INTERNET POLICY REVIEW
Journal on internet regulation

Volume 12 **Issue** 1

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

The grey-zones of public-private surveillance: Policy tendencies of facial recognition for public security in Brazilian cities

André Ramiro *Alexander von Humboldt Institute for Internet and Society*
andrebramiro@gmail.com
Luã Cruz *State University of Campinas (Unicamp)*

DOI: https://doi.org/10.14763/2023.1.1705

Published: 31 March 2023
Received: 16 September 2022 **Accepted:** 21 December 2022

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Ramiro, A. & Cruz, L. (2023). The grey-zones of public-private surveillance: Policy tendencies of facial recognition for public security in Brazilian cities. *Internet Policy Review*, *12*(1). https://doi.org/10.14763/2023.1.1705

Keywords: Facial recognition software, Security, Surveillance, Privacy, Brazil

Abstract: The provision of biometric surveillance systems in cities' administration in Brazil is commonly delegated to private companies, where businesses supply facial recognition technologies (FRTs) to law enforcement entities. These public-private partnerships often manifest a lack of transparency, while counting on the legitimacy of the public administration to offer public services. These regulatory "grey-zones" affect smart city policies in Brazil, sidelining civil society and researchers, while narratives of efficiency push ahead the digitalisation of public services without proper safeguards. In Brazil, the collaborative work of civil society before the courts and government authorities has been the most successful path in halting FRTs in the area of public security, establishing strategic precedents that discursively focus on the "right to the city". This paper aims to achieve three goals: 1) shed light on these governance grey zones in order to identify the particularities of public-private models employed in the Brazilian socio-economic context; 2) examine the Brazilian human rights' organisations' attitudes towards the use of FRTs; and 3) provide a set of resilient principles that must guide biometric surveillance policies at the city level.

This paper is part of **Future-proofing the city: A human rights-based approach to governing algorithmic, biometric and smart city technologies**, a special issue of *Internet Policy Review* guest-edited by Alina Wernick and Anna Artyushina.

Introduction

Digitalisation is among the top priorities for national and local governments around the world. It is common for the technological development – and therefore the economy ouvertures made possible by the "innovation demand" – of public policies to be assumed as a "smart city" programs, although the concept of it is not yet unified in different strategic planning processes for cities (Angelidou, 2015), and does not always include innovative forms of governance. Some cities, like Barcelona, are implementing participatory mechanisms for the technological development and governance by the public sector and civil society (Morozov & Bria, 2018). In other cases, public-private partnerships (PPP) are a model for public services based on new technologies, keeping citizens apart from the decision-making process and affecting the assessment of risks to human rights (Brandusescu, 2021; Reia & Belli, 2021).

Regarding public security in particular, the datafication paradigm (van Dijck, 2014; Majias & Couldry, 2019) has been assuming the form of, for example, crime prediction algorithms and risk assessments in criminal justice systems (Angwin et al., 2016; Bennett Moses & Chan, 2018), as well as surveillance programs (Clarke, 1988; van Dijck, 2014), more specifically when biometric systems are prevalent throughout the public space collecting the bulk of citizens' personal and sensitive data. Furthermore, the narrative marketing of "smart technologies" companies, by creating discourses where cities are permanently at the threshold of urban crisis, involve increasing insecurity, influencing the conditions for city governments to commission their private solutions, which would supposedly offer more results with less data-driven effort (Sadowski & Bendor, 2018).

At least two conditions compose "grey-zones" of public-private surveillance, illustrated in the deployment of FRTs in Brazilian cities: (i) the nature of public security policies at the city level, broadly based on PPP that, while counting on the legitimacy of the public sector, require limited transparency and accountability from private companies that provide the technology; and (ii) the lack of specific data protection regulation for law enforcement and public security purposes, resulting in uncertainty in the Brazilian legal framework concerning surveillance technologies, such as biometric systems.

First, the private sector takes a leading role in the deployment of emerging technologies in cities, which often leads to the commercial interests overriding the public interest in such areas as education, urban planning and public security (Voorwinden, 2021; Green, 2019). As argued by Sadowski and Pasquale (2015, p. 3), "Getting smart is the handy panacea for overcoming austerity, managing the urban system, and becoming an attractive place for capital to flow into". This arrangement establishes legal conditions for PPP that serve the interests of businesses' rather than protecting the privacy and data rights of citizens (Brown, 2019). These public private partnerships challenge traditional mechanisms of democratic accountability, public participation in policy-making processes and influence how cities will be defined in the future (Grossi & Pianezzi, 2017). In Latin America, for instance, public bids for the FRTs often do not require public consultations (Venturini & Garay, 2021), or often push it to the "future" (Santos, 2021).

Second, the Brazilian legal framework regarding data protection has been evolving gradually over the past decade (Data Privacy Brasil, 2023), but still has loopholes in the area of public security. The Brazilian General Data Protection Law (LGPD) has been effectively enforced since 2019 and established a long-expected regulation to private and public entities when processing personal data. Some critical areas were nevertheless left outside of its scope, such as law enforcement investigations and public security. Data protection scholars in Brazil think that the deployment of surveillance systems without a proper data protection regulation in this area could lead to a disruption of the presumption of innocence, essential to the rule of law (Belli & Doneda, 2021). Additionally, civil society has been calling for the ban of the technology in the area of public security (Coalizão Direitos na Rede, 2022).

Regardless of the exception aimed at public security actions, the LGPD itself also defines some limits, stating that the processing of personal data will be governed by specific legislation, which should provide the proportional measures strictly necessary to meet the public interest. Subject to due process, data protection principles and data subject rights are provided for in the LGPD. In addition, the LGPD also provides mechanisms, such as the production of specific reports to the data protection authority, as well as personal data protection impact assessments in order to give more transparency to data processing activities for public security purposes. In this sense, it is worth remembering that PPP are an essential part of smart cities, but many of these agreements are rarely subject to any public oversight or scrutiny on a regular basis.

On the other hand, the country has seen continuous advances in its data protection

regime. At the end of 2020, a draft bill was proposed to the Chamber of Deputies by a special commission chaired by a Superior Court of Justice (STJ) judge, Néfi Cordeiro, and composed by renowned legal scholars and data protection experts, in order to regulate data protection in the the field of law enforcement and public security: a "Criminal LGPD" (Superior Tribunal de Justiça, 2020). According to the Brazilian "Coalizão Direitos na Rede" (2020), which is composed of more than fifty civil society organisations and research institutes, the bill offers a fundamental compatibility between law enforcement needs in accessing personal data and safeguards to citizens, as well as legal remedies in cases of abuse by public authorities.

In a case involving a Presidential Provisional Measure (MP 954/2020) during the pandemic, Brazilian telecom companies were ordered to share personal data of more than 200 million users with a federal government entity – the Brazilian Institute of Geography and Statistics (IBGE) – but a 2020 Federal Supreme Court (STF) decision halted the effects of the MP, considering it disproportionate and ruled that data protection constitutes an autonomous fundamental right (Poder 360, 2020). The decision opened a pathway for the Federal Senate, in 2022, to amend the Federal Constitution (EC nº 115/2022) and add the right to data protection to its scope of fundamental rights (Autoridade Nacional de Proteção de Dados, 2022). This shift in the data protection regime can be interpreted as a new chapter in the federal and local governments' duties to protect human personality and dignity by promoting proactive data protection policies, not only avoiding unauthorised use of citizens' data, but also by promoting institutional means to continuously improve the protection of personal data (Ramiro & Canto, 2021; Bioni & Monteiro, 2020).

Despite the aforementioned legislative horizon and the recent Supreme Court ruling, the mentioned grey-zones gain ground in the lack of proper regulation. In this article, we analyse these conditions and offer a mapping of the current human rights organisations' public responses to the use of FRT for public security. Our aim is to analyse the governance of the biometric surveillance technologies in the Global South by using Brazil as our case study. We also aim to provide some policy recommendations to the municipalities who seek to engage in PPP with technology businesses.

