iUS PUBLICUM NETWORK REVIEW
www.ius-publicum.com

FACIAL RECOGNITION AND PUBLIC SECURITY IN THE CITY OF RIO DE JANEIRO: A CRITICAL ANALYSIS IN THE PERSPECTIVE OF FEDERATIVE COMPETENCES AND FUNDAMENTAL RIGHTS

Eleonora MESQUITA CEIA - Chiara SPADACCINI DE TEFFÉ[1]

INDEX

[1] E. Mesquita Ceia is Doctor of Law at Saarland University, Germany. Professor of Constitutional Law at Ibmec University Center, Brazil. E-mail: emceia@gmail.com. C. Spadaccini de Teffè is Doctor of Civil Law at the Rio de Janeiro State University (UERJ), Brazil. Research and publishing coordinator of the graduate program in Digital Law of ITS Rio (Institute for Technology & Society), in partnership with UERJ-CEPED. Professor of Civil Law and Law and Technology at Ibmec University Center, Brazil. Lawyer. E-mail: chiaradeteffe@gmail.com.

1. INTRODUCTION

Since the first half of the 20th century, Brazil has experienced a rapid and poorly controlled urbanization process, which culminated in the emergence of megacities. They include São Paulo and Rio de Janeiro with more than 12 and 6 million inhabitants respectively[2]. Most Brazilian cities face pressures and demands regarding housing, public health, transport, environmental protection, poverty, and violence. Searching for solutions and answers to these issues, cities engage in projects and initiatives of innovation and mutual cooperation based on the notions of "sustainable cities", "solidarity cities" and "smart cities"[3].

Smart cities are those that implement new technologies to conduct and monitor urban life, with the purpose to solve their major challenges, such as urban violence. In fact, public security is identified as the third main problem of Brazilian cities, after health and education, in line with opinion polls carried out during the 2020 municipal elections[4].

Therefore, new technologies are more and more being used in combating crime by local authorities. One of these technologies is facial recognition, whose use for public security is controversial: due to some technical failures and false positives, it has reinforced discrimination against particular social groups and brought a series of questions concerning

[2] Instituto Brasileiro de Geografia e Estatística, *Cidades e Estados* (2020), https://www.ibge.gov.br/cidades-e-estados.

[3] R. HIRSCHL, *City, State*: *constitutionalism and the megacity*, 2020.

[4] F. VASCONCELLOS, *Em ano de pandemia, saúde bate recorde como principal problema apontado pelos eleitores nas capitais, segundo o Ibope*. G1 (Oct. 9) 2020, https://g1.globo.com/politica/eleicoes/2020/eleicao-em-numeros/noticia/2020/10/09/em-ano-de-pandemia-saude-bate-recorde-como-principal-problema-apontado-pelos-eleitores-nas-capitais-segundo-o-ibope.ghtml.

the protection of fundamental rights. It is also understood by many as an instrument of political and social control.

In this context, different institutions around the world, including some Brazilian organizations, presented in June 2021 an "open letter calling for a global ban on uses of facial recognition and remote biometric recognition technologies that enable mass and discriminatory surveillance"[5]. Up to the present time, in Brazil, the use of these technologies for public security purposes has not been yet regulated by a specific law, which should address their application, as well as the respective data treatment.

According to Brazilian General Data Protection Law – Lei Geral de Proteção de Dados, LGPD, in Portuguese – (Law n. 13,709/2018), the processing of personal data that is done exclusively for purposes of public security, national defense, state security, or activities of investigation and prosecution of criminal offenses should be regulated by specific legislation. In practice, however, the local authorities did not wait for the due regulation. In 2019, at least 37 Brazilian cities[6] were already making use of facial recognition technologies in the fight against urban violence. In addition, there are state and municipal laws in force which regulate facial recognition practices and draft bills on the same subject.

Considering the constitutional autonomy of cities under Brazilian law, the paper aims to analyze the main controversies on facial recognition technologies for public security purposes, namely the potential conflicts of competence between federated entities and the risks of violations of minorities' fundamental rights. To reach its goal and answer its central problems, the paper uses bibliographical and documentary research methods. As a case study, the paper assesses the experience of the city of Rio de Janeiro, where facial recognition has

[5] Accessnow, *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance*, 2021, https://www.accessnow.org/ban-biometric-surveillance/.

[6] Instituto Igarapé, *Tecnologias policiais no contexto brasileiro*, 2020, https://igarape.org.br/tecnologias-policiais-no-contexto-brasileiro/.

been increasingly implemented since the 2019 Carnival. It is organized as follows: in the next section, the principles, purposes, and risks of the use of facial recognition technology in smart cities will be examined, particularly regarding the provisions of the Brazilian General Data Protection Law. Subsequently, the analysis will turn to the legislative power division system among federative entities in Brazil, on the matter of facial recognition technology for public security purposes, with emphasis placed on the autonomous status of cities under the Brazilian Constitution. After, the recent developments in the application of facial recognition technology for public security purposes in Rio de Janeiro will be discussed.

2. FACIAL RECOGNITION TOOLS IN SMART CITIES: HOW TO PROTECT PERSONAL DATA AND PROMOTE PUBLIC SECURITY?

Technology expands the reach of human capabilities by accurately recording geographic locations, personal preferences, sensitive data, and people with whom we interact. Therefore, it is necessary to define, as well as a specific legal basis for the processing of data, when, where, how and for what purposes personal information may be processed. In addition, good practices, restrictions, and safeguards for the human person in all data-related activity must be established, bearing in mind the strategic, financial, and commercial values they hold. The crossings and inferences obtained from the treatment of personal information have significantly boosted sectors related to the economy, the market, and security (public and private), with an increase, as a result, in surveillance structures and data extraction.

The use of big data and artificial intelligence in the activities of the State is in line with a discourse on expanding the efficiency and digitization of Public Administration. It is understood that large databases accessible to a greater number of institutions allow an increase in the accuracy of diagnoses, planning, and the synergy of activities. The expansion of the State's capacity to handle information increases its power in front of citizens and asserts the asymmetry between the parties. In the field of public security, such tools make more precise and invasive identification, tracking, and surveillance mechanisms used both preventively and for criminal prosecution.

Systems endowed with Artificial Intelligence[7] have applications in various activities aimed at security and defense, for example, in platforms and applications related to smart cities and in facial recognition and intelligent policing structures. Some solutions allow the identification of objects and people in images, as well as audio analysis applications demonstrate the ability to detect, for example, the sounds of gunshots, car crashes, or agglomerations, with automatic alerts being sent to the authorities responsible.

In the current context, it can be seen how difficult it is to leave structures established by major technology agents and by the States, either because of the usefulness and quality of the services offered or because of their essentiality for the exercise of rights and duties as citizens. This can become even more difficult if people start to depend on the networks both to make a large part of their decisions and to use goods and services. The traceability of the person has been increasingly sophisticated, including the sharing of data between agents for control and security purposes in public and private spheres, such as airports, places of major events, and areas identified as demanding greater attention.

This dynamic is analyzed by Shoshana Zuboff[8], who developed the concept of surveillance capitalism: a framework that considers human experience as raw material, free, and available for hidden business practices of extracting, predicting, and selling data. By offering seemingly free services to billions of people, the providers responsible for these services monitor user behavior, obtaining surprising details, inferring, and even shaping behavior. Surveillance capitalists discovered that they could process data not only to know our behavior but also to shape it. This has become an economic imperative. It was no longer enough to automate the flow of information about us; the goal became to automate us. This

[7] Brasil, *Ordinance GM No. 4,617. Establishes the Brazilian Strategy for Artificial Intelligence and its thematic axes*, 2021, https://www.in.gov.br/en/web/dou/-/portaria-gm-n-4.617-de-6-de-abril-de-2021-*-313212172.

[8] S. ZUBOFF, *The Age of Surveillance Capitalism*: *The Fight for a Human Future at the New Frontier of Power*, 2019.

would be another phase in the evolution of capitalism: it would aim at exploiting behavioral predictions secretly derived from the surveillance imposed on users.[9]

In this way, almost every product or service that begins with the word "smart" or "custom", every internet-enabled device and every "digital assistant" represent part of the supply chain of behavioral data that is used to predict our futures in a surveillance economy. While some of this data is applied to service improvement, much of it feeds advanced processes known as machine intelligence and is important for building predictive products that anticipate what you will do now, soon, and later.

These prediction products are traded in a new kind of marketplace that Zuboff calls *behavioral futures markets*.[10] In this scenario, the agents of surveillance capitalism would have enriched immensely from these commercial operations, as many companies would be willing to bet on our future behavior. She claims that knowledge, authority, and power rest with surveillance capital, for which we are only "natural human resources".

