BRAZILIAN SMART CITIES: FROM PRINCIPLES TO PRACTICE

// **BÁRBARA SIMÃO,** HEAD OF RESEARCH, PRIVACY AND SURVEILLANCE, INTERNETLAB
BLENDA SANTOS, RESEARCHER, PRIVACY AND SURVEILLANCE, INTERNETLAB

When it comes to articulating principles for democratic smart cities, Brazil's recent efforts stand out. In recent years, Brazilian cities have raced to become "intelligent" by adopting new digital tools for connectivity, urban mobility, education, and public safety. To steer these projects, authorities have launched a range of new rules and institutions. **Documents including the Brazilian Charter for Smart Cities and National Policy for Smart Cities propose important democratic norms in this area, including respect for rights, public participation, and engagement with civil society.** On the ground, however, officials and vendors are still far from taking the steps needed to ensure that municipal digitalization serves democracy.

In the 2021 report "Smart Cities and Data Protection: Recommendations and Best Practices,"[44] InternetLab together with Article19 and LAPIN identified gaps in the management of Brazilian smart cities that threaten to seriously undermine democratic principles. These issues include a **lack of transparency, privacy risks, discrimination against historically marginalized groups, increased surveillance, and unbalanced relationships between local governments and private companies**. To ensure that smart city initiatives respect people's rights and respond to their wishes, we recommend that officials prioritize adherence to technical and legal standards, avoid dependence on vendors, and consider alternative approaches to digital development.

THE QUEST TO BECOME "SMART CITIES"

Designation as a smart city offers a coveted stamp of modernity and innovation. Although the formal title may be elusive—São José dos Campos was certified just this year as Brazil's first smart city, according to criteria set by the International Organization for Standardization and the World Council on City Data—many Brazilian cities are working on digital projects that will allow these municipalities to bill themselves as "smart."[45] What do their efforts entail? According to our study, the greatest share of **ICT (Information and Communications Technology) projects seem to be concentrated in four main categories: (a) connectivity, (b) urban mobility, (c) education, and (d) public safety**.

Connectivity projects are aimed at boosting citizens' access to digital networks or services through infrastructure advancements, offering free Wi-Fi in public spaces, and facilitating access to government bureaucracies or public services, among other innovations. In *urban mobility*, the main ICTs involve databases, electronic ticketing, and smart traffic lights. *Education* ICTs include management and teaching software, while projects aimed at improving *public safety* might involve video surveillance cameras, mobile access to databases, or license plate recognition. Notably, **facial recognition technologies (FRTs)** that automatically identify individuals based on images of their faces are present across the mobility, education, and public safety sectors.

A "free internet area" in Manaus, Brazil.

There is a vast array of different technology companies offering these types of solutions in Brazil. Some companies specialize in smart cities technologies and sell business intelligence. Others focus on specific areas, such as mobility, health, or surveillance technologies. They are mostly domestic companies, but the procedures involved in concluding these contracts are substantively similar for both domestic and foreign vendors. Also common across all cases is the **opacity of the contracts, their terms, and their limitations**.

Recently, Brazilian public officials have put great effort into regulating these initiatives and establishing **national standards**. In 2019, the federal level government promulgated a National Plan for the Internet of Things, and in 2021 it adopted a Digital Government Law setting out frameworks to make public administration more efficient through de-bureaucratization, innovation, and digital transformation. In that context, a Digital Cities program was developed to help connect municipal public bodies to the ICT world. Some **municipalities have established their own programs, offices, and guidelines** to improve digital connectivity and digital governance tools.

Brazilian public officials have put great effort into regulating smart city initiatives and establishing national standards.

In 2019-2020, through a participatory process that involved three rounds of consultations and input from more than two-hundred civil society stakeholders, Brazil's Ministry of Regional Development led the drafting of a Brazilian Charter for Smart Cities. The Charter aspires to be "a democratic political document that expresses a public agenda for the digital transformation of cities," and it outlines 163 recommendations in support of strategic goals that touch on themes from sustainable development and urban inequality to data privacy.[46] A platform for assessing Brazilian smart cities was launched on the basis of this document, and its work has fed into the development of a National Policy for Smart Cities currently under discussion in the National Congress.