Facial recognition, privacy and the urban experience

The emergence of biometric surveillance systems has been long described as a means for mass identification and social control (Lyon, 2008; Pugliesi, 2010; van

der Ploeg, 2005). Technically, it mostly depends on biological – physical and behavioural – metric patterns (Agarwal, n.d. as cited in Finck, 2022) that have their data collected in order to provide, through an algorithmic process, personal identification outputs based on a prior database. In biometric surveillance policies, it is possible to argue that the most prominent application is FRT, which is intended to identify data subjects based on their "measurable" facial features, such as the distance between their eyes and ears, size of cheekbones, shape of jaws and so on (Leslie, 2020). Those mechanisms offer multiple prejudices, as they don't encompass the variety of nuances bodies have, and experiences they live, which often result in racist, misogynist and transphobic biometric algorithm outputs (Silva, 2022; Herberling, 2022).

In the European Union, the European Data Protection Board has recently published guidelines on the use of FRTs in the area of law enforcement, broadly based on the European Charter of Fundamental Rights, the European Convention on Human Rights and the Law Enforcement Directive (European Data Protection Board, 2022). On the other hand, in the case of FRTs in "public accessible spaces", the EDPB and the European Data Protection Supervisor (2021) have called for its ban. This position was also promoted by European civil society groups in the region, including the Privacy International, European Digital Rights, Article 19, Bits of Freedom and La Quadrature du Net (Goujard, 2022; Reclaim Your Face, 2023). Despite the heated discussions over its use, the FRTs are still deployed. Recently, the critics pointed out that the proposed AI Act did not establish proper guardrails to sufficiently address the risks to fundamental rights posed by this technology (Mobilio, 2023).

From an international human rights law perspective, the deployment of FRTs for law enforcement and public security purposes needs to be safeguarded by effective impact assessments, as well as on policy tools that further necessity, proportionality and oversight provisions. For instance, the Pact of San José da Costa Rica (American Convention on Human Rights) (Convenção dos Estados Americanos, 1969), and the International Covenant on Civil and Political Rights (United Nations, 1966), from which Brazil is a signatory, bring principles, such as legality and necessity, that must be observed when evaluating restrictions to human rights, such as freedom of expression and opinion. In the case of Brazil, it is not only the legal framework that still doesn't count on a specific law to address the processing of personal data in such areas, as stated above, but also the National Data Protection Authority (ANPD), effectively created in 2019, still has not established guidelines on the subject.[1]

1. For contextualisation, Brazil has a dualist legal system, according to which the ratification of an in-

An additional layer to assess impacts on human rights would be to assume that the trade-offs affect not only individuals' rights, but also collective dimensions of the "right to the city", which is deeply attached to the exercise of political rights, social participation and transformation (Purcell, 2013; Harvey, 2008, 2013). Especially in cities with a considerable level of technology development within their urban services infrastructure, the rights to privacy and data protection can protect or stifle the freedoms of expression, assembly and association, making the mutual relations between those rights clearer (Doneda, 2022; La Rue, 2013). The United Nations Human Rights Committee's General Comment nº 37 on the Right to Peaceful Assembly (2020) states that, concerning FRTs identifying people in a crowd, "[t]he mere fact that a particular assembly takes place in public does not mean that participants' privacy cannot be violated", which means that personal data disposed in public space is not merely "available" to be processed, but deserves the same protection as in private spaces, even more so when the matter of concern is sensitive. As a result, even in public spaces reasonable expectations of privacy would also have to be assumed under privacy and data protection laws (Edwards, 2016).

The effects of FRTs on political freedoms are evident in the stifling of protests around the globe. For example, in the anonymity struggles in Hong Kong that manifested in 2019 and 2020 (Millet, 2020), and in the 2021 peaceful protests in Moscow (Bacchi, 2021) (in both instances protesters used means to disguise their identity with masks, face paintings, and umbrellas); also recently, the use of FRTs to track Black Lives Matter activists in the United States (Vincent, 2020); and in Colombia during the 21N protests, which were pushed by a variety of social sectors such as student movements and trade unions, helicopters were used to track manifestants (Dejusticia, 2021). The chilling effects of FRTs are easily perceived and, as a result, unproportional surveillance can compromise potential social justice transformations.

This is the case not only with regard to political dimensions of the city space; a lack of privacy impacts the citizens' involvement when experiencing the city. In "The Death and Life of Great American Cities", Jane Jacobs has already called attention to how excessive identification might jeopardise individual's quality of life when interacting with the city:

ternational treaty is not enough for the international rule to come into effect. In order for citizens to claim their human rights, it has to be incorporated in the national legislation. See Lupi (2009).

> Privacy is precious in cities. It is indispensable. Perhaps it is precious and indispensable everywhere, but most places you cannot get it. In small settlements everyone knows your affairs. In the city everyone does not-only those you choose to tell will know much about you. This is one of the attributes of cities that is precious to most city people, whether their incomes are high or their incomes are low, whether they are white or colored. [...] A good city street neighborhood achieves a marvel of balance between its people's determination to have essential privacy and their simultaneous wishes for differing degrees of contact (Jacobs, 1961, pp. 58-59).

Investigating the role of smart cities in the functioning of city administrations, while also considering sociopolitical factors that affect them, can reveal citizens' perceptions of freedom when experiencing the city and interacting with other people and places – to Jacobs, this is the "sidewalk life" (1961). In the contemporary Brazilian cases of urban management, what is seen is the expansion of surveillance-based public security programs founded on models of privatisation. Bruno Firmino (2018) has analysed the "Center of Operations" (COR) in the city of Rio de Janeiro, which was once the locus, for example, of IBM's Smart Cities project investments, in order to monitor the daily routine of the city, including traffic, climate and social media interactions, in order to "respond effectively" to emergency situations – "a synoptic, war room-style overview" (Greenfield, 2015). The COR used to share data with the "Integrated Centers for Command and Control" (CICC), which were specific government entities for public security. The CICC's model has been expanded to several capitals in Brazil (Firmino, 2018; de Vasconcelos Cardos, 2019) and it now increasingly relies on FRT (Centro de Análise da Liberdade e do Autoritarismo [LAUT], 2021; Nascimento, 2022; Sampaio, 2022).

Those "perceptions of freedom" in Brazil necessarily deal with the racial aspect of the urban experience, also illustrated in recent statistics about the odds of a black person being arrested because of facial recognition. In the country, 56,1% of the population is black or brown-skinned (74,5% in the Northeastern region, for instance) according to recent survey by the Brazilian Institute of Geography and Statistics (Ferrari, 2022), and 8 out 10 black citizens already were approached by the Military Police in States as São Paulo and Rio de Janeiro, as shown in research conducted by the Instituto de Defesa do Direito de Defesa and Data_Labe (2022). Other research from 2019 has shown that when it comes to arrests assisted by FRT, 90% of the people were black, according to the Rede de Observatórios da Segurança (Nunes, 2019). Pablo Nunes, researcher of the Centro de Estudos em Segurança e Cidadania (CESeC), has stated that to young black people, FRT "is the cer-

tainty that they will continue to be approached by the police arbitrarily" (2019, para. 5).

Lila Lee-Morrison (2019) argues that the "automation of the visual sense" ideal, once applied to the controlled environments of industrial factories in order to sort and inspect manufacturing flows, has resulted in surveillance systems that monitor, inspect and target the flow of people in society. In association with the inequalities that already characterise the urban space in places such as Brazil, this automation breeds structural racism at the algorithmic level,[2] especially when considering the sociopolitical history of public institutions that have been understood as instruments of segregation (Costa & Kremer, 2022; Silva, 2022).

Public-private characteristics and regulatory grey-zones

Marketing discourse precedes public-private FRT deals to frame it as the ultimate efficiency and optimisation of public services. This business-led, optimistic rhetoric has been subject of criticism in the growing body of literature that examines how corporate visions have prevailed in smart cities projects (Reia & Cruz, 2023; Grossi & Pianezzi, 2017; Hollands, 2015; Greenfield, 2013). In the last twenty years, major technology companies such as Alphabet (Google), IBM and CISCO have been selling their products to the public sector in order to collect data and provide "urban solutions" (Sadowski & Bendor, 2018), helping create a widespread model of city administration that values privatisation of the city services as unavoidable process (Wiig, 2015). Cities have been serving as terrestrial spaces where neoliberal initiatives continue to establish their roots (Brenner & Theodore, 2002) and portray urban problems as crises that can be addressed through PPP.