Then, what Frank Pasquale called the "one way mirror"[11] was created, in which the personal data of citizens have been processed by governments and tech giants so that such agents know everything about people, while they do nothing or little about the first two. Your predictions are about us, but not for us. All this happens through constant and massive

[9] S. ZUBOFF, *'Surveillance capitalism' has gone rogue. We must curb its excesses*, in *The Washington Post*, Jan. 24, 2019, https://www.washingtonpost.com/opinions/surveillance-capitalism-has-gone-rogue-we-must-curb-its-excesses/2019/01/24/be463f48-1ffa-11e9-9145-3f74070bbdb9_story.html.

[10] S. ZUBOFF, *'The goal is to automate us': welcome to the age of surveillance capitalism*, in *The Guardian*, Jan. 20, 2019, https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.

[11] "We do not live in a peaceable kingdom of private walled gardens; the contemporary world more closely resembles a one-way mirror. Important corporate actors have unprecedented knowledge of the minutiae of our daily lives, while we know little to nothing about how they use this knowledge to influence the important decisions that we—and they—make." See F. PASQUALE, *The black box society* (2015), at 9.

monitoring and vigilance about each step of our life, which leads to surveillance capitalism, whose main consequence is the consolidation of a surveillance society as well.[12]

In this environment, the Brazilian General Data Protection Law (Law No. 13,709/18 – *Lei Geral de Proteção de Dados*: LGPD) entered into force in the second half of 2020. Then, in February 2022, Constitutional Amendment No. 115 was enacted, which amended the 1988 Federal Constitution to include the protection of personal data among fundamental rights. Therefore, this protection explicitly became an indelible clause, being guaranteed to individuals and groups.

Considering the rules on this subject, the protection of personal data in Brazil is understood as a way of a) containing the harmful effects of surveillance capitalism and the manipulations arising from large platforms; b) removing the risks that certain applications with algorithms can pose to fundamental freedoms; and c) providing assurances to people in the face of opacity and lack of accountability of many political and economic structures.[13]

The LGPD (Brazilian Data Protection Law) brought a wide range of principles for the protection of personal data and mandatory compliance rules for all persons involved in the processing of personal data. It presents a normative structure that imposes that both a natural person and a legal entity of either public or private law conform to its commands.

[12] "The corporate strategists and governmental authorities of the future will deploy their massive resources to keep their one-way mirrors in place; the advantages conferred upon them by Big Data technologies are too great to give up without a fight. But black boxes are a signal that information imbalances have gone too far. We have come to rely on the titans of reputation, search, and finance to help us make sense of the world; it is time for policymakers to help us make sense of the sensemakers." *Id.*, at 17.

[13] "As more and more data flows from your body and brain to the smart machines via the biometric sensors, it will become easy for corporations and government agencies to know you, manipulate you, and make decisions on your behalf. Even more importantly, they could decipher the deep mechanisms of all bodies and brains, and thereby gain the power to engineer life. If we want to prevent a small elite from monopolizing such godlike powers, and if we want to prevent humankind from splitting into biological castes, the key question is: who owns the data? Does the data about my DNA, my brain and my life belong to me, to the government, to a corporation, or to the human collective?" See Y. NOAH HARARI, *21 Lessons for the 21st Century*, E-book, 2018.

Considering the importance of information for power structures and the asymmetric structures often existing between controllers and data subjects, the LGPD seeks to guarantee legal and technical instruments that increase the power and control of the natural person over their data (understood as information relating to an identified or identifiable natural person).

Therefore, there are requirements such as, for example, the documental record of informational flows, contractual amendments that deal with the processing of personal data, updating of privacy policies and terms of use, expansion of the areas of information security and data protection (with the establishment of a data protection officer) and minimization of the risk of unauthorized access to data by third parties or unauthorized persons.

In article 5, item II, the LGPD details which data is considered sensitive, such as those dealing with racial or ethnic origin, religious conviction, political opinion, and membership in a union or organization of a religious, philosophical, or political nature. Data relating to health or sex life and genetic or biometric data are also sensitive. The expanded protection of sensitive data in legal norms represents the realization of the principles of free development of the personality and non-discrimination.[14] It is particularly relevant for guaranteeing the fundamental rights and freedoms of data subjects. This is because, due to the quality and nature of the information sensitive data brings, its treatment or possible leakage may generate significant risks to human beings and may be a source of prejudice and unlawful or abusive discrimination.

Thus, to avoid adverse effects for the data subject, the processing of sensitive data for legitimate purposes must be accompanied by adequate safeguards, which consider the

[14] The principle of non-discrimination – a relevant foundation for the expanded protection of sensitive data – appears in the LGPD twice: first, in item IX of article 6, which defines it as the "impossibility of carrying out the processing for unlawful or abusive discriminatory purposes", and in the second, paragraph 2 of Article 20, which provides for the possibility for the National Data Protection Authority to carry out an audit to verify discriminatory aspects in the automated processing of personal data. See A. FRAZÃO, *Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de dados*, in Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro v. 1, Gustavo Tepedino, Ana Frazão & Milena Donato Oliva org., 2019.

risks at stake and the rights to be protected, as specific and more restrictive legal bases for its treatment (such as Article 11 of the LGPD); obligation of professional secrecy; risk analysis; data protection impact assessment [15]; and organizational and technical security measures. Actions aligned with the privacy by design[16] logic — privacy and data protection must be considered from the beginning and throughout the life cycle of the project, system, service, product or process, that is, companies and organizations are encouraged to implement technical and organizational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from

[15] The LGPD uses the expression "relatório de impacto à proteção de dados pessoais" (impact report) instead of "impact assessment". However, considering that "Data Protection Impact Assessment" (DPIA) is more common in laws of data protection, we chose to translate the term as "data protection impact assessment". Although in Brazil developing a data protection impact assessment is not a mandatory rule for the processing of sensitive data, in addition to being good practice and instrument of compliance and accountability, it may be required by the National Data Protection Authority (article 38, LGPD). The impact assessment can be defined as documentation from the controller that contains the description concerning the proceedings of the personal data processing that could pose risks to civil liberties and fundamental rights, as well as measures, safeguards, and mechanisms to mitigate said risk. The document must be prepared before the institution starts processing data.

[16] A. CAVOUKIAN, *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*, 2012, http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf. A. CAVOUKIAN, *Privacy by Design: The 7 Foundational Principles*, 2010, https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/. European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en. In turn, article 46 of LGPD states: "Processing agents shall adopt security, technical and administrative measures able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing. §1 The national authority may provide minimum technical standards to make the provisions of the lead sentence of this article applicable, taking into account the nature of the processed information, the specific characteristics of the processing and the current state of technology, especially in the case of sensitive personal data, as well as the principles provided in the lead sentence of article 6 of this Law. §2 The measures mentioned in the lead sentence of this article shall be complied with as from the conception phase of the product or service until its execution". And article 49 of LGPD declares: "The systems used for processing personal data shall be structured in order to meet the security requirements, standards of good practices and governance, general principles provided in this Law and other regulatory rules". See R. LEMOS *ET AL*, *Brazilian General Data Protection Law* (2020), https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.

the start[17] — must always be taken in the development of surveillance and control technologies, including prior impact assessments and technical and organizational accountability measures.

In surveillance technologies, such as facial recognition, there is usually significant processing of biometric data, because they offer resources to identify and authenticate individuals reliably and quickly, based on a set of recognizable and verifiable data, which are unique and specific information about their holders. The body becomes the password, the unique and exclusive means of individualizing the person.

Biometrics is the science of establishing someone's identity by measuring and analyzing their physiological (can be either morphological or biological) or behavioral attributes.[18] In the first case, examples are fingerprints, iris recognition, retinal identification, the face's shape, dental arch, the hand's shape, and vein pattern. DNA, blood, saliva, or urine may be used by medical teams and police forensics. Physiological measures often offer the benefit of remaining more stable throughout an individual's lifetime.

In the second case (behavioral measurements), it is possible to mention the way the person types, how he walks, characteristic gestures, signature dynamics (speed of pen movement, accelerations, pressure, and inclination), the height that the individual usually holds the cell phone, the shape how he moves the computer mouse, the pressure he exerts on the keyboard or screen, and even how he corrects the words. It is understood that the concept of biometric data should be extracted both from studies published by specific groups[19] and

[17] European Commission, *What does data protection 'by design' and 'by default' mean?*, 2021, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en.

[18] See T. GROUP, *What is biometrics? Authentication & identification*, 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics.