Many of Brazil's policies on smart cities show **awareness of the need to consult different stakeholders, prioritize human rights, and engage the wider public** in what the Charter calls "democratic management of cities." The Digital Government Law, for instance, includes citizen participation as one of its principles. Some municipalities have grappled independently with the rights impacts of smart city ICTs: The city of Vinhedo near São Paulo, for instance, in 2018 approved Brazil's first act regulating municipal data protection.[47] This decision sets an important and positive precedent, as although data protection is regulated at the federal level in Brazil, municipalities can also enact subsidiary laws that may address local specificities.

Most important, the Charter establishes a number of key democratic principles. It stresses the **crucial role of civil society organizations (CSOs) as well as educational and research institutions** in disseminating knowledge and ensuring the quality of public debate; emphasizes that authorities should **hire project implementers that are committed to human rights**; calls for smart cities to meet **standards of cybersecurity, transparency, and privacy protection** with regard to their handling of data; and reinforces that these projects should **serve the public interest above all**.

The effort to articulate a **participatory vision for smart cities** throughout this process is remarkable. It forms a notable contrast with the general practice of the Brazilian government in recent years, which repeatedly obstructed the participation of civil society in public policy councils. This divergence may stem in part from backing for the Charter's elaboration under a technical cooperation agreement between the governments of Brazil and Germany (started in 2015 with the terms of execution defined in 2017) that aimed to support the preparation of a national urban development strategy based on economic, social, and environmental sustainability.[48]

TECH RISKS AND GOVERNANCE GAPS

Despite this promising vision, current practices around "smart city" ICTs in Brazil create **roadblocks to informed public participation**. In the absence of stakeholder engagement that might better reveal the needs and concerns of local communities, **the race to become "smart" could end up harming rather than helping municipal democracy**. Serious attention to human rights impacts and adequate understanding of new technologies themselves are also crucial. Researchers and civil society groups are currently leading initiatives to identify concerns and understand whether smart cities are genuinely improving citizens' lives.

View of the Operations and Intelligence Center, of the Public Security Secretariat of Bahia in Salvador, Brazil.

While some smart city ICTs may offer benefits in terms of efficiency, convenience, and connectivity, specific applications as well as the broad trend toward personal data collection also threaten democratic values. Digitalizing public services, for example, can **deepen social inequalities** since the digital divide (unequal access to digital networks across different social groups) can place these services out of reach for marginalized communities.[49] Digital educational technologies may also jeopardize privacy and equal opportunity for children and adolescents—a particularly vulnerable group.[50] And in the public safety field, the use of FRT has increased the number of people wrongly identified as having committed crimes.

Most smart city ICTs carry risks related to the use and handling of personal data.

Although many smart city projects use facial recognition technology (FRT), it is a highly controversial tool. **When São Paulo deployed FRT in its subway—under the justification of protecting commuter safety—research and advocacy organizations found that the technology contravenes Brazilian privacy laws.** In addition, it could produce discriminatory outcomes due to its higher rates of misidentification for certain groups (such as Black and transgender people).[51] In 2022, several of these organizations—including Article19, the Brazilian Institute for Consumer Protection (IDEC), and the Public Defender's Office of the State of São Paulo—filed a public civil action that managed to prevent implementation of the system for capturing and processing subway users' biometric data.[52] Following global appeals for banning FRT in public spaces, a group of CSOs in June 2022 launched the "*Tire meu rosto da sua mira*" ("take my face out of your sight") campaign, calling for a general ban on FRT in public security.[53]

Beyond these case-specific concerns, **most smart city ICTs carry risks related to the use and handling of personal data**. Speaking broadly, these projects frequently involve either (a) collecting new personal data from citizens; or (b) providing data that is already in the authorities' possession to outside contractors. Sensitive information about individuals' gender and sexuality, race and ethnicity, class, age, and address are often included. In a political context where powerful actors dispute the very concept of human rights and acts of violence are systemic, especially against historically marginalized groups such as women or LGBTQIA+ and Black people, this practice could endanger citizens' safety as well as their rights to privacy and equal treatment. Moreover, the collective risk of these data-driven projects is greater than the sum of its parts, since personal data taken from different contexts can be combined in ways that present new threats to privacy and human rights.