These narratives mobilised by the private sector to sell smart city technologies contribute to the expansion of sociotechnical imaginaries (Jasanoff, 2015) that see cities existing on the cliff of an urban crisis that can and must be solved through new technologies – what Morozov would describe as techno-solutionism (2013).

2. It is important to mention that the violations to due process and fair trial fundamental rights, for example, are at the centre of the public debate in Brazil, as the country has seen several episodes of police arrests that later were proved to be based on FRT false-positives: in the Federal District, the Civil Police arrested a low income black man, yelling and kicking his house door at 5 a.m., as he was mistaken for someone else because of the FRT in the city (Bomfim, 2021); in Rio de Janeiro, a woman was also arrested for the same reason, mistaken for an outlaw (Correio 24 Horas, 2019), just to mention a few cases. Even with the arrests being later reverted, the violation of rights was in place beforehand, and the involved persons were unaware of their rights or the reasons for their arrests. The context gives form to a Kafkian-Orwellian dystopia where a lack of information added to constant surveillance leads society to a state of collective anguish (Solove, 2011).

In terms of public security, the mobilised discourses meet, for example, with how city mayors address urban violence as an issue that must take advantage of "the latest in technology" (New York City, 2022) – without qualifying results provisions or providing risk assessments – and take the opportunity to pitch FRT private providers as a means to "revolutionize" the security model of public events (Burt, 2022). In France, the Mayor of Nice has supported start-up providers of FRTs while calling public oversight entities, like the Commission Nationale de l'Informatique et des Libertés (CNIL), the French national data protection agency, as "dusty institutions" because of their criticism over the unregulated use of the technology (Rees, 2022). As a result, a solutionist narrative portrays the rights guarantees enforced by oversight authorities as outdated.

As noticed by Alcides Eduardo dos Reis Peron (2019, 2021), security programs in the State of São Paulo, such as the "Detecta", "City Câmeras" and "São Paulo Inteligente", have been impacted by the notion of "smart cities" and increasingly count on partnerships between the government, national private companies and also on the international industry of security. He argues that this model of governmentality explores a broader surveillance digital apparatus, such as FRTs, and presupposes a permanent administration of fear to create a permanent atmosphere that would be "saved" by PPP and technology solutions.

The impact of FRTs on the work of law enforcement in Brazil, a developing country that historically struggles with socioeconomic inequalities that manifest in the level of urban violence (Adorno, 2002) and racial bias in the work of police, is insurmountable. Notably, the promotion of FRT for public security is not even about achieving better crime statistics, but about how contracts with FRT vendors help create a positive image of a particular city administration. An example of this would be the creation of new job opportunities, or even a larger municipal budget as a result of private investments (a trend similar to the United States and Europe, see Green, 2019; Hollands, 2015). In Salvador, the deployment of FRT is seen as necessary to, beyond preventing criminal activities, to help create new jobs and income for citizens, as well as tourism opportunities in the city (A Tarde, 2021). In Recife, the arrangement of the public private partnerships (PPP) is framed as a possibility of economic success for the City Hall: the vendor will have to actually pay to install "totems" in the public space – with a range of "smart" gadgets such FRT, as well as led screens for advertising and Wi-Fi – and, in exchange, the company will be able to rent the led screens to other businesses (Tenório, 2022). The public discourse on economic development, fueled by private sector marketing, appeals to the underdeveloped conditions of Brazilian cities, and creates

workarounds that deviate from the privacy and data protection debate, as well as from the very possible inefficiency of FRTs regarding tackling crime rates. While social and political issues could remain unaddressed, such as transparency and algorithm accountability requirements, PPPs have framed public services as a for-profit area that benefits public and private economic discourses (Voorwinden, 2021).

When it comes to applying regulatory models concerning privacy, the big challenge is to find an *ex ante* framework to enforce strict data protection provisions. In the case of Brazilian PPP-based biometric surveillance policies at the city level, as argued by Malgieri and Pasquale (2022), it is necessary to assume that artificial intelligence systems are "unlawful by default", thus developers have the burden of proving that they are not discriminatory, unfair or inaccurate prior to deployment, not after a rights violation happens. There are at least three challenges in this respect: first, the lack of transparency in algorithmic solutions due to the imposed intellectual property protections (such as trade secret rights), or because of the inscrutability of automated decisions to the public; second, these same vendors succeed in deploying their technologies with the city administration as a legitimate proxy to offer public services (Colleta et al., 2017), while the same administration takes advantage of the opacity of the algorithms to deflect the attention of the civic services from the decisions they make; and third, if the national data protection regulation has exception loopholes to its enforcement when it comes to public security ends, such as the Brazilian LGPD, the lack of legal contemporary tools to call for transparency and accountability in such systems can pave the way for a regulatory grey-zone that facilitates opaque public-private mass surveillance policies in the cities.

The result is a model of technology governance applied to public services that sidelines the civil society concerns. It offers greater social repercussions when the focus of such policies are areas and segments of society historically surveilled and targeted based on race and socioeconomic conditions (Browne, 2015). That is especially important in the context of public security in Brazil, where the suspension of human rights not only regarding privacy, freedom of expression and manifestation, but the very liberty and life of black people, is a massive issue. This model defines how the power plays in Internet and new technologies governance (Carr, 2015), gives legitimacy to private companies that develop digital infrastructure for public services and helps state actors obscure the violations of the public interest in their work. This equation creates dangerous grey-zones in which citizens' rights are sidelined, which paves the way to undemocratic city policies, even more so in

territories where racial and socioeconomic pre-conditions are already extremely biassed and exclusionary.

The privatisation of public security services at the city level echoes the trend of privatisation of prisons – a market tendency for private companies that profit by providing infrastructure, such as surveillance technologies. Prisons serve as "both the laboratory and first market" (Gow, 1997) for surveillance technologies, which has now been expanded to outdoor spaces as a result of the securitisation processes in the city spaces (Williams, 2003).

The human rights organisations' responses to the use of FRT for public security

In recent years, there is a widespread deployment of surveillance technologies, such as facial recognition, throughout the Global South. For instance, in Latin America, a number of civil society organisations have begun to submit requests for access to information to public administrations, in order to understand the details of the use of facial recognition in public spaces (Venturini & Garay, 2021). For these organisations, in their words, it was essential to ask appropriate questions about measures that interfere with the full enjoyment and exercise of fundamental rights, especially considering the region's background of the implementation of surveillance technologies in a non-transparent way and without due public debate (Ucciferri, 2019).

Such actions have been the starting point for more robust actions in an attempt to block the implementation of FRTs, and some have been successful, while others not so much. For example, in Argentina, Brazil and Peru, public agencies have been fined and/or forced to suspend the implementation of such systems because it was found – after the aforementioned requests for information – that in all cases a series of regulations related to the personal data protection had not been respected (Vida, 2022). In Paraguay, it was not even possible to access the information. When faced with successive denials of access to information on the operation of the facial recognition system implemented in the city of Asuncion, in 2019 the digital rights defence organisation TEDIC filed an action of unconstitutionality, questioning the allegation that it was reserved national security information (Venturini, 2020).

While in Latin America the implementation of FRTs is increasing, in recent years, some US cities and states, and European countries, have achieved advancements in establishing constraints regarding FRT based on the understanding that they vio-

late privacy and the presumption of innocence, and that the technology boosts discrimination against marginalised groups, among many other problems (Kak, 2020; Laperruque, 2022; Mobilio, 2023). With this dual scenario – increasing impetus for restrictions in the global north and lack of regulation in the global south – in mind, in an initiative promoted by Brazilian civil society called #SaiDaMinhaCara (Get Off My Face), more than fifty lawmakers from different parties acting in the municipal or state legislature have introduced bills to ban facial recognition in public spaces (Coding Rights, 2022).

In addition to strategic litigation[3] and legislative efforts against the FRT implementations mentioned above, organisations have created broad campaigns for the banning of FRTs: Argentinian #ConMiCaraNo (Asociación por los Derechos Civiles, 2019), Mexican #NoNosVeanLaCara (Red en Defensa de los Derechos Digitales, 2020) and Brazilian #TireMeuRostoDaSuaMira (2022). By understanding that there are sufficient reasons to completely restrict the use of facial recognition, for surveillance purposes, by security and intelligence forces, various organisations that are building such campaigns are (i) monitoring the situation in their countries to report when a government implements such technology; (ii) writing open letters addressed to various actors and; (iii) producing materials for the general public regarding the implementation of biometric technologies in Latin America.