[19] European Union, *Article 29 Data Protection Working Party. Working document on biometrics*, 2003, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf. European Union, *Article 29 Data Protection Working Party. Opinion 02/2012 on facial recognition in online and mobile*

from foreign standards.[20] Based on the General Data Protection Regulation[21], it is possible to understand biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

As technology advances, the use of human characteristics as information will continue to present challenges to notions of privacy and the protection of personal data. The reliability of biometric data and systems has increased. Biometrics is generally considered strong and valuable for authentication systems. However, it is necessary to understand ways to better protect such data and avoid disproportionate processing. In addition to issues related to public security, criminal prosecution, and terrorism prevention, in recent times, there has been a growing debate about the establishment of biometric databases for the identification of citizens in identity validation processes and for granting financial benefits from the government.

Article 4 of the LGPD presents hypotheses in which this Law does not apply directly to the processing of personal data. The provision is particularly relevant for the present study

services (2012), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf. European Union, *Article 29 Data Protection Working Party. Opinion 3/2012 on developments in biometric technologies* (2012), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

[20] The California Consumer Privacy Act (CCPA) understands biometric information as "(…) an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information". See TERMSFEED, *Biometrics and the CCPA*, 2021, https://www.termsfeed.com/blog/ccpa-biometrics/.

[21] Eur-Lex, *Regulation (EU) 2016/679 of the European Parliament and of the Council*, 2016, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679.

since it exempts from the direct application of the LGPD the data processing done exclusively for purposes of a) public security; b) national defense; c) State security; or d) activities of investigation and prosecution of criminal offenses (article 4, III, of the LGPD). Even if the processed data is sensitive, if the situation is within the scope of article 4, III, as is the application of facial recognition technology for public security purposes, the LGPD will not be applied.

Paragraph 1 of article 4 of the LGPD provides that the processing of personal data established in item III shall be governed by *specific legislation*, which shall provide proportional and strictly necessary measures for fulfilling the public interest, subject to due legal process, the general principles of protection and the rights of the data subjects as provided in this Law. It is understood that such legislation must be of federal scope and present the general provisions on the matter, to directly guide the other entities. In addition, the National Data Protection Authority shall issue technical opinions or recommendations regarding the exceptions provided in item III of the lead sentence of this article and shall request of the responsible parties a data protection impact assessment (§3). This is a case of mandatory reporting, which highlights the protective nature of the rule.

Given the legal provision, a commission of jurists was created by the president of the Chamber at the time to prepare a draft of the specific legislation, which was released in November 2020 and became known as the "Criminal LGPD".[22] The text sought to provide specific and secure parameters for personal data processing operations within the scope of public security and criminal prosecution activities, balancing both the protection of the data subject against abuses and the access of authorities to the full potential of tools and platforms for public security and investigations.

[22] Brasil, *Explanatory Memorandum: initial text to compose the draft bill for Data Protection for public security and criminal prosecution*, 2020, https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf.

When published, this specific legislation will have a profound impact on public structures that make use of facial recognition and will be relevant to promoting a homogeneous and federal treatment of the subject. In Brazil, so far, there is significant use of facial recognition by both the public and private sectors, with little regulation and some state[23] and municipal norms[24]. In the selected cases, there is no detailed analysis on the part

[23] Federal District - Law No. 6,712/20 provides for the use of facial recognition technology in public security: "Article 2 For the purposes of this Law, the following are considered: I – Facial Recognition Technology: the technology that analyzes facial characteristics used for the exclusive personal identification of individuals in static images or videos; II - continuous surveillance: the use of FRT to engage in a continuous effort to track the physical movements of an identified individual in one or more public places where these movements occur, for a period of time exceeding 72 hours, either in real time or through the application of this technology to historical records. Article 3 The use of FRT for continuous surveillance of an individual or group of individuals is prohibited, under any circumstances. Article 4 The use of FRT in public security is restricted to public equipment located in public spaces. Single paragraph. In places where images are captured with FRT, visible plaques containing the respective information must be attached." Free translation of the original text in Portuguese.

There are also state laws on the application of facial recognition in football stadiums: a) Law No. 21,737/15 - State of Minas Gerais – "Article 4 The installation of facial recognition systems in football stadiums located in the State is authorized." b) Law No. 8,113/19 - State of Alagoas – "Article 5 The installation of facial recognition systems in stadiums located in the State is authorized." c) Law No. 16,873/19 - provides for the sale and consumption of alcoholic beverages in stadiums and sports arenas in the state of Ceará and defines penalties for non-compliance with the marketing rules. "Article 5 It is forbidden to enter stadiums and sports arenas for people carrying any type of drink. Single paragraph. Stadiums and sports arenas, which will be subject to the Public-Private Partnership or Concession, must have video surveillance equipment with facial recognition associated with the turnstiles, as well as the registration of fans". Free translation of the original text in Portuguese.

[24] Law No. 2,474, of July 3, 2019 - Manaus - provides for the incorporation of the Facial Biometric Identification System, in the inspection of the use of gratuity and half-ticket, in Collective Urban Passenger Transport through the Electronic Ticketing System, in the city of Manaus and other measures. See Prefeitura Manaus, *Prefeitura inicia instalação de câmeras de monitoramento para acelerar respostas à população* (2021), https://www.manaus.am.gov.br/noticia/prefeitura-inicia-instalacao-de-cameras-de-monitoramento-para-acelerar-respostas-a-populacao/.

Law No. 15,405 of April 9, 2019 – Creates and defines the Municipal Video Monitoring Policy of Curitiba and other measures. "Article 1 The Curitiba Municipal Video Monitoring Policy – is created to standardize the monitoring by images of public roads, including public places, areas, environments, vehicles, equipment, and public events in the Municipality." Free translation of the original text in Portuguese. It is observed that, in Curitiba, in an article published in 2020, it was stated that: "Almost 500 new video surveillance cameras will be installed in strategic points of the city by the end of the year. They are high-resolution full HD equipment that includes cameras with facial recognition and with license plate recognition, which are added to the approximately 700 cameras that already exist in streets and tube stations. The project, which marks the launch of the Digital Wall, is a partnership between the city Hall and the Institute of Smart Cities /*Instituto das Cidades Inteligentes* (ICI)". Free translation of the original text in Portuguese. See Prefeitura Curitiba, *Cidade terá câmeras com reconhecimento facial em pontos*

of the legislator about the purpose, proportionality, and the real need for the use of facial recognition and the processing of sensitive data.

The use of facial recognition technologies brings several controversies. Around the world, cities and private companies have been widely debating its application, limits, and eventual ban. Greater technology improvement and the development of specific legislation are also sought. In addition to questions relating to the protection of fundamental freedoms, there is a high concern that facial recognition systems are inaccurate and perpetuate racial discrimination. The relationship developed between facial recognition, public security, and policing creates deep concerns regarding the risks of a broad and general application of such a tool.

Differences in the accuracy rate in the recognition of people of different races (the false positives being more common in the face of black people), genders and ages have already been demonstrated, and the use of this technology may lead to possible scenarios of illicit or abusive discrimination. The bias is especially aggravated in the field of public security, due to historical relations of inequality and discrimination against socially vulnerable populations. Without proper care, algorithms can deepen inequalities and cause coercive measures to be taken wrongly. Given the expansion of this technology and the risks it can generate, it is necessary to promote public, multi-sectorial and informed debate on where, how, and when to apply it.[25]

estratégicos, 2020, https://servidor.curitiba.pr.gov.br/noticias/cidade-tera-cameras-com-reconhecimento-facial-em-pontos-estrategicos/56463.

[25] An interesting example is a test conducted by the US Civil Liberties Association (ACLU). The association conducted a "test with a facial recognition program used by Amazon called 'Rekognition'. Among deputies and senators, the system "identified" 28 representatives as criminals. The tool linked the politicians' images to photos in databases of people arrested. In addition to the error in recognition, the association indicated a discriminatory functioning in the case of black people. About 40% of politicians falsely identified as criminals belonged to this segment, although it represents only 20% of the members of Congress whose photos were submitted to the test". Free translation of the original text in Portuguese. See J. VALENTE, *Erros em sistema de reconhecimento facial geram polêmica nos EUA*. Agência brasil, July 28, 2018,

Undoubtedly, the use of facial recognition tools, in the state of the art in which they are found, is surrounded by controversies for affecting several issues related to fundamental freedoms and equality. However, completely prohibiting its use can undermine collective and public interest issues, such as those concerning the prevention of terrorism and the containment of urban violence. Therefore, measures such as regulatory impact analysis report, data protection impact assessment, prior judicial authorization, restrictions on the imposition of real-time surveillance and constant investment in technology improvement are suggested.

