based technologies is to be limited, and national strategies for AI will need to be developed. Most importantly, Latin American governments which have allowed the widespread adoption of facial recognition technology must acknowledge the potential risks associated with its use and enact proper regulation to prevent such abuses.

161 European Commission (undated), 'A European approach to artificial intelligence', https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

About the author

Carolina Caeiro is an Academy Associate at Chatham House and was the Richard and Susan Hayden Academy Fellow, hosted by the US and the Americas Programme, in 2021. After completing her fellowship, she took up the position of senior policy and governance specialist at Oxford Information Labs. She specializes in internet and technology policy with a focus on regional perspectives from the Global South.

Prior to joining Chatham House, Carolina worked in the internet and media industry, including the Regional Internet Registry for Latin America and the Caribbean (LACNIC) and Argentina's first fact-checking organization, Chequeado. At LACNIC she coordinated a range of initiatives aimed at promoting internet freedom, stability and access in Latin America and the Caribbean. At Chequeado, she worked on forging partnerships to fight misinformation and innovate in how readers interact with news through the use of technology.

Carolina holds a BA in Political Science and Sociology from Middlebury College in the US, and an MA in International Development from the Graduate Institute of International and Development Studies in Geneva, Switzerland.

Acknowledgments

The author would like to thank Christopher Sabatini for his guidance and mentorship in the preparation of this paper, and her former colleagues Anar Bata, Courtney Rice, Marianne Schneider-Petsinger and Leslie Vinjamuri of the US and the Americas Programme at Chatham House for their valuable feedback and continued support during the research and publication processes.

The author is also indebted to numerous interviewees who took the time to share their perspectives and expertise during the research: Eduardo Bertoni, Emiliano Falcon-Morano, Eduardo Ferreyra, Pedro Augusto P. Francisco, Elena Lazarou, Christian Perrone, Tamara Taraciuk Broner, Leandro Ucciferri and Jamila Venturini.

Sincere thanks are also due to Richard Whitman and Carolina Aguerre for their valuable advice on the onset of the project, as well as to Kate Jones, Yasmin Afina and the anonymous peer reviewers for their helpful feedback on an earlier draft of the paper. The author would also like to thank Susan and Richard Hayden for sponsoring her fellowship, and the team at Chatham House's Queen Elizabeth II Academy for Leadership in International Affairs. Finally, the author would like to thank Vera Chapman Browne for her excellent editing.

Cover image: Visitors to the Botero park in Medellín, Colombia, observe the city's first robotic policeman on 30 September 2022.
Photo credit: Copyright © Jorge Calle/Anadolu Agency/Getty Images

ISBN 978 1 78413 540 9
DOI 10.55317/9781784135409

Cite this paper: Caeiro, C. (2022), *Regulating facial recognition in Latin America: Policy lessons from police surveillance in Buenos Aires and São Paulo*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784135409.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223