More specifically, Brazilian civil society has influenced and been influenced by all these neighbouring movements, and its performance on this issue has been an example that deserves further debate, and this is what we intend to do in the following section.

The countervailing movements towards facial recognition technologies in Brazil

Facial recognition has been in use in Brazil since 2011, but it became especially popular in 2019 (Lobato et al., 2020), and the advancement of the technology in the country has led to movements for the regulation of facial recognition and, in some cases, its partial or complete ban.

It is important to mention that this is not a completely new debate. In 2009, the Madrid Declaration, signed by Brazilian organisations such as the Brazilian Institute for Consumer Protection (Idec) and the Nupef Institute, already called for a

3. Based on Leticia Marques Osorio (2019), we understand strategic litigation as a form of advocacy: a process with a broader impact than simply providing a remedy for a plaintiff in a certain specific case, whose goal is to modify, through judicial decisions, the law and public policies.

moratorium on FRTs for surveillance purposes:

> Civil Society takes the occasion of the 31st annual meeting of the International Conference of Privacy and Data Protection Commissioners to: [...] Call for a moratorium on the development or implementation of new systems of mass surveillance, including facial recognition, whole body imaging, biometric identifiers, and embedded RFID tags, subject to a full and transparent evaluation by independent authorities and democratic debate (The Public Voice, 2009)

Almost ten years later, in August 2018, Idec went to court against ViaQuatro, the concession holder of São Paulo's metro's yellow line, a privately-run line, for processing emotion data from passengers (Columbia Global Freedom of Expression, 2021). The camera system recognised human presence and performed the identification of emotion, gender and age from the people positioned in front of advertisements billboards with the intention of capturing their reactions.

The lawsuit was the result of collaborative work between Idec, the Latin American Network of Surveillance, Technology and Society Studies (Lavits) and the Tutorial Education Program (PET) of the Law School of the University of São Paulo. In addition, the Public Defender's Office of São Paulo participated in the lawsuit as a co-plaintiff and the Alana Institute as *amicus curiae* (friend of the court). The Institute for Research on Internet and Society (IRIS) and Access Now also produced technical opinions on the case (Teofilo et al., 2019; Arroyo & Leufer, 2020).

With the country lacking a data protection law at the time, the lawsuit was based on the violation of basic consumer rights, such as consenting to the collection of their data and being informed about what will be done with it. In addition, it highlighted the illegality of the non-consented use of FRTs, supported by the fact that ViaQuatro's cameras were not intended to improve the transportation service, but to analyse people's emotions when facing advertisements. In 2021, the company was ordered to pay a fine of 100,000 Brazilian reais and is prohibited from reactivating its 2018 initiative. The decision was the first of its kind in the country and emphasised the need to obtain users' prior consent for their data to be collected and, further, that the validity of consent is conditioned on the provision of clear and specific information about the collection and processing of data.

Since the lawsuit filed against ViaQuatro, civil society has been acting on other fronts to prevent the collection of facial recognition data without citizens' consent. In February 2019, Idec notified Hering, a Brazilian clothing franchise, about the

use of facial recognition for targeted advertising purposes without permission (Mari, 2019). Following this, Senacon (the National Consumer Secretariat) convicted the company of violating citizens' right to information and their personality rights, ordering them to pay a fine of 58,767 Brazilian reais.

Public agencies, related to law enforcement and social security, and other businesses, such as supermarkets, credit bureaus and ride-hailing apps, have also begun to be warned by civil society due to their attempts to implement FRTs, and were questioned about how they obtained consent from citizens to use biometric data, how they handle the information and whether they foresee sharing the databases with third parties or the government (Soprana, 2019). The complaints did not assume that the companies had committed an infringement, but asked for evidence to analyse whether there was sufficient transparency in their data processing. The questions were based on the Consumer Code, the Marco Civil da Internet, and the General Data Protection Law (LGPD).

In March 2022, another lawsuit – this time against the Companhia do Metropolitano de São Paulo (Metrô), the public company running the São Paulo metro system – was initiated and generated great repercussions, contesting FRT use for public security purposes. The class action lawsuit filed by Idec, the Public Defender's Office of the State of São Paulo, the Federal Public Defender's Office, Intervozes, Article 19 Brazil and South America and CADHu (Human Rights Lawyers Collective) was the result of analysis of the documents presented by Metrô in a previous lawsuit that demanded information about the implementation of the project, which cost more than 50 million BRL, and that, among other measures, involved the forecast of facial recognition in whoever used the public transportation system.

An injunction ordered the São Paulo Subway to halt the implementation of the facial recognition system, which reaches about 4 million daily users of public transportation in the state capital (Mari, 2022). According to the Court's decision, no evidence was presented that the Subway system was used only for public safety actions, which affects the fundamental rights of citizens and goes against the General Data Protection Law (LGPD).

The Brazilian backlash against facial recognition beyond the courts

The court victories are definitely being duly celebrated and recognised as important milestones in the fight against the increasing use of technology to track

Brazilian citizens (Souza & Zanatta, 2021), however, the expansion of FRTs continue, and likewise, other battlegrounds also continue to be fought over. Here we highlight a few relevant cases.

For instance, in March 2021, a state bill in São Paulo sought to authorise the use of FRTs in subway and train stations. Thus, more than 20 civil society organisations released an open letter about Bill 865/2019, which had recently been approved in the Legislative Assembly of the State of São Paulo (Instituto Ethos, 2021). According to the letter, the text of the bill, which was pending sanction by pro-FRT Governor João Dória, was approved in haste, without transparency or any dialogue with the society and sectors that work with this issue. As drafted, the legal provisions were unable to mitigate the risks involved and ensure the fundamental rights of the nearly 8 million passengers who use the system daily. Weeks after the demonstrations against the bill, the governor vetoed the bill, arguing that the project unduly interfered in the competencies of the companies that manage the passenger rail transportation system in the São Paulo metropolitan region, that is, the bill was rejected on procedural rather than human rights grounds (Vicentin, 2021).

On an international level, in June 2021, an open letter was published calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance (Access Now, 2021). The open letter prepared by Access Now, Amnesty International, European Digital Rights (EDRi), Human Rights Watch, Internet Freedom Foundation (IFF) and Idec argued that the ban was necessary because, although a moratorium could temporarily halt the development and use of these technologies, the deployment of the tool in places accessible to the public was incompatible with human rights and civil liberties. The letter defined its scope and the risks potentially caused by the use of the technology, as well as requests and recommendations for legislators, administrative agencies, judicial bodies and private entities.

Several civil society organisations, activists, technologists and other experts around Brazil joined together to sign this worldwide open letter; such a movement helped spur the creation of a national open letter and a new campaign. Thus, in late May 2022, during the 12th edition of the Brazilian Internet Governance Forum, which took place in Natal, Rio Grande do Norte, more than 30 civil society organisations launched the campaign #TireMeuRostoDaSuaMira (2022) to call for a total ban on the use of FRTs in Brazilian public security.

In addition to the traditional digital rights organisations, this movement differs from other national campaigns as it includes a series of other social organisations

from the black movement, sex workers' rights movement and informal street vendors movement, among others. Moreover, the organisations involved in the campaign have not only restricted themselves to publishing their manifesto, but are full steam ahead with various actions. In addition to the open letter, the campaign has mapped all the bills that attempt to induce the implementation of FRTs by Brazilian states, identifying the justifications and authors of the proposals. In order to exchange strategies to learn more about successes and mistakes, the campaign has also met with other campaigns fighting for the same goal in different parts of the world: United States (American Civil Liberties Union), Mexico (Red en Defensa de los Derechos Digitales), European Union (Reclaim Your Face), Argentina (Asociación por los Derechos Civiles) and India (Internet Freedom Foundation).

In terms of practical actions, some organisations that are part of the national campaign have been articulating with city councillors and state legislators for them to send access to information requests to law enforcement agencies, promote public hearings and draft laws to ban the implementation of facial recognition in public spaces. They are also mobilising public bodies, such as the Public Defender's Office, the Public Prosecutor's Office and the National Data Protection Authority, urging them to conduct proceedings to take legal action against companies and governments.