In the face of these risks, transparency, stakeholder engagement, and clear human rights protections are critical. At present, however, municipal ICT projects often omit these safeguards. Private marketing and consultancy agencies have issued various rankings to assess smart cities (rankings that may sometimes be influenced by criteria other than the public interest).[54] Appearing at the top confers prestige and may make cities more attractive to additional companies deciding where to invest. **As cities race to boost their standing by deploying new ICTs, dangerous oversights in procurement and implementation can occur.**

Municipalities scrambling to make it to the top may not, for instance, adequately consider how their projects intersect with social and digital inequalities on the ground; effectively foster democratic participation in the planning and management of ICT projects; or ensure that citizens' privacy and other rights are properly protected. Haste to conclude contracts can also result in a **lack of transparency** about the process and **non-compliance with relevant international norms** (such as technical standards and guiding principles on business and human rights).

As cities race to deploy new ICTs, dangerous oversights in procurement and implementation can occur.

When it comes to privacy, ICT contracts often lack specific provisions on the use of data, even when the projects involve extensive access to personal information. Without such safeguards, data ownership may be unclear, and **citizens' data rights can become a bargaining chip** between public bodies and private companies. For example, disputes may arise around what happens to the personal data of users of a public service after the end of a public-private contract.

This possibility is all the more concerning in light of **widespread opacity around public-private partnerships** for municipal digitalization. Many of these agreements are not publicly available. Several requests for access to information made during our research went unanswered or received an incomplete response. This secrecy leaves open questions about what kind of projects are being implemented; why and for whom they are being implemented; what they will cost; and who sells and operates the resulting systems.

Finally, municipalities do not generally appear to have given much consideration to the risks associated with the technologies they are using: **Almost no authorities reported that they had carried out data protection or human rights impact assessments during the adoption and deployment of ICTs**—activities which should be standard practice. Although it is difficult to pinpoint the exact reasons why these assessments were not carried out, we believe it is due to a lack of awareness of the privacy laws that are now in force in Brazil, in addition to a general lack of interest in taking these precautions.

PATHS FORWARD

Bringing the practices of Brazilian cities closer to the aspirations expressed in the country's policies will require a more deliberate approach to existing models of implementation and an openness to new options. **InternetLab, Article 19, and LAPIN call for both the public and the private sectors to adopt a series of practices aimed at ensuring security, transparency, and respect for human rights.** Below are three key recommendations we wish to highlight:

First, **municipal agencies as well as private contractors should make an effort to observe relevant standards for ICT projects**. In addition to national policy documents, such as the Brazilian Charter for Smart Cities, these standards should include those set by international technical bodies (such as the IEEE, ITU, ISO,

and IEC), and human rights commitments such as the UN Guiding Principles on Business and Human Rights. These global and national frameworks establish useful principles for new technologies in areas such as interoperability (systems should be able to work and exchange information with others from different companies), efficiency, and scalability, as well as indicators for assessing particular ICTs on these dimensions. They also contain valuable norms for smart city projects in particular (for instance, that municipal authorities should dictate the ethical, technical, and social principles that underlie a smart city's operation explicitly).

Second, where possible given security and capacity considerations, **smart city projects should make use of non-proprietary software so that the management of cities does not become dependent on specific companies**. When applied to technologies that are used to provide public services, private intellectual property rights can create governance challenges. For example, vendors that supply key systems to municipal agencies may gain a de facto monopoly over that municipality's future ICT contracts, as officials seek to maintain existing systems and acquire compatible ones. Consequently, such dependence may enable the chosen companies to extract rents from the municipal budget, burdening the public treasury, or exploit the data collected from municipal ICT systems, thus endangering citizens' privacy.