In April 2021, the European Commission unveiled a new proposal for an EU regulatory framework on artificial intelligence, which has been intensely debated by researchers worldwide:

The proposal sets harmonised rules for the development, placement on the market and use of AI systems in the Union following a proportionate risk-based approach. (…) Certain particularly harmful AI practices are prohibited as contravening Union values, while specific restrictions and safeguards are proposed in relation to certain uses of remote biometric identification systems for the purpose of law enforcement. The proposal lays down a solid risk methodology to define "high-risk" AI systems that pose significant risks to the health and safety or fundamental rights of persons. Those AI systems will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures before those systems can be placed on the Union market. Predictable, proportionate, and clear obligations are also placed on providers and users of those systems to ensure safety and respect of existing legislation protecting fundamental rights throughout the whole AI systems' lifecycle. (…) Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. This is particularly relevant when it comes to age, ethnicity, sex or

https://agenciabrasil.ebc.com.br/internacional/noticia/2018-07/erros-em-sistema-de-reconhecimento-facial-geram-polemica-nos-eua.

disabilities. Therefore, 'real-time' and 'post' remote biometric identification systems should be classified as high-risk. In view of the risks that they pose, both types of remote biometric identification systems should be subject to specific requirements on logging capabilities and human oversight.[26]

Facial recognition technologies (FRTs) are used by private or public actors for verification, identification, and categorization purposes. The proposal introduces rules for *biometric* technologies and differentiates them according to their risk levels and characteristics. According to the text, many FRTs would be considered "high risk" systems that would be prohibited or need to comply with strict requirements (being permitted only for specific exceptions). The use of real-time facial recognition[27] systems in publicly accessible spaces for the purpose of law enforcement would be prohibited unless Member States choose to authorize[28] them for important public security reasons and the appropriate judicial or administrative authorizations are granted.[29] Taking into account the text of the

[26] EUR-Lex, *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*. *COM/2021/206 final* (2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[27] For the purpose of this Regulation, the following definitions apply: "(36)'remote biometric identification system' means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified; (37)''real-time" remote biometric identification system' means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention. (38)''post' remote biometric identification system' means a remote biometric identification system other than a 'real-time' remote biometric identification system;". *Id*., at 42.

[28] "(22) Furthermore, it is appropriate to provide, within the exhaustive framework set by this Regulation that such use in the territory of a Member State in accordance with this Regulation should only be possible where and in as far as the Member State in question has decided to expressly provide for the possibility to authorise such use in its detailed rules of national law. Consequently, Member States remain free under this Regulation not to provide for such a possibility at all or to only provide for such a possibility in respect of some of the objectives capable of justifying authorised use identified in this Regulation." *Id*., at 22-23.

[29] "The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is considered particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling

proposal, Madiega and Mildebrath[30] point out with concern that a range of facial recognition technologies used for purposes other than law enforcement (e.g., border control, market places, public transportation and schools) would be permitted, but subject to a conformity assessment and compliance with some safety requirements, before entering the EU market.

In June 2021 the European data protection board (EDPB) and the European Data Protection Supervisor (EDPS) published the Joint Opinion5/2021 on the proposal for an AI Regulation.[31] The EDPB and EDPS stressed:

Remote biometric identification of individuals in publicly accessible spaces poses a high-risk of intrusion into individuals' private lives, with severe effects on the populations' expectation of being anonymous in public spaces. For these reasons, the EDPB and the EDPS call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context. A ban is equally recommended on AI systems categorizing individuals from biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination under Article 21 of the Charter. Furthermore, the EDPB and the EDPS

of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in 'real-time' carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities." See EUR-Lex, *supra* note 27.

[30] T. ANDRÉ MADIEGA, H. ALEXANDER MILDEBRATH, *Regulating facial recognition in the EU*, 2021, https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)698021.

[31] European Data Protection Board, *EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other use of AI that can lead to unfair discrimination*, 2021, https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en.

consider that the use of AI to infer emotions of a natural person is highly undesirable and should be prohibited.[32]

At the same time, the Council of Europe released Guidelines on facial recognition, which provide a set of reference measures that governments, facial recognition systems developers, manufacturers, service providers, and user organizations should apply to ensure that this technology does not adversely affect the human dignity.[33]

Later, the European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters highlighted that:

(...) strongly believes that the deployment of facial recognition systems by law enforcement should be limited to clearly warranted purposes in full respect of the principles of proportionality and necessity and the applicable law; reaffirms that as a minimum, the use of facial recognition technology must comply with the requirements of data minimisation, data accuracy, storage limitation, data security and accountability, as well as being lawful, fair and transparent, and following a specific, explicit and legitimate purpose that is clearly defined in Member State or Union law; is of the opinion verification and authentication systems can only continue to be deployed and used successfully if their adverse effects can be mitigated and the above criteria fulfilled; 26. Calls, furthermore, for the permanent prohibition of the use of automated analysis and/or recognition in publicly accessible spaces of other human features, such as gait, fingerprints, DNA, voice, and other biometric and behavioural signals; 27. Calls, however, for a moratorium on the deployment of facial

[32] European Data Protection Board, *EDPB-EDPS 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)* (2021) at 2-3, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

[33] Council of Europe, *Guidelines on facial recognition* (2021), https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html.

recognition systems for law enforcement purposes that have the function of identification, unless strictly used for the purpose of identification of victims of crime, until the technical standards can be considered fully fundamental rights compliant, results derived are non-biased and non-discriminatory, the legal framework provides strict safeguards against misuse and strict democratic control and oversight, and there is empirical evidence of the necessity and proportionality for the deployment of such technologies; notes that where the above criteria are not fulfilled, the systems should not be used or deployed; 28. Expresses its great concern over the use of private facial recognition databases by law enforcement actors and intelligence services, such as Clearview AI (...).[34]

Outside Europe, we find binding rules applicable to FRTs even in countries that have a high concern about public safety, such as the USA and China. Policy and lawmakers around the world have the opportunity to discuss – in multilateral and bilateral contexts – how to put in place more or less strict controls on the use of these systems. Considering foreign experiences and current debates, Brazil should follow the most advanced AI strategies to develop laws that effectively protect human rights.

It is known that with the expansion of facial recognition for public security purposes, the State will be able to track its citizens, verify which places they frequent, and maintain databases with information on participants in political demonstrations or people with different political opinions. The collection of images of faces may end up being carried out without the effective knowledge of individuals, opening the door for collective, opaque, and non-transparent biometric surveillance. This imposes necessary care with the observance of legal norms and codes of ethics, being relevant also the continuous supervision and accountability by the agents responsible for the technology and its use. In fact, "political

[34] European Parliament, *Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters* (2021), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html.

manifestations, social interaction, basic freedom and the equal treatment of individuals will remain in check if specific parameters for the use of such technology are not drawn up."[35]

3. THE AUTONOMY AND RELEVANCE OF CITIES IN BRAZILIAN FEDERATION: A STUDY OF THE LEGISLATIVE POWERS ON THE TECHNOLOGIES OF FACIAL RECOGNITION APPLIED TO PUBLIC SECURITY

The Brazilian Federation comprises the Union, the states, the municipalities, and the Federal District, all of them endowed with autonomy, as stated in article 18 of the Constitution. It adopts the cooperative model[36] that lay down, together with matters of exclusive and private competences of the Union, areas in which the federative entities act and legislate side by side as follows: the Union enacts general rules, principles, and standards, whereas the subnational units (states, municipalities, and the Federal District) legislate and execute public policies according to the federal guidelines defined by the Union.

Cooperative federalism has a democratic nature. In Brazil, it is to primarily support the equalization of structural inequalities in the Federation. For instance, the Constitution of 1988 provides for mechanisms of cooperation among the federal entities, within the wide range of common administrative powers, which embrace the fundamental objectives of the Republic, such as poverty and discrimination eradication and the promotion of national development.

[35] C. SPADACCINI DE TEFFÉ, ELORA FERNANDES, *Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites*, in O direito civil na era da inteligência artific, ial v. 1, Gustavo Tepedino & Rodrigo da Guia Silva org., 2020.

[36] M. PIANCASTELLI, *Federal Republic of Brazil*, in *Distribution of powers and responsibilities in federal countries. A global dialogue on federalism* v. II, Akhtar Majeed *et al* eds., 2006.

This cooperative character of Brazilian federalism does not prevent the arise of disputes or even conflicts between its entities. In fact, in addition to cooperation, they are stimulated to formulate practices and public policies to compete among themselves for citizens, investments, political influence, and better responses to global challenges. The COVID-19 pandemic in Brazil serves to illustrate this argument. Since the beginning of the sanitary crisis, there weren't enough measures to prevent and combat the disease by the federal government. In this context, the Federal Supreme Court recognized the power of states and municipalities to act and adopt legal measures to control and minimize the harmful impact of coronavirus on their territories. As consequence, new crisis management public policies have emerged, as well as competition among the states for a faster and more efficient vaccination of the respective populations[37].