Although the fight against facial recognition is not only a privacy issue, it is interesting to see how the Brazilian actions materialise what Colin J. Bennett (2010) has described as the strategies used by activists to raise awareness about complex and abstract privacy issues, and to build support for their cause. In addition to the "insider" strategy, when civil society organisations engage with the government to advance their privacy goals, such ban campaigns also bring some "outsider" strategies, that is, through public campaigns and direct action. According to Bennett, a combination of both insider and outsider strategies is most effective in advancing privacy goals, and this is what we are seeing in this new Brazilian movement, which combines litigation, legislative proposals, meetings with activists, make-up art contests and podcasts, among many other relevant strategies.

The battle against the rampant implementation of FRTs throughout Brazil seems an inglorious task, especially given the fact that all regions in Brazil use and continue to implement the technology, and civil society efforts still cannot cope with the more than 5000 Brazilian municipalities and 26 states, most of them eager to solve their structural problems with surveillance technologies. Despite this, the strategies and arguments used by the Brazilian civil society have been an example that even in adverse scenarios it is possible to counterattack in every way avail-

able, whether through legal actions, complaints to government agencies, open letters, FRT deployment mapping, or awareness raising,and using the most diverse reasoning of rights and principles, which will be explored in detail further in the subsequent session.

Colouring the surveillance grey-zones: National horizons on data protection and international principles

The challenging actions mentioned in the previous sections fall both within a new wave of personal data protection legislations, as well as in the more traditional fields of non-discrimination and the abuse of rights in the provision of public services. In other words, it is not only relevant to violations of personal data protection laws, but data subjects who have their rights violated and are also **users of public services**, protected by specific laws such as the Public Service User Defense Code (Federal Law No. 13.460/2017), and are covered under **consumer legislation**, whether in relation to their data, the processing of such data and the information that must be made available, even more so when the provision of such surveillance structures are made by the private sector.

Under Brazilian law, **protection and security against dangerous and harmful services is a basic consumer right**,[4] and equally, security is a principle and right of the public service user. This legal framework imposes a corresponding series of duties on those who process or intend to process data, as governments and companies[5] do when implementing FRTs. In practice, these principles translate into precautions in database governance; system reliability features; anonymization of data subjects; impact assessment and risk mitigation plans in case of breaches or other violations to the data subjects' rights. With the way these facial recognition systems have been installed around Brazil – promoting the capture of biometric data of all passers-by in the city without any visual or audible warnings, experts and activists claim that they disproportionately violate indiscriminately the privacy and autonomous right to data protection of people on a daily basis, without any consent from the data subjects and without any clarity on how such data will be treated under the justification of public safety (Martins, 2022). Thus, according to this group of critics, the implementation of FRTs violate consumer rights, due to its abusiveness, lack of proportionality, disrespect for the right to information, self-de-

4. See Brazilian Consumer Defense Code, Federal Law no. 8.078. Available here.
5. The provisions of the Public Service User Defense Code apply on a subsidiary basis to public services provided by private parties.

termination, violation of the principle of vulnerability and hypo-sufficiency[6] and the right to free and informed consent provided for in the national consumer legislation.

Brazilian consumer law, with code in effect since 1990, also brings an important procedural tool, a **collective redress mechanism** called "public civil action". Therefore, the public civil action became the most modern and democratic instrument to defend the interests of consumers as a social group, interests that could never be solved if their protection was pursued by some of its members, including in discussions about data protection and the offering of transparent digital products and services, where there is a clear asymmetrical power relationship (van de Waerdt, 2020). Such a reference is relatively important in the European context as the European Parliament has recently approved a new law that will allow consumer groups to join forces and launch class actions in the European Union (BEUC, 2020). The new rules introduce a harmonised model for collective action in all Member States, ensuring consumers are adequately protected against large-scale harm and guaranteeing adequate safeguards to prevent abusive lawsuits.

The sentencing of ViaQuatro, cited above, was the result of a public civil action, for example.[7] Other public civil actions have been used to handle cases based on different situations involving privacy and data protection issues, regarding credit bureaus, data brokers, telecommunications companies and other data-driven sectors.

With robust infra-constitutional legislation in material terms, especially when it comes to consumer and public service user protection, and important procedural instruments for the defence of collective rights, the legal system is also supported by a number of other human rights principles that can be mobilised to deal with the rampant use of FRT. Here we can name a few of these: proportionality and necessity, accountability and transparency, due process and fair trial, the best interests of children and the right to equality and non-discrimination.

Conclusion

Conceptual and practical tensions follow the development of "smart cities" models in different territories, whether in Latin American metropolises or major Silicon

6. According to Brazilian consumer legislation and jurisprudence, vulnerability is a situation intrinsic to the consumer, that is, every consumer is considered vulnerable in consumer relations, and hypo sufficiency is related to the condition of disparity, where the consumer is inferior in the technical sense.

7. See The Case of São Paulo Subway Facial Recognition Cameras. Available here.

Valley cities. The particularities of how city administrations choose to establish those models tend to vary even more when comparing, for example, European and Latin American city capitals. On the one hand, the broadening of surveillance technologies such as FRTs is a tendency in public security policies worldwide and comes as a synonym for "urban planning modernity". In Brazil, the adoption of FRTs within public security policies comes mostly with PPPs that often appeals to economic narratives that could benefit local populations that historically live under socioeconomic inequalities. Therefore, the shift in the discourse brings together the will of social control under the façade of economic development.

The perceived political arrangement gives form to grey-zones of public-private surveillance, making it challenging to demand for transparency due to the intellectual property protection of such systems, as provided by the private sector and deployed under the legitimacy of the city administration to pursue public security policies. Even so, the huge privacy and data protection impact of such policies has brought together several civil society reactions in Brazil, including public campaigns nation and local wide, litigating together with public bodies such as the Public Defenders and Prosecutors, as well as the National Data Protection Authority. The legislative and judicial branches have also been activated and have already produced crucial results to qualify the debate around FRTs, such as several city level bills that aim to ban the use of the technology for public security. This would apply to judicial decisions that recognised the illegality in using FRTs, for example, to map people's emotions.

These precedents, together with civil society reactions, the Supreme Court decisions and legislative horizons in Brazil, suggest that the narratives from PPPs are suffering a shift in the public debate, something that happens as data protection culture gradually shows results in the country. Even though the sociotechnical imaginaries over technological modernity are still in dispute, and suffer from new rounds of marketing and fascination in every new public administration that wants to hit the brand of "smart cities" in every stage of urban public policies, power plays over privacy and data protection will continue to count on the city space as territory to define the limits of surveillance policies.

ACKNOWLEDGEMENTS

The authors would like to express their sincere gratitude to Jess Reia for their invaluable and insightful discussions over the past years, which have greatly enhanced the quality of this work.

References

A Tarde. (2021, October 13). Salvador terá câmeras de reconhecimento facial em pontos turísticos. *A Tarde*. https://atarde.com.br/bahia/bahiasalvador/salvador-tera-cameras-de-reconhecimento-facial-em-pontos-turisticos-1174976

Access Now. (2021). *Ban biometric surveillance*. https://www.accessnow.org/ban-biometric-surveillance/

Adorno, S. (2002). Exclusão socioeconômica e violência urbana. *Sociologias*, *8*, 84–135. https://doi.org/10.1590/S1517-45222002000200005

Angelidou, M. (2015). Smart cities: A conjuncture of four forces. *Cities*, *47*, 95–106. https://doi.org/10.1016/j.cities.2015.05.004

Angwin, J., & Larson, J. (2016, December 30). Bias in criminal risk scores is mathematically inevitable, researchers say. *ProPublica*. https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say

Arroyo, V., & Leufer, D. (2020, June 24). *Data for sale in Brazil: Access Now files expert opinion in São Paulo metro facial recognition case*. Access Now. https://www.accessnow.org/data-for-sale-in-brazil/

Asociación por los Derechos Civiles. (2019). *Con mi cara no*. Asociación por los Derechos Civiles. https://conmicarano.adc.org.ar/

Autoridade Nacional de Proteção de Dados. (2022). *Proteção de Dados Pessoais agora é um direito fundamental* [Press release]. Governo do Brasil. https://www.gov.br/anpd/pt-br/protecao-de-dados-pessoais-agora-e-um-direito-fundamental

Bacchi, U. (2021, February 4). Fears raised over facial recognition use at Moscow protests. *Reuters*. https://www.reuters.com/article/russia-protests-tech-idUSL8N2KA54T

Belli, L., & Doneda, D. (2021, September 2). O que falta ao Brasil e à América Latina para uma proteção de dados efetiva? *JOTA*. https://www.jota.info/opiniao-e-analise/artigos/o-que-falta-ao-brasil-e-a-america-latina-para-uma-protecao-de-dados-efetiva-02092021

Bennett, C. J. (2010). *The privacy advocates: Resisting the spread of surveillance*. The MIT Press.