Third, **public agencies should not assume that cooperation amongst themselves or with private companies are the only viable paths to implementing ICT projects**. Municipalities can also employ more inclusive, bottom-up approaches that draw on the strength of diverse stakeholders within society—such as **CSOs, independent collectives, social movements, universities, and research institutes**. In 2022, the city of Contagem in southeast Brazil, for instance, has strengthened partnerships with CSOs to improve ICT systems, standardize administrative processes, and improve transparency in contract management.[55]

Municipal agencies and private contractors **should observe relevant standards** for ICT projects, such as national policies, technical standards, and human rights commitments.

Smart city projects **should use free software** where possible to avoid city management operations becoming dependent on specific companies.

Public agencies **should use more inclusive approaches** for implementing ICT projects—bringing in diverse stakeholders such as CSOs, independent collectives, social movements, universities, and research institutes.

Just as there is no accepted global definition of what a smart city is, we believe there is no formula for making a municipality "smart." Certainly, this endeavor is not limited to establishing offices or projects and acquiring ICTs. Instead, the path runs through a long process of **analyzing and understanding the local context and the social reality of each city**, from its geographical position and material resources to the interests, needs, and capacities of the population when it comes to engaging with particular technologies. Municipal authorities must **leverage public participation** to deepen their understanding of social inequalities; craft context-appropriate digital strategies; and more effectively guarantee democracy, access, and justice for all.

ENDNOTES

Smart Cities and Democratic Vulnerabilities

1 Marcus Michaelsen and Marlies Glasius, "Authoritarian Practices in the Digital Age," *International Journal of Communication* 12, (2018), 3788-3794.

2 David Belcher, "A New City, Built upon Data, Takes Shape in South Korea," *New York Times,* 28 March 2022, www.nytimes.com/2022/03/28/technology/eco-delta-smart-village-busan-south-korea.html.

3 Menna A. Farouk, "Saudi 'surveillance city': Would you sell your data to The Line?," Reuters, 23 August 2022, www.reuters.com/article/saudi-city-surveillance-idAFL8N2ZL0CM. This project, however, has been slow to materialize in practice—for more information, please see: Nicolas Pelham, "MBS: Despot in the Desert," *the Economist*, 28 July 2022, www.economist.com/1843/2022/07/28/mbs-despot-in-the-desert.

4 Katherine Atha et al., "China's Smart Cities Development," U.S.-China Economic and Security Review Commission, January 2020, www.uscc.gov/sites/default/files/China_Smart_Cities_Development.pdf.

5 For more information, please consult: Sidney Fussell, "The City of the Future Is a Data-Collection Machine," *the Atlantic*, 21 November 2018, www.theatlantic.com/technology/archive/2018/11/google-sidewalk-labs/575551/; Alissa Walker, "Sidewalk Labs' 'smart' city was destined to fail," Curbed, 7 May 2020, https://archive.curbed.com/2020/5/7/21250678/sidewalk-labs-toronto-smart-city-fail; and Moira Warburton, "Alphabet's Sidewalk Labs cancels Toronto 'smart city' project," Reuters, 7 May 2020, www.reuters.com/article/us-canada-sidewalk/alphabets-sidewalk-labs-cancels-toronto-smart-city-project-idUSKBN22J2FN.

6 Steven Feldstein et al., *The Global Struggle over AI Surveillance: Emerging Trends and Democratic Responses*, National Endowment for Democracy, June 2022, www.ned.org/wp-content/uploads/2022/06/Global-Struggle-Over-AI-Surveillance-Emerging-Trends-Democratic-Responses.pdf.

7 Katherine Atha et al., "China's Smart Cities Development."

8 Huirong Chen and Sheena Chestnut Greitens, "Information capacity and social order: The local politics of information integration in China," *Governance,* (2021), 1-27, www.sheenagreitens.com/uploads/1/2/1/1/121115641/chen__greitens_-_info_capacity__social_order__governance_2021_.pdf.