The Federation is a space of coexistence among autonomous spheres of government. It is the Federal Constitution that guarantees the harmonious unity between the federative entities, by introducing effective mechanisms for resolving conflicts and a solid power distribution system. The model of division of competences of any Federation is based on the premise that there is no hierarchy between the federal units. The Brazilian Constitution presents a complex system of power division, which combines the explicit enumeration of administrative, legislative and tax competences to the federative entities and fields of shared competences between them. The allocation of powers among the Union, states, municipalities, and Federal District is grounded in the principle of predominant interest, according to which the federative unit that has the predominant interest in a certain matter, will the competent entity to handle it.

The matters reserved to the Union's private legislative competences in article 22 of the Constitution are extremely broad, as they cover a significant part of subjects related to

[37] E. MESQUITA CEIA, *Subsidiariedade, poder local e crises globais*, in C*adernos adenauer: eleições municipais e os desafions de 2020*, v. XXI 2. ed. (Fundação Konrad Adenauer org., 2020). M. PEREIRA JORGE, *Gincana da vacina*. *Folha de são paulo* (June 15, 2021), www1.folha.uol.com.br/colunas/marilizpereirajorge/2021/06/gincana-da-vacina.shtml.

the Law. The Constitution allows the Union, through federal complementary legislation, to delegate to the states and the Federal District legislative power to regulate specific issues regarding the matters enumerated by article 22. In this respect, the Brazilian Federation is centralized, since there is a larger number of competences conferred on the central than on the subnational entities, "what to a great extent erodes the cooperative nature of the Brazilian federalism"[38]. To the states the Constitution allocates the following powers: the private legislative competence[39]; the concurrent and supplementary competences on the subjects listed in article 24; and the residual competences[40]. To the municipalities are conferred private and supplementary competences on matters of local interest[41] and, to the Federal District, in turn, are reserved the powers attributed to the states and the municipalities by its hybrid nature[42].

The Brazilian Constitution assigns also to the Union legislative powers next to the other federative unities. In the matters that fall within this domain (listed in article 24) the entities have the competence to legislate but under different conditions. In the area of concurrent legislative competence, the states, and the Federal District "shall exercise full legislative competence to provide for their peculiarities, if there is no federal law on general

[38] Free translation of the original text in Portuguese. See V. AFONSO DA SILVA, *Direito Constitucional Brasileiro* 2021, p. 354.

[39] Article 25, paragraph 2, of the Constitution, declares: "The states shall have the power to operate, directly or by means of con- cession, the local services of piped gas, as provided by law; governors are forbidden to issue any provisional decree for its regulation (CA 5, 1995)". See Brazil, *Constitution of the Federative Republic of Brazil of 1988* (2020) at 34, http://www.stf.jus.br/arquivo/cms/legislacaoConstituicao/anexo/brazil_federal_constitution.pdf.

[40] Article 25, paragraph 1, of the Constitution, states: "All powers that this Constitution does not prohibit the states from exercising shall be conferred upon them". *Id.*

[41] Article 30 I and II of the Constitution declares: "The municipalities have the power to: I – legislate upon matters of local interest; II – supplement federal and state legislation where pertinent". *Id.*, at 40.

[42] J. DOLINGER, L. ROBERTO BARROSO, *Federalism and Legal Unification in Brazil*, in *Federalism and legal unification: a comparative empirical investigation of twenty systems*, Daniel Halberstam & Mathias Reimann eds., 2014.

rules"[43]. The later issue of a federal law on general rules suspends the effectiveness of a state or district law to the extent they are contrary to it.[44] In turn, in supplementary legislative competence, the Union sets up general rules, guidelines and principles that orientate and uniform the legal system, whereas the states, the Federal District and the municipalities enact specific rules in order to supplement federal legislation. It is worth underlining that the municipalities have only supplementary competences on matters listed in article 24, pursuant the clause of local interest as foreseen in article 30 I of the Constitution.

Therefore, states and municipalities must have priority in enacting specific rules, to respond to the demands of their population, which vary according to socioeconomic factors, provided that federal legislation is observed. State, district, and municipal rules contrary to federal legislation are unconstitutional and, consequently, must have their effects suspended. Likewise, article 24 of the Constitution constrains the performance of the Union:

If the central authority oversteps the limits of its legislative competence, the resulting law will be unconstitutional and, as a consequence, void. (...) in areas of concurrent jurisdiction, the Union shall only enact general rules. The enactment of specific rules – invading the states' jurisdiction – violates the allocation of legislative jurisdiction set forth in the Constitution.[45]

Given the above considerations, it is important to analyze the fact that cities have been becoming more relevant over the last decades, by emerging as significant actors in decision-making processes on diverse topics. The urbanization process has caused the relocation of political and economic power in favor of local governments responsible for managing these urban areas. Some cities have become a true metropolis, where new identities

[43] Article 24, paragraph 3. See Brasil, *supra* note 40.

[44] Article 24, paragraph 4. *Id*.

[45] Dolinger & Barroso, *supra* note 43, at 157-158.

and centers of power arise[46]. It is in this context that cities can reveal themselves as spaces of democracy, efficiency, and innovation. The central power, increasingly seen as bureaucratic and distant from the citizens, has been losing ground to the local power. The cities start experimenting successfully with welfare, environmental, and minority protection programs and, consequently, play an active role in global governance[47].

However, constitutional law did not follow this trend. Not only in theory but also in constitutional practice there is a "fundamental void"[48] characterized by the lack of studies and debates on the massive process of urbanization and the appearance of the so-called megacities[49]. In general, cities do not have the constitutional status as autonomous federated units. In most Federations, they are mere decentralizations dependent on the states.

Most constitutional orders currently in existence treat cities, including some of the world's most significant urban centers, as "creatures of the state", fully submerged within a Westphalian constitutional framework, and assigned limited administrative local governance authority. Their *constitutional* statuses range anywhere from secondary to nonexistent.[50]

[46] G. DILL, *O município em tempos de globalização*, in Federalismo na alemanha e no brasil. Série debates n. 22, Wilhelm Hofmeister & José Mário Brasiliense Carneiro org., 2001.

[47] Y. BLANK, *Federalism, Subsidiarity, and the role of local governments in an age of global multilevel governance*, Fordham urban law journal, 2010, 37.

[48] Hirschl, *supra* note 4, at 1.

[49] Megacities are cities with 5 million inhabitants or more or cities whose metropolitan zone has at least 10 million people. *Id*., at 6.

[50] *Id*., at 10.

In this perspective, the Brazilian federalism is an exception[51], since it is a case of "*deep federalism*" that takes the role of municipalities seriously[52]. The Brazilian Constitution assigns cities a prominent position compared with other federative constitutions. It provides for the implementation of an urban development policy that prioritizes the social function of cities and the public welfare[53]. Indeed, the recognition of municipal constitutional autonomy took over core relevance in the constituent and redemocratization process of 1988.[54]

Nonetheless, in accordance with the constitutional rules that govern the Brazilian Federation, the municipal autonomy is more limited than the state one. In contrast to the states, the Brazilian municipalities do not have a constitution, but rather are organized by ordinary organic laws. They do not have a strong political representation in federal level as states do. Then, municipalities do not participate in the constitutional reform process nor in the system of abstract constitutional review before the Federal Supreme Court. Furthermore, the exercise of municipal competences is subject to the Federal Constitutional as well as to the state constitution and the Brazilian municipalities are financially dependent on the

[51] Silva, *supra* note 39.

[52] L. KING, *Cities, subsidiarity, and federalism*, in Federalism and subsidiarity, James E. Fleming & Jacob T. Levy eds., 2014.

[53] Article 182 of the Brazilian Constitution: "The urban development policy carried out by the municipal government, according to general guidelines set forth by law, is aimed at ordaining the full development of the social functions of cities and ensuring the wellbeing of its inhabitants." See Brazil, *supra* note 40, at 149. The implementation of article 182 is regulated by the so-called City Statute (Law No. 10,275/2011) which defines binding guidelines to federal, state, and local governments towards the realization of a sustainable and democratic municipal administration with the active participation of civil society.

[54] "As has been the case throughout Brazil's constitutional history, tensions between the different orders of government have persisted, and what occurred after the 1988 constitutional reform has been no exception. These tensions became more evident as the municipalities were granted full autonomy by the new Constitution. The drafters, mainly from opposition parties, emphasized a decentralization process with the major aim of bringing power closer to the people in the ultimate hope of enhancing democratic institutions". See Piancastelli, *supra* note 37, at 75.

resources distributed by the Union and the states[55]. In practice, the funding for urban development projects depends to a large extent on the political alignment between federal, state, and municipal governments[56].