Bennett Moses, L., & Chan, J. (2018). Algorithmic prediction in policing: Assumptions, evaluation, and accountability. *Policing and Society*, *28*(7), 806–822. https://doi.org/10.1080/10439463.2016.1253695

BEUC, The European Consumer Organisation BEUC. (2020, June 23). EU institutions reach historic deal on EU-wide collective redress law. *Press Release*. https://www.beuc.eu/press-releases/eu-institutions-reach-historic-deal-eu-wide-collective-redress-law

Bioni, B. R., & Monteiro, R. L. (2020, June 9). *A landmark ruling in Brazil: Paving the way for considering data protection as an autonomous fundamental right*. Future of Privacy Forum. https://fpf.org/blog/a-landmark-ruling-in-brazil-paving-the-way-for-considering-data-protection-as-an-autonomous-fundamental-right/

Bomfim, F. (2021, December 15). 'Disseram que eu era traficante', diz pedreiro preso injustamente. *R7 Brasilia*. https://noticias.r7.com/brasilia/disseram-que-eu-era-traficante-diz-pedreiro-preso-injustamente-16122021

Brandusescu, A. (2021). Artificial intelligence policy and funding in Canada: Public investments, private interests. *Centre for Interdisciplinary Research on Montreal, McGill University*, 1–61. http://dx.doi.org/10.2139/ssrn.4089932

Brenner, N., & Theodore, N. (2002). Cities and the geographies of 'Actually Existing Neoliberalism'. *Antipode*, *34*(3), 349–379. https://doi.org/10.1111/1467-8330.00246

Brown, T. E. (2019). Human rights in the smart city: Regulating emerging technologies in city places. In L. Reins (Ed.), *Regulating new technologies in uncertain times* (Vol. 32, pp. 47–65). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-279-8_4

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press. https://doi.org/10.1215/9780822375302

Burt, C. (2022, April 5). Wicket fields biometric fan access for baseball's NY Mets, Incode signs up soccer teams. *Biometric Update*. https://www.biometricupdate.com/202204/wicket-fields-biometric-fan-access-for-baseballs-ny-mets-incode-signs-up-soccer-teams

Carr, M. (2015). Power plays in global internet governance. *Millennium: Journal of International Studies*, *43*(2), 640–659. https://doi.org/10.1177/0305829814562655

Centro de Análise da Liberdade e do Autoritarismo. (2021). *Governador do Rio de Janeiro aprova Centro Integrado de Comando e Controle para a Baixada Fluminense*. https://agendadeemergencia.laut.org.br/2021/02/governador-do-rio-de-janeiro-aprova-centro-integrado-de-comando-e-controle-para-a-baixada-fluminense/

Cianciardo, J. (2010). The principle of proportionality: The challenges of human rights. *Journal of Civil Law Studies*, *3*(1), 177–186.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512. https://doi.org/10.1145/42411.42413

Coalizão Direitos Na Rede. (2020, November 9). *Proteção de dados pessoais na segurança pública e em investigações criminais* [Letter]. https://direitosnarede.org.br/2020/11/09/protecao-de-dados-pessoais-na-seguranca-publica-e-em-investigacoes-criminais/

Coalizão Direitos Na Rede. (2022). *Sociedade civil faz campanha para banir reconhecimento facial na segurança pública*. https://direitosnarede.org.br/2022/06/17/sociedade-civil-faz-campanha-para-banir-reconhecimento-facial-na-seguranca-publica/

Coding Rights. (2022, June 22). Legislators from all regions of Brazil present bills to ban facial recognition in public spaces. *Medium*. https://medium.com/codingrights/legislators-from-all-regions-of-brazil-present-bills-to-ban-facial-recognition-in-public-spaces-31d8da0d3822

Colleta, C., Heaphy, L., Perng, S.-Y., & Waller, L. (2017). Data-driven cities? Digital urbanism and its proxies: Introduction. *Italian Journal of Science and Technology Studies*, *8*(2), 1–18.

Columbia Global Freedom of Expression. (2021). *The case of São Paulo subway facial recognition cameras* [Case analysis]. Columbia University. https://globalfreedomofexpression.columbia.edu/cases/the-case-of-sao-paulo-subway-facial-recognition-cameras/

Convenção Americana de Direitos Humanos (Pacto de San José de Costa Rica), (1969). https://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sanjose.htm

Correio 24 Horas. (2019, July 11). Inocente é confundida com criminosa por câmera de reconhecimento facial no Rio. *Journal Correio*. https://www.correio24horas.com.br/noticia/nid/inoce

nte-e-confundida-com-criminosa-por-camera-de-reconhecimento-facial-no-rio/

Costa, R. S., & Kremer, B. (2022). Inteligência artificial e discriminação: Desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. *Revista Brasileira de Direitos Fundamentais & Justiça*, *16*(1), 145–167. https://doi.org/10.30899/dfj.v16i1.1316

Data Privacy Brasil. (2023). *Observatório da Privacidade e da Proteção de Dados—Memória da LGPD*. Data Privacy Brasil. https://www.observatorioprivacidade.com.br/memorias/

de Vasconcelos Cardoso, B. (2019). A lógica gerencial-militarizada e a segurança pública no Rio de Janeiro: O CICC-RJ e as tecnologias de (re)construção do Estado. *Dilemas - Revista de Estudos de Conflito e Controle Social*, *3*, 53–74.

Dejusticia. (2021). Día de la protección de datos: Helicópteros, reconocimiento facial y protesta. *Dejusticia*. https://www.dejusticia.org/dia-de-la-proteccion-de-datos-helicopteros-reconocimiento-facial-y-protesta/

Doneda, D. (2022). *Diretrizes para atores judiciais sobre privacidade e proteção de dados* (pp. 1–23) [Programme]. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000381298_por

dos Reis Peron, A. E., & Alvarez, M. C. (2019). Governing the city: The Detecta Surveillance System in São Paulo and the role of private vigilantism in the public security. *Sciences & Actions Sociales*, *12*(2), 33–68. https://doi.org/10.3917/sas.012.0033

dos Reis Peron, A. E., & Alvarez, M. C. (2021). O governo da segurança: Modelos securitários transnacionais e tecnologias de vigilância na cidade de São Paulo. *Lua Nova: Revista de Cultura e Política*, *114*, 175–212. https://doi.org/10.1590/0102-175212/114

Edwards, L. (2016). Privacy, security and data Protection in smart cities: A critical EU law perspective. *European Data Protection Law Review (Lexxion)*. https://doi.org/10.2139/ssrn.2711290

European Data Protection Board. (2022). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* (Guidelines 05/2022 Version 1.0; pp. 1–49). European Data Protection Board. https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

European Data Protection Board & European Data Protection Supervisor. (2021). *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)* (pp. 1–22). European Data Protection Board. https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

Ferrari, H. (2022). *População cresce com mais pessoas pretas e pardas* [Survey]. Instituto Brasileiro de Geografia e Estatística. https://www.poder360.com.br/brasil/populacao-cresce-com-mais-pessoas-negras-e-pardas/

Fight for the Future. (2022). *Ban facial recognition* [Petition]. https://www.banfacialrecognition.com/

Finck, N. (2022). Biometrics. In G. McHendry (Ed.), *Key concepts in surveillance studies*. Pressbooks. https://surveillancestudies.pressbooks.com/chapter/biometrics/

Firmino, R. J. (2017). Securitização, vigilância e territorialização em espaços públicos na cidade neoliberal. *Risco Revista de Pesquisa Em Arquitetura e Urbanismo (Online)*, *15*(1), 23–35. https://doi.org/10.11606/issn.1984-4506.v15i1p23-35

Goffman, E. (1986). *Frame analysis: An essay on the organization of experience* (Northeastern

University Press). Northeastern University Press.