9 Samantha Hoffman, "China's Tech-Enhanced Authoritarianism," *Journal of Democracy* 33, 2 (2022), 76-89, https://muse.jhu.edu/article/852746.

10 Jonathan E. Hillman and Maesea McCalpin, *Watching Huawei's* "*Safe Cities,*" Center for Strategic and International Studies, 4 November 2019, www.csis.org/analysis/watching-huaweis-safe-cities; and for details on the spread of PRC Safe City projects, please see: https://chinatechmap.aspi.org.au/#/map/f5-Smart%20City-Public%20Security%20project,f6-Smart%20cities.

11 Chen and Greitens, "Information capacity and social order."

12 Dan Strumpf and Waqar Gillani, "Huawei Accused in Suit of Installing Data 'Back Door' in Pakistan Project," *Wall Street Journal*, 14 August 2021, www.wsj.com/articles/huawei-accused-in-suit-of-installing-data-back-door-in-pakistan-project-11628947988.

13 Samantha Hoffman, *Engineering global consent: The Chinese Communist Party's data-driven power expansion*, Australian Strategic Policy Institute, 14 October 2019, www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

14 Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, 15 August 2019, www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

15 For more information on the risks of dependence, please consult: Stefan Vladisavljev, *China's 'Digital Silk Road' Enters the Western Balkans*, China Observers in Central and Eastern Europe (CHOICE), June 2021, https://chinaobservers.eu/wp-content/uploads/2021/06/CHOICE_policy-paper_digital-silk-road_A4_web_04.pdf; and Stefan Vladisavljev, "Surveying China's Digital Silk Road in the Western Balkans," War on the Rocks, 3 August 2021, https://warontherocks.com/2021/08/surveying-chinas-digital-silk-road-in-the-western-balkans/.

16 For more information about Serbia's case, please see: Danilo Krivokapić, "Starting the Debate on Facial Recognition: A Case Study from Belgrade," part of Feldstein et al., *The Global Struggle over AI Surveillance: Emerging Trends and Democratic Responses*, June 2022, www.ned.org/wp-content/uploads/2022/06/Starting-Debate-on-Facial-Recognition-Case-Study-from-Belgrade-Krivokapic.pdf.

17 Bianca Wylie, "In Toronto, Google's Attempt to Privatize Government Fails—For Now," *Boston Review*, 13 May 2020, www.bostonreview.net/articles/bianca-wylie-sidewalk-labs-toronto/.

18 Dahlia Peterson, *How China harnesses data fusion to make sense of surveillance data*, Brookings Institution, 23 September 2021, www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/.

19 I am grateful to Samantha Hoffman for calling my attention to this issue. For more information, please see: "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, 1 May 2019, www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

20 Feldstein et al., *The Global Struggle over AI Surveillance: Emerging Trends and Democratic Responses*.

21 Henry Farrell, Abraham Newman, and Jeremy Wallace, "Spirals of Delusion: How AI Distorts Decision-Making and Makes Dictators More Dangerous," *Foreign Affairs*, September/October 2022, www.foreignaffairs.com/world/spirals-delusion-artificial-intelligence-decision-making.

22 Chen and Greitens, "Information capacity and social order." In addition, and as a possible variant on this theme, which Gulnaz Sharafutdinova describes in the case of Russia, is the introduction of digital platforms that selectively allow popular input on "non-political" aspects of urban governance in order to shore up support for the government.

23 Ben Green, *The Smart Enough City: Putting Technology in its Place to Reclaim Our Urban Future* (Cambridge, MA: MIT Press, 2020).

24 Priyal Bhatt, Chris Doten, and Jillian Gilburne, *Municipal Digital Transformation Guidebook: A guide for municipal leaders with the drive to embark on digital transformation programs*, National Democratic Institute, 2021, www.ndi.org/sites/default/files/Municipal%20Digital%20Transformation%20Guidebook_final%20%281%29.pdf.

25 Farrell et al., "Spirals of Delusion."

Is Digitalization Endangering Democracy in Mauritius?