Article 29 of the Brazilian Constitution sets forth the municipal self-government and legislative and administrative prerogatives, including financial management. Cities have the supplementary legislative power under the matters enumerated in article 24, to address local demands and needs through the enactment of specific rules in line with the existing federal and state legislations. Moreover, cities legislate on matters of local interest, for instance, garbage collection and opening hours of commercial businesses and establishments[57]. Some doctrines defend a broad interpretation of the term "local interest" to ensure the effectiveness of constitutional attributions to the municipalities and the constitutional value of decentralization. Otherwise, few competences would remain to the municipalities, given the extensive competences of the Union and the residual powers reserved to the states. Hence, the term "local interest" is not restricted to subjects of exclusive interest of a certain city, without any effect on other federated units, but rather encompasses any subject that proves necessary to establish local policies, even though it indirectly affects other federated units[58].

Within this hermeneutic perspective, the principle of subsidiarity is of fundamental importance. Subsidiarity is a notion present in federation structures that acknowledge the cities a special status[59], such as the Brazilian federalism. The principle of subsidiarity

[55] Dolinger & Barroso, *supra* note 43.

[56] Hirschl, *supra* note 4.

[57] Dolinger & Barroso, *supra* note 43.

[58] R. HERMANY, *(Re)Discutindo as políticas públicas no espaço local: interconexões entre federalismo, subsidiariedade e direito social no Brasil*, in Federalismo e constituição: estudos comparados, Antonio Moreira Maués org., 2012.

[59] Blank, *supra* note 48.

declares that the central government shall exercise its powers only to support the subnational entities, in other words, shall act only if subnational governments are unable to perform on their own the task to be carried out[60]. When applied in the context of allocation of powers between federated entities, the principle of subsidiarity serves to conciliate uniformity and flexibility regarding regional and local realities, "emphasizing a more pluralistic and spatially-consciousness view of public law"[61]. Concerning municipal legislative competence, the notion of subsidiarity gives precedence to the achievement of local interest in accordance with the existing federal and state legislation[62].

At times, difficulties of interpretation arise by defining the competences of each entity. A subject of civil law – which falls under the private legislative power of the Union – can be, at the same time, a matter of local interest of a certain municipality. The Brazilian Federal Supreme Court plays an important role in solving conflicts between the jurisdictions of the federated entities. The Court is criticized by some legal experts for not having developed clear criteria regarding the resolution of conflicts among federative entities[63].

In any case, by analyzing its jurisprudence, one can note that the Court usually rules in favor of the Union on controversies related to matters that fall within the federal private legislative powers[64]. With respect to concurrent and supplementary competences, the Federal Supreme Court "rarely declares a federal law unconstitutional based on the allegation that its

[60] D. HALBERSTAM, *Federal powers and the principle of subsidiarity*, in Global perspectives on constitutional law, Vikram David Amar & Mark V. Tushnet eds., 2009.

[61] Hirschl, *supra* note 4, at 15.

[62] M. MONT'ALVERNE BARRETO LIMA, *Art. 29*, in Comentários à constituição do brasil, J. J. Gomes Canotilho *et al* coords., 2013.

[63] Silva, *supra* note 39.

[64] Dolinger & Barroso, *supra* note 43, at 159.

provisions are not general"[65]. However, in certain cases, the Court applies the principles of subsidiarity and cooperation and thus guarantees the exercise of competences by the municipalities considering their respective realities. The ruling on Direct Action of Unconstitutionality No. 3,921 is a good example.

In this judgment of 2020 the Federal Supreme Court, by the majority of votes, declared Law No. 10,501/1997 of the state of Santa Catarina constitutional with *erga omnes* effects. The law obliges banks and financial institutions located in this state to install security systems, such as guards, security doors and alarms. The rapporteur, Justice Edson Fachin, in his vote, followed by most judges, dismissed the action and declared the state law constitutional based on the legislative power of the states, Federal District and municipalities on the subject of public security.

The Constitution uses the phrase "is duty of the state" to deal with specific themes, namely public security[66], health[67], education[68] and sports[69]. Health, education, and sports are listed as matters which fall under the concurrent and supplementary legislative competences

[65] Free translation of the original text in Portuguese. See Silva, *supra* note 39, at 371.

[66] Article 144 of the Constitution states: "Public security, the **duty of the State** and the right and responsibility of all, is exercised to preserve public order and the safety of people and property, by means of the following agencies […]" [our emphasis]. See Brazil, *supra* note 40, at 120.

[67] Article 196 of the Constitution states: "Health is a right of all and a **duty of the State** and shall be guaranteed by means of social and economic policies aimed at reducing the risk of illness and other hazards and at the universal and equal access to actions and services for its promotion, protection and recovery" [our emphasis]. *Id*., at 157.

[68] Article 205 of the Constitution states: "Education, which is the right of all and **duty of the State** and the family, shall be promoted and fostered with the cooperation of society, with a view to the full development of people, their preparation for the exercise of citizenship and their qualification for work" [our emphasis]. And article 208 declares: "The **duty of the State** towards education shall be fulfilled by ensuring the following: […]" [our emphasis]. *Id*., at 163-164.

[69] Article 217 of the Constitution states: "**The State has the duty** to foster the practice of formal and informal sports, as a right of each person, with due regard for: […]" [our emphasis]. *Id*., at 170.

of the states, Federal District, and municipalities[70]. In line with this consideration, the Court understands that the Constitution likewise grants the subject of public security the qualification of a matter that falls within the legislative competences of the states, Federal District, and municipalities[71].

Justice Fachin clarifies that the state law of Santa Catarina covers two main topics, specifically financial institutions and public security. On one hand, the Union has private competence to legislate on financial institutions[72] and, on the other hand, the states have concurrent and supplementary power to legislate on public security (article 24, IX and XII). In such cases, Justice Fachin warns that doubts about the exercise of legislative competences by the federative entities can emerge and the principle of predominant interest does not always offer a satisfactory solution. As a result, the interpreter must invoke other principles of Brazilian federalism, namely the subsidiarity and the cooperation, to resolve the conflict of competence.

Therefore, the Brazilian Constitution of 1988 is a historic milestone regarding the political decentralization in favor of cities. Based on the system of division of federative competences entrenched in the Constitution, cities became responsible for the implementation of most social policies and services, aside from exercising new legislative powers related to matters of local interest. Nevertheless, the Brazilian Federation continues to be characterized as centralized not only because of the financial dependency of most municipalities on the federal transfers of revenues – to respond to the needs of the population

[70] Article 24 IX and XII of the Constitution states: "The Union, states and Federal District have the power to legislate concurrently on: […] IX – **education**, culture, teaching, **sports**, science, technology, research, development, and innovation; (CA 85, 2015) […] XII – social security, **protection, and defense of health**; [our emphasis]". *Id*., at 34.

[71] Brazil, *Direct Action of Unconstitutionality No. 3,921/Santa Catarina. Vote Rapporteur Justice Edson Fachin*, 2020.

[72] Article 22 VI and VII of the Constitution states: "The Union has the exclusive power to legislate on: […] VI – the monetary and measures systems, metal certificates and guarantees; VII – policies for credit, foreign exchange, insurance, and transfer of values". See Brazil, *supra* note 40, at 32.

– but also because of the large legislative competences of the Union in defining general rules and guidelines to be observed by the municipalities in the execution of social policies and services[73].

As discussed in section 1, there are several concerns about the use of facial recognition systems in cities, for example, the dangers of mass surveillance and the violation of individual freedoms as well as the lack of transparency on the technology implementation and the methods applied to deal with sensitive data. Accordingly, specific regulation on the use of facial recognition technologies is essential, which should combine the harnessing of the potential of this new technology with the protection of fundamental rights.

In the context of Brazilian federalism, the following question arises: which is the federated entity responsible for legislating the use of systems of facial recognition for the purpose of public security? This issue has not been discussed by the Federal Supreme Court yet, nor has received special attention from constitutional scholars. Despite the Union has not enacted general rules on the subject, some states and municipalities have been at the forefront of passing specific legislation to meet their demands.

In any event, the answer to the question must be justified by constitutional rules concerning the distribution of federative competences and core principles that guide the application of those rules, namely the principles of predominant interest and subsidiarity. The first step is identifying the dominant subject in the specific matter of the use of facial recognition technologies for the purpose of public security. This is important, at the next stage, to point out which federated unit has a predominant interest in the subject based on the federative constitutional rules and principles.

The difficulty resides in the identification of the dominant subject related to the use of facial recognition technologies for the purpose of public security. It is possible to spot two

[73] Piancastelli, *supra* note 37.

major themes in this matter: a) civil law, since it relates to a technology whose operation depends on personal data treatment and, consequently, deals with personality Rights foreseen in the Brazilian Civil Code; and b) public security, because the prevention and combat of crimes are the specific intended purposes by the systems of facial recognition through personal data treatment.