Goujard, C. (2022, September 20). Europe edges closer to a ban on facial recognition. *Politico*. https://www.politico.eu/article/europe-edges-closer-to-a-ban-on-facial-recognition/

Green, B. (2019). *The smart enough city: Putting technology in its place to reclaim our urban future*. The MIT Press. https://doi.org/10.7551/mitpress/11555.001.0001

Greenfield, A. (2013). *Against the smart city* (Kindle edition). Do projects.

Grossi, G., & Pianezzi, D. (2017). Smart cities: Utopia or neoliberal ideology? *Cities*, *69*, 79–85. https://doi.org/10.1016/j.cities.2017.07.012

Harvey, D. (2008). The right to the city. *New Left Review*, *53*.

Harvey, D. (2013). *Rebel cities: From the right to the city to the urban revolution* (Paperback edition). Verso.

Hayward, D. (1997). The privatised city: Urban infrastructure, planning and service provision in the era of privatisation. *Urban Policy and Research*, *15*(1), 55–64. https://doi.org/10.1080/08111149708551640

Heberling, W. B. (2022). Stop surveilling my genre!: On the biometric surveillance of (black trans) people. *Seattle Journal for Social Justice*, *20*(3), 861–914.

Hollands, R. G. (2015). Critical interventions into the corporate smart city. *Cambridge Journal of Regions, Economy and Society*, *8*(1), 61–77. https://doi.org/10.1093/cjres/rsu011

Instituto Defesa do Direito de Defesa & Data_Labe. (2022). *Por que eu? Como o racismo faz com que as pessoas negras sejam o perfil alvo das abordagens policiais* [Report]. https://iddd.org.br/por-que-eu-como-o-racismo-faz-com-que-as-pessoas-negras-sejam-o-perfil-alvo-das-abordagens-policiais/

Instituto Ethos. (2021). *Organizações pedem veto ao sistema de reconhecimento facial dos usuários do Metrô e CPTM*[Press release]. Instituto Ethos. https://www.ethos.org.br/cedoc/organizacoes-da-sociedade-civil-divulgam-carta-aberta-pedindo-veto-ao-sistema-de-reconhecimento-facial-dos-usuarios-do-metro-e-cptm/

Jacobs, J. (1961). *The death and life of great American cities*. Vintage Books.

Jasanoff, S., & Kim, S.-H. (2015). *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power*. University of Chicago Press. https://doi.org/10.7208/chicago/9780226276663.001.0001

Kak, A. (2020). *Regulating biometrics: Global approaches and urgent questions* (pp. 1–111) [Compendium]. AI Now Institute. https://ainowinstitute.org/regulatingbiometrics.html

La Rue, F. (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/23/40; pp. 1–23). United Nations. https://digitallibrary.un.org/record/756267

Laperruque, J. (2022). *Limiting face recognition surveillance: Progress and paths forward* [Report]. Center for Democracy and Technology. https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/

Lavits. (2022). *Sai da Minha Cara. Parlamentares de todas as regiões do Brasil apresentam projetos de lei pelo banimento do reconhecimento facial em espaços públicos* [Press release]. https://lavits.org/parlamentares-de-todas-as-regioes-do-brasil-apresentam-projetos-de-lei-pelo-banimento-do-reconhe

cimento-facial-em-espacos-publicos/

Lee-Morrison, L. (2019). *Portraits of automated facial recognition: On machinic ways of seeing the face*. transcript Verlag. https://doi.org/10.1515/9783839448465

Leslie, D. (2020). *Understanding bias in facial recognition technologies: An explainer* (pp. 1–49) [Report]. The Alan Turing Institute. https://doi.org/10.5281/ZENODO.4050457

Lobato, L. C., Francisco, P. A. P., & Hurel, L. M. (2020). *Videomonitoramento webreport* [Report]. Instituto Igarapé. https://igarape.org.br/videomonitoramento-webreport/

Lupi, A. L. . P. B. (2009). O Brasil é dualista?: Anotações sobre a vigência de normas internacionais no ordenamento brasileiro. *Revista de Informação Legislativa*, *46*(184), 29–45.

Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics*, *22*(9), 499–508. https://doi.org/10.1111/j.1467-8519.2008.00697.x

Malgieri, G., & Pasquale, F. A. (2022). From transparency to justification: Toward ex ante accountability for AI. *Brooklyn Law School, Legal Studies Paper No. 712*. https://doi.org/10.2139/ssrn.4099657

Mari, A. (2019, March 13). Brazilian retailer quizzed over facial recognition tech. *ZDNet*. https://www.zdnet.com/article/brazilian-retailer-quizzed-over-facial-recognition-tech/

Mari, A. (2022, April 21). São Paulo metro forced to halt facial recognition roll-out. *ZDNet*. https://www.zdnet.com/article/sao-paulo-metro-forced-to-halt-facial-recognition-roll-out/

Martins, L. (2022, June 20). Brazilian facial recognition ruling can set an important precedent for country-wide use. *Global Voices*. https://globalvoices.org/2022/06/20/brazilian-facial-recognition-ruling-can-set-an-important-precedent-for-country-wide-use/

Mejias, U. A., & Couldry, N. (2019). Datafication. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1428

Millet, T. (2020, October 18). A face in the crowd: Facial recognition technology and the value of anonymity. *Columbia Journal of Transnational Law Bulletin*. https://www.jtl.columbia.edu/bulletin-blog/a-face-in-the-crowd-facial-recognition-technology-and-the-value-of-anonymity

Mobilio, G. (2023). Your face is not new to me: Regulating the surveillance power of facial recognition technologies. *Internet Policy Review*, *12*(1). https://doi.org/10.14763/2023.1.1699

Morozov, E. (2013). *To save everything, click here: Technology, solutionism and the urge to fix problems that don't exist.* Allen Lane.

Morozov, E., & Bria, F. (2018). *Rethinking the smart city: Democratizing urban technology* (Report No. 5; City Series, pp. 1–54). Rosa Luxemburg Stifung, New York Office. https://www.rosalux.de/fileadmin/rls_uploads/pdfs/sonst_publikationen/rethinking_the_smart_city.pdf

Nascimento, L. (2022, June 25). Segurança durante São João tem atuação do CICC e tecnologia de reconhecimento facial. *A Notícia Digital*. https://anoticiadigital.com.br/noticia/39351/seguranca-durante-sao-joao-tem-atuacao-do-cicc-e-tecnologia-de-reconhecimento-facial

New York City. (2022, January 24). *Mayor Adams releases blueprint to end gun violence in New York City* [Press release]. The Official Website of the City of New York. https://www1.nyc.gov/office-of-the-mayor/news/045-22/mayor-adams-releases-blueprint-end-gun-violence-new-york-city#/0

Nunes, P. (2019). *Artigo: LLvantamento revela que 90,5% dos presos por monitoramento facial no Brasil*

são negros[Report]. Centro de Estudos de Segurança e da Cidadania. https://cesecseguranca.com.br/artigo/levantamento-revela-que-905-dos-presos-por-monitoramento-facial-no-brasil-sao-negros/

Osorio, L. M. (2019). Litígio estratégico em direitos humanos: Desafios e oportunidades para organizações litigantes. *Revista Direito e Práxis*, *10*(1), 571–592. https://doi.org/10.1590/2179-8966/2019/39337

Peets, L., Hansen, M., Jungyun Choi, S., Drake, M., & Ong, J. (2021, October 12). European Parliament votes in favor of banning the use of facial recognition in law enforcement. *Inside Privacy*. https://www.insideprivacy.com/artificial-intelligence/european-parliament-votes-in-favor-of-banning-the-use-of-facial-recognition-in-law-enforcement/

Poder360. (2020, May 7). STF derruba MP que compartilhava dados telefônicos com IBGE. *Poder360*. https://www.poder360.com.br/justica/stf-forma-maioria-para-suspender-mp-que-compartilha-dados-telefonicos-com-ibge/

Privacy International. (2022). *Legality, necessity and proportionality*. https://privacyinternational.org/our-demands/legality-necessity-and-proportionality

Pugliese, J. (2010). *Biometrics. Bodies, technologies, biopolitics* (1st ed.). Routledge. https://doi.org/10.4324/9780203849415