26 "Digital Mautirius 2030," Ministry of Technology, Communication & Innovation, Government of the Republic of Mauritius, 17 December 2018, https://govmu.org/EN/communique/Documents/DM%202030%2017%20December%202018%20at%2012.30hrs.pdf.

27 "Autocratization Turns Viral: Democracy Report 2021," Varieties of Democracy Institute (V-Dem), March 2021, www.v-dem.net/static/website/files/dr/dr_2021.pdf.

28 "Mauritians' satisfaction with democracy reaches new low, Afrobarometer study shows," Afrobarometer, 9 June 2022, www.afrobarometer.org/wp-content/uploads/2022/06/mau_r9.news_release-mauritians_satisfaction_with_democracy_reaches_new_low_9jun22.pdf.

29 Jessica Fjeld et al., "Mauritius Is Considering an Unprecedented Attack on Online Freedom," *Slate*, 20 May 2021, https://slate.com/technology/2021/05/mauritius-online-speech-government-proxy-servers.html.

30 "Consultation Paper on proposed amendments to the ICT Act for regulating the use and addressing the abuse and misuse of Social Media in Mauritius," Information & Communication Technologies Authority (ICTA), 14 April 2021, www.icta.mu/documents/2021/10/Social_Media_Public_Consultation.pdf.

31 "Constitution of the Republic of Mauritius," Attorney General's Office of the Government of the Republic of Mauritius, 12 March 1968, https://attorneygeneral.govmu.org/Documents/Laws%20of%20Mauritius/A-Z%20Acts/C/Co/Constitution,%20GN%2054%20of%201968.pdf.

32 "Mauritius 2020 Human Rights Report," U.S. Department of State, 2021, www.state.gov/wp-content/uploads/2021/10/MAURITIUS-2020-HUMAN-RIGHTS-REPORT.pdf.

33 "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, 1 May 2019, www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

34 "Mauritius ICT Act Submission," Access Now, 12 May 2021, www.accessnow.org/cms/assets/uploads/2021/05/Mauritius-ICT-Act-Submission.pdf.

35 For more information, please see the Australian Strategic Policy Institute's "Mapping China's Tech Giants" interactive map here: https://chinatechmap.aspi.org.au/#/map/f2-Huawei.

36 For more information, please see: https://chinatechmap.aspi.org.au/#/map/f5-Smart%20City-Public%20Security%20project.

37 "The Data Protection Act 2017," Government of the Republic of Mauritius, 15 January 2018, https://dataprotection.govmu.org/Documents/DPA_2017_updated.pdf?csf=1&e=0rlrff.

38 Mauritius Telecom was selected to provide security equipment, related hardware and software and licenses to the Government of Mauritius for a contractual period of 20 years.

39 Huawei is the principal supplier of MSCP equipment.

40 Samantha Hoffman, "China's Tech-Enhanced Authoritarianism," *Journal of Democracy* 33, 2 (2022), 76-89, https://muse.jhu.edu/article/852746.

41 "Polémiques : Liying Zhu, ambassadeur de Chine « Je laisse le soin aux autorités d'enquêter »," *Le Mauricien*, 8 August 2022, www.lemauricien.com/actualites/societe/polemiques-autour-de-huawei-liying-zhu-ambassadeur-de-chine-je-laisse-le-soin-aux-autorites-denqueter/507262/.

42 Axcel Chenney and Florian Lepoigneur, "«Sniffing» allégué: pourquoi l'excuse Huawei avancée par Hurreeram est complètement bidon," *L'Express*, 31 July 2022, https://lexpress.mu/article/411747/sniffing-allegue-pourquoi-lexcuse-huawei-avancee-hurreeram-est-completement-bidon.

43 Praveen Swami, "How fears of Chinese digital espionage 'got RAW involved in Mauritius, led to snooping scandal'," *the Print*, 28 July 2022, https://theprint.in/world/how-fears-of-chinese-digital-espionage-got-raw-involved-in-mauritius-led-to-snooping-scandal/1055705/; and Axcel Chenney