If civil law is the dominant subject, the Union will have the power to legislate on the use of facial recognition technologies for the purpose of public security in accordance with article 22, I, of the Constitution. In this scenario, states and the Federal District could only legislate on specific issues regarding the use of facial recognition technologies for the purpose of public security, when authorized by the Union by means of a supplementary law[74]. At present, there is no current supplementary law of this kind. In turn, to the municipalities is not assigned any competence on the matters enumerated in article 22, including civil law, and hence to them would not be recognized legislative powers on the use of facial recognition technologies for the purpose of public security.

In February 2022, Constitutional Amendment No. 115 entered into force and added item XXX to article 22 to establish the private competence of the Union to legislate on the protection and treatment of personal data. The goal is to uniform the legislation due to the existence of various state and municipal draft bills on the subject and, consequently, to prevent normative fragmentation and multiplicity of criteria defined by each region and city[75].

[74] Article 22, sole paragraph, of the Brazilian Constitution: "*A supplementary law may authorize the states to legislate upon specific topics related to the matters listed in this Article*". See Brazil, *supra* note 40, at 33.

[75] The Constitutional Amendment No. 115/22 has also included the item XXVI to article 21, to determine the exclusive competence of the Union to organize and supervise the protection and treatment of personal data, under the terms of the law. Câmara dos Deputados, *Promulgada PEC que inclui a proteção de dados pessoais entre direitos fundamentais do cidadão* (2022), https://www.camara.leg.br/noticias/850028-promulgada-pec-que-inclui-a-protecao-de-dados-pessoais-entre-direitos-fundamentais-do-cidadao/.

However, the present work follows the position of the Federal Supreme Court laid out in the above outlined ruling on Direct Action of Unconstitutionality No. 3,921: "In cases where there is doubt about identifying the legislative competence, because more than one subject falls under the legal provision in question, the court must choose the interpretation which does not impair the competence that smaller entities have to legislate on a particular matter"[76].

We argue that the dominant subject related to the use of facial recognition technologies for the purpose of public security shall be, indeed, public security. On this matter states, the Federal District and municipalities have concurrent and supplementary powers to legislate next to the Union, as decided by Federal Supreme Court. In his vote, Justice Alexandre de Moraes stressed that:

When applied in the context of the Brazilian Federation the principle of subsidiarity (...) must enhance the preponderant action of the federated entity within its sphere of competence in proportion to its greater capacity to solve matters of public concern, considering the regional peculiarities. The greater state autonomy to legislate on subjects related to public and prison security will enable a better observance of regional peculiarities and efficiency in fighting organized crime, including inside penitentiary facilities[77].

Before the National Congress is currently running the Proposal of Constitutional Amendment No. 33/2014, which intends to amend articles 23 and 24, to textually insert the subject of public security within the scope of common, concurrent, and supplementary competences of the federative entities. In the justification of the proposal, the authors explain that the amendment serves the purpose of only rectifying the omission of the original

[76] Free translation of the original text in Portuguese. See Brazil, *Direct Action of Unconstitutionality No. 3,921/Santa Catarina. Full text of the decision. Rapporteur Justice Edson Fachin* (2020), at 3.

[77] Free translation of the original text in Portuguese. See Brazil, *Direct Action of Unconstitutionality No. 3,921/Santa Catarina. Vote Justice Alexandre de Moraes* (2020), at 11.

constituent[78]. Likewise, Justice Fachin emphasizes in his vote that the Proposal of Constitutional Amendment No. 33/2014 "thus seeks to make explicit what already derives from a systematic interpretation of the Constitution"[79], namely the legislative power of subnational entities besides the Union on the subject of public security.

In conclusion, we argue that all entities of Brazilian Federation have the competence to legislate on the specific matter of the use of facial recognition technologies for the purpose of public security. On the one hand, the Union will be responsible for establishing by law principles, limits, and general rules on the subject according to article 4, paragraph 1, of Brazilian General Data Protection Law, and, on the other hand, states, the Federal District, and municipalities may supplement federal legislation through the enactment of specific rules to meet regional and local needs in the area of public security.

4. FACIAL RECOGNITION AND PUBLIC SECURITY IN THE CITY OF RIO DE JANEIRO

In addition to the risks and ethical concerns associated with the use of facial recognition technology, the high rate of misunderstandings undermines its reliability and effectiveness in reducing crime. The literature exemplifies this problem in cases of application of this technology in several cities around the world, mainly reaching traditionally discriminated and more vulnerable groups.[80] As a case study, this paper examines the

[78] Brazil, *Proposal of Constitutional Amendment No. 33* (2014), https://www25.senado.leg.br/web/atividade/materias/-/materia/144585.

[79] Free translation of the original text in Portuguese. See Brazil, *supra* note 72, at 6.

[80] B. DIAS FRANQUEIRA, I. A. HARTMANN, L. ABBAS DA SILVA, *O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina*, 8 Revista digital de direito administrativo 1, 2021. F. TAUTE, *Reconhecimento facial e suas controvérsias*, Heinrich böll stiftung, 2020, https://br.boell.org/pt-br/2020/02/05/reconhecimento-facial-e-suas-controversias#_ednref1.

experience of the city of Rio de Janeiro (capital of the state of Rio de Janeiro, Brazil) with the use of facial recognition systems in the field of public security.

On the one hand, few Brazilian cities have legislation to regulate the use of facial recognition technology, on the other hand, many cities have been using such technology for various purposes: to promote public security, control entrances into the territory, control access to restricted areas and curb the misuse of gratuities and crime in public transport, football stadiums, toll booths and public spaces. In some cases, the application of this technology takes place based on the regulations of the respective state in which the municipality is located.

The state of Rio de Janeiro presents some bills, under analysis in its Legislative Assembly, on the use of facial recognition systems in different applications. The bills deal with the installation of surveillance cameras with facial recognition technology in the subway, bus, train, and ferry stations, as well as in toll booths, with the following purposes: to identify suspects and wanted by the courts; curb the illegal sale of products; and control the undue use of gratuities and tariff benefits.

Besides this, there are two laws in force in the state of Rio de Janeiro related to the topic of the use of technologies in public security. Law No. 4,291/04 (amended by Law No. 7,123/2015) determines the control of gratuities and tariff benefits in public transport services, through biometrics, but without specifically mentioning facial recognition technology[81]. Also, in the state of Rio de Janeiro, Law No. 9,167/21 provides that the

[81] "Paragraphs 1 and 2 of Article 9 of Law No. 4,291/04 (amended by Law No. 7,123/2015) of the state of Rio de Janeiro establishes: "(...) Paragraph 1 - The control of gratuities and tariff benefits will use technologically adequate means, including biometrics, obligatorily paid by concessionaires and licensees of public passenger transport services by bus, to ensure its legitimate exercise, prohibiting, in any event, the cost of implementing the technology to be transferred to the public service tariff or to the Granting Authority in the form of economic and financial rebalancing. Paragraph 2 - The implementation of biometric control, preferably facial or other technologically appropriate, will be carried out through means of registration or re-registration of users, considering the definition of validity periods of the electronic card at the discretion of the Grantor." Free translation of the original text in Portuguese.

Executive Branch may establish the Database for Facial and Digital Recognition of Missing Children and Adolescents, linked to Detran/RJ[82]. None of these documents specifically address the guarantee of rights and accountability of agents for possible abuses in the handling of facial recognition systems.

Facial recognition technology began to be used more intensively in the city of Rio de Janeiro in 2019 when a cooperation agreement was signed between the State Secretariat of Military Police of the state of Rio de Janeiro and the telephone company Oi. The objective was to implement facial recognition technologies in activities related to public security. The program worked in connection with the Command and Control Center of the Military Police of the state of Rio de Janeiro, which received the images in real-time and performed their cross-referencing with the state's Civil Police database, which gathers data from fugitives from justice. The pilot project was applied during the Carnival of the same year, with the installation of 34 cameras and specific training for police officers. During this period, in Copacabana, three arrest warrants and five arrest warrants for teenagers were served, as well as three stolen vehicles were recovered. The use of facial recognition technology during Carnival in Rio showed an error rate of 90%. Later, the project was expanded in the city and the number of cameras increased significantly. The use of such technology resulted in the arrest of people, against whom there were open arrest warrants, but also in the occurrence of false positives. In the Copacabana neighborhood, for example, a woman was wrongly identified as a criminal who was already in prison. The woman was taken to the police station, as she did not have an identity document at the time of the police approach. After verifying

[82] Departamento de Trânsito do Estado do Rio de Janeiro – DETRAN. Traffic Department of the State of Rio de Janeiro.

her identity at the police station, the woman was released. This case exposes another problem related to the use of the system in the city of Rio de Janeiro: the use of outdated databases.[83]

In 2019, 184 arrests were made using facial recognition technology. In 90% of them, the people arrested were black and were detained for crimes of low violence, such as petty theft and robbery.[84] Even though facial recognition has been increased, some questions concern us: how is monitoring carried out? What is the location of the cameras? Do they work 24 hours a day? Is the data analyzed in real-time? Where does the data processed by the devices go? What is the retention time? Who can access the information? How are people identified? Which database is used to identify people? Creating more diverse databases to train machines and artificial intelligence, seeking diversity in teams, working inclusive codes, auditing technologies, and avoiding discriminatory practices are essential practices for the development of more inclusive, fair, and ethical technologies.

In January 2020, the city of Rio de Janeiro announced the signing of an agreement with the Ministry of Justice, which establishes the sharing of images captured by individual cameras installed in the uniform of Municipal Guard agents with facial recognition technology, to identify fugitives from justice and stolen vehicles.[85] The initiative of R$ 3.8 million in total will be funded by the Special Fund for Public Order, created by Municipal Law No. 6,235 of 2017, whose objective is to provide resources for activities in the interest of public order in the city of Rio de Janeiro. It is worth mentioning that, in 2019, the Ministry of Justice and Public Security issued Ordinance No. 793, which encourages the

[83] Taute, *supra* note 81. A. LUIZA ALBUQUERQUE, *Em fase de testes, reconhecimento facial no Rio falha no 2º dia*, Folha de são paulo, July 17, 2019, https://www1.folha.uol.com.br/cotidiano/2019/07/em-fase-de-testes-reconhecimento-facial-no-rio-falha-no-2o-dia.shtml.

[84] Câmara Rio, *Identificação facial é tema de audiência de Comissão Especial*, 2021, http://www.camara.rio/comunicacao/noticias/394-identificacao-facial-e-tema-de-audiencia-de-comissao-especial.

[85] Rio Prefeitura, *Município estende Rio+Seguro à Zona Oeste com câmeras de reconhecimento facial*, 2020, https://prefeitura.rio/cidade/municipio-estende-rioseguro-a-zona-oeste-com-cameras-de-reconhecimento-facial/.

implementation of video surveillance systems with facial recognition in territories with high crime rates in the country.[86]

In June 2021, a public hearing was held at the City Council to discuss a public-private partnership for the modernization of public lighting and connectivity in the city in the years to come. This is the *Luz Maravilha* Program, through *Rioluz*, a municipal energy and lighting company, and the Municipal Infrastructure. The project foresees the installation of 10,002 cameras, 40% of which are equipped with facial recognition technology. On that occasion, councilors and civil society representatives expressed concern about the impact of the use of this technology, especially on the black population.[87]

Also in June 2021, the City of Rio announced that it will start a project to expand and modernize the Rio Operations Center (*Centro de Operações Rio* - COR), the largest urban monitoring center in Latin America. The expansion of the agency, located in Cidade Nova, in the central region of the city, will cover 1,400 square meters – which represents an increase of about 50% to the total area currently built. The project is one of the results of the Public-Private Partnership for public lighting in the city of Rio de Janeiro, mentioned above. The program also provides for 5,000 Wi-Fi points and around 9,000 georeferenced sensors, among other gains for the municipality.

With the expansion, COR will have more human and technological resources capable of developing solutions related to the Internet of Things and smart cities. According to institutional information, these points will work with intelligent sensors capable of generating data that will be processed by a technical team to transform them into service for

[86] As a reaction to the mass implementation of facial recognition, it is worth mentioning Federal Bill 604/2021, which amends Decree-Law No. 3689/41 (Code of Criminal Procedure) and Law No. 7,960/89, to prohibit preventive detention based exclusively on recognition by photographic identification.

[87] Câmara Rio, *supra* note 85.

the citizen. The aim is to use technology to make the operation increasingly predictive and less reactive, anticipating crisis and improving the prompt response to occurrences.[88]

5. CONCLUDING REMARKS

The urbanization process has led cities to occupy a prominent position in the global scenario. The central government, increasingly seen as bureaucratic and distant from the citizens, has been losing ground to the local power, which is closer to individuals. Through responsive leadership and good practices, cities start experimenting successfully with economic, social, and environmental programs. Hence, cities can reveal themselves as spaces of democracy, efficiency, and innovation. From this perspective, it is of great importance the concept of smart cities, which use new technologies to implement public policies and boost processes that guarantee the quality of life for citizens, sustainability, greater efficiency in services, and competitiveness.

Urban violence is a common problem in megacities, especially in those situated in the Global South. For this reason, is more and more frequent the use of new technologies in the fight against crime by local authorities, for instance, facial recognition technologies. As highlighted in this work there are several concerns associated with the use of facial recognition systems, such as mass surveillance, undue treatment of sensitive personal data, violation and inhibitory effects on the exercise of fundamental rights (like freedom of speech and assembly), high rates of error (particularly against certain groups and minorities) and lack of transparency. These risks are exacerbated in societies characterized by social inequality and racial discrimination, such as Brazilian society. Therefore, facial recognition technologies need, apart from in-depth multisectoral discussions and more refined

[88] Rio Prefeitura, *Com expansão do COR, Rio avança no conceito de cidades inteligentes*, 2021, https://prefeitura.rio/cidade/com-expansao-do-cor-rio-avanca-no-conceito-de-cidades-inteligentes/.

development and analysis, a framework regulation that carefully observes the protection of fundamental rights, international human rights norms, and ethical considerations.

The report on the experience of the city of Rio de Janeiro exposes the dangers and problems directly related to the use of facial recognition technologies in the context of public security. Rio is more and more committed to initiatives that involve these technologies but needs to implement greater attention and specific criteria for their responsible use.

Based on the constitutional norms in force and on the recent jurisprudence of the Federal Supreme Court, we conclude that all entities of the Brazilian Federation have the competence to legislate on the specific matter of the use of facial recognition technologies for public security. The Union will be responsible for establishing by Law principles and general rules on the subject, whereas states, the Federal District, and municipalities may supplement federal legislation through the enactment of specific rules to respond to their peculiar demands.

As explained before there is no federal law on the use of facial recognition systems in force in Brazil yet. Within this legal vacuum states and municipalities have enacted specific laws to regulate the matter. We argue that these laws are constitutional since they fall under the lawful exercise of legislative powers on the matter of public security in accordance with articles 24 and 30, I, of the Constitution. If posteriorly federal law over general rules on the subject enters in force, state or municipal legislation will have their effectiveness suspended to the extent they are contrary to the federal law.

For the harmonic coexistence among the different legislations, it will be essential that, on the one hand, the Union issues only general rules on the subject – and not usurp the competence of subnational entities through the enactment of specific rules – and, on the other hand, states, the Federal District, and municipalities enforce specific laws respecting the federal general rules. The municipalities shall also observe the existing state legislation. The position in favor of the legislative competence of all Brazilian federative entities on the use of facial recognition technologies for the purpose of public security reflects the will of the

Constitution of 1988 to fulfill political decentralization and, consequently, the democratic exercise of political power, especially on a matter intrinsically related to civil liberties.

A legal landmark on the use of facial recognition technologies for the purpose of public security is urgent in Brazil. The absence of specific legislation on the use of facial recognition systems is common in several countries in Latin America. According to the cooperative model of Brazilian federalism, it is possible to conciliate local autonomy – with special attention to the peculiarities of cities – with the need for action coordination between all federative units based on general guidelines defined by the Union. Thus, it is imperative the enactment of federal legislation that provides a general regulatory model based on the principles of Brazilian General Data Protection Law and the constitutional principles of presumption of innocence and broad defense, in addition to liability rules for cases of fundamental rights abuses and violations. Such a regulatory model would ensure the necessary legal uniformization and, as a result, mitigate eventual divergences between the central and subnational entities that could create legal uncertainty among individuals, public authorities, and enterprises.

Abstract. *Cities have effectively become spaces for democracy and innovation. In this context, it is of great importance the concept of smart cities, which use new technologies to implement public policies and boost processes that guarantee the citizens a better quality of life, sustainability, greater efficiency in services, and competitiveness. Urban violence is one of the major challenges faced by Brazilian big cities. Therefore, new technologies are more and more being used in combating crime by local authorities. One of these technologies is facial recognition, whose use for public security is controversial, especially because of the risk of reinforcing discrimination and the absence of regulation by a specific law. According to Brazilian General Data Protection Law, the processing of personal data that is done exclusively for purposes of public safety, national defense, state security or activities of investigation and prosecution of criminal offenses should be regulated by specific legislation, probably enacted by the Union. In practice, however, the local authorities did not wait for the due regulation. Several Brazilian cities are already making use of facial recognition technologies in the fight against urban violence. Considering the constitutional autonomy of cities under Brazilian law, the paper aims to analyze the main controversies on facial recognition technologies for public security purposes, namely the potential conflicts of competence between federated entities and the risks of violations of minorities' fundamental rights. As a case study, the paper assesses the experience of the city of Rio de Janeiro, where facial recognition has been increasingly implemented since the 2019 Carnival.*