Purcell, M. (2014). Possible worlds: Henri Lefebvre and the right to the city. *Journal of Urban Affairs*, *36*(1), 141–154. https://doi.org/10.1111/juaf.12034

Ramiro, A., & Canto, M. (2022). *Global Information Society Watch 2021-2022: Digital futures for a post-pandemic world* (pp. 87–91) [Report]. Association for Progressive Communications (APC). https://www.giswatch.org/en/country-report/brazil-0

Reclaim Your Face. (2023). *Reclaim your face. Ban biometric mass surveillance*. https://reclaimyourface.eu/

Red en Defensa de los Derechos Digitales. (2020). *No nos vean la cara*. No Nos Vean La Cara. https://nonosveanlacara.r3d.mx/

Rees, M. (2022, June 1). Une "espèce d'institution poussiéreuse": Christian Estrosi (66 ans) s'attaque à la CNIL (44 ans). *Next INpact*. https://www.nextinpact.com/article/69293/une-espece-dinstitution-poussiereuse-christian-estrosi-66-ans-sattaque-a-cnil-44-ans

Reia, J., & Belli, L. (2021). *Smart cities no Brasil: Regulação, tecnologia e direitos*. Editora Letramento. https://doi.org/10.18130/p1me-mf66

Reia, J., & Cruz, L. (2023). Cidades inteligentes no Brasil: Conexões entre poder corporativo, direitos e engajamento cívico. *Cadernos Metrópole*, *25*(57), 467–490. https://doi.org/10.1590/2236-9996.2023-5705

Richardson, R. (2021). *Facial recognition in the public sector: The policy landscape* [Brief]. The German Marshall Fund. https://www.gmfus.org/news/facial-recognition-public-sector-policy-landscape

Romine, C. (2019, June 4). Facial recognition technology: Ensuring transparency in government use. *National Institute of Standards and Technology*. https://www.nist.gov/speech-testimony/facial-recognition-technology-ensuring-transparency-government-use

Sadowski, J., & Bendor, R. (2019). Selling smartness: Corporate narratives and the smart city as a sociotechnical imaginary. *Science, Technology, & Human Values*, *44*(3), 540–563. https://doi.org/10.1177/0162243918806061

Sadowski, J., & Pasquale, F. (2015). The spectrum of control: A social theory of the smart city. *First Monday*, *20*(7).

Sampaio, A. (2022). *Plataforma de observação elevada reforça a segurança no 'Rap In Cena World' na Capital* [Press release]. Secretaria de Segurança Pública do Estado do Rio Grande do Sul. https://ssp.rs.gov.br/plataforma-de-observacao-elevada-reforca-a-seguranca-no-rap-in-cena-world-na-capital

Santos, M. C. (2021, November 26). Prefeitura do Recife adia discussão sobre implantação de vigilância com reconhecimento facial. Marco Zero Conteúdo. *Macro Zero*. https://marcozero.org/prefeitura-do-recife-adia-discussao-sobre-implantacao-de-vigilancia-com-reconhecimento-facial/

Sem câmera na minha cara. (2022). *Sem câmera na minha cara*. https://www.semcameranaminhacara.meurecife.org.br

Silva, T. (2022). *Racismo algorítmico: Inteligência artificial e discriminação nas redes digitais*. Edições Sesc.

Smith, G. J. (2020). The politics of algorithmic governance in the black box city. *Big Data & Society*, *7*(2). https://doi.org/10.1177/2053951720933989

Snijder, M. (2015). *Biometrics, surveillance and privacy* (Report EUR 28389; pp. 1–19). European Commission. Joint Research Centre. Institute for the Protection and the Security of the Citizen. https://data.europa.eu/doi/10.2788/986068

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.

Soprana, P. (2019, June 2). ONG de defesa do consumidor questiona reconhecimento facial. *Folha de São Paulo*. https://www1.folha.uol.com.br/colunas/painelsa/2019/06/ong-de-defesa-do-consumidor-questiona-reconhecimento-facial.shtml

Souza, M., & Zanatta, R. (2021). The problem of automated facial recognition technologies in Brazil: Social countermovements and the new frontiers of fundamental rights. *Latin American Human Rights Studies*, *1*(2021). https://revistas.ufg.br/lahrs/article/view/69423

Superior Tribunal de Justiça. (2020). *Comissão entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal* [Press release]. Câmara dos Deputados. https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx

Tenório, A. (2022, June 22). Relógios espiões: Prefeitura do Recife recebe proposta milionária para PPP. *Blog do Jamildo*. https://jc.ne10.uol.com.br/colunas/jamildo/2022/06/15030205-relogios-espioes-prefeitura-do-recife-recebe-proposta-milionaria-para-ppp.html

Teofilo, D., Kurtz, L., Porto Jr., O., & Vieira, V. B. R. (2019). *Public civil action: IDEC vs. ViaQuatro* (IRIS' opinion, pp. 1–31) [Research paper]. Institute for Research on Internet and Society (IRIS). https://irisbh.com.br/en/publicacoes/public-civil-action-idec-vs-viaquatro-iris-opinion/

The Public Voice. (2009). *The Madrid Privacy Declaration: Global privacy standards for a global world* [Declaration]. https://thepublicvoice.org/madrid-declaration/

Tire Meu Rosto da Sua Mira. (n.d.). *Tire Meu Rosto da Sua Mira* [Campagne]. https://tiremeurostodasuamira.org.br/

International covenant on civil and political rights, (1966). https://www.ohchr.org/en/instruments-

mechanisms/instruments/international-covenant-civil-and-political-rights.

United Nations. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25; pp. 1–20). Convention on the rights of the child. https://criancaeconsumo.org.br/wp-content/uploads/2021/04/general-comment-n-25-2021.pdf

United Nations Human Rights Committee. (2020). *General comment no. 37 (2020) on the right of peaceful assembly (article 21)* (CCPR/C/GC/37; pp. 1–18). International Covenant on Civil and Political Rights. https://digitallibrary.un.org/record/3884725

van de Waerdt, P. J. (2020). Information asymmetries: Recognizing the limits of the GDPR on the data-driven market. *Computer Law & Security Review*, *38*, 105436. https://doi.org/10.1016/j.clsr.2020.105436

van der Ploeg, I. (2005). *The machine-readable body: Essays on biometrics and the informatization of the body*. Shaker Publ.

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Venturini, J. (2020, February 21). La sociedad exige explicaciones sobre la implementación de sistemas de reconocimiento facial en América Latina. *Derechos Digitales América Latina*. https://www.derechosdigitales.org/14207/la-sociedad-exige-explicaciones-sobre-la-implementacion-de-sistemas-de-reconocimiento-facial-en-america-latina/

Venturini, J., & Garay, V. (2021). *Reconocimiento facial en América Latina: Tendencias en la implementación de una tecnología perversa* (pp. 1–24). Al Sur. https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf

Vicentin, T. (2021, March 12). Doria vetoes facial recognition in the São Paulo Metro. *Olhar Digital*. https://web.archive.org/web/20210319092404/https://olhardigital.com.br/en/2021/03/12/pro/doria-veta-reconhecimento-facial-no-metro-de-sao-paulo/

Vida, M. (2022, August 5). Advocacy groups in the Americas focus on tackling rising surveillance technology. *Global Voices*. https://advox.globalvoices.org/2022/08/05/advocacy-groups-in-the-americas-focus-on-tackling-rising-surveillance-technology/

Vincent, J. (2020, August 18). NYPD used facial recognition to track down Black Lives Matter activist. *The Verge*. https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram

Voorwinden, A. (2021). The privatised city: Technology and public-private partnerships in the smart city. *Law, Innovation and Technology*, *13*(2), 439–463. https://doi.org/10.1080/17579961.2021.1977213

Wiig, A. (2015). IBM's smart city as techno-utopian policy mobility. *City*, *19*(2–3), 258–273. https://doi.org/10.1080/13604813.2015.1016275

Williams, M. C. (2003). Words, images, enemies: Securitization and international politics. *International Studies Quarterly*, *47*(4), 511–531. https://doi.org/10.1046/j.0020-8833.2003.00277.x

Published by
Alexander von Humboldt Institute for Internet and Society

in cooperation with
CREATe
cnrs centre internet et societe
R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya
University of Tartu Johan Skytte Institute of Political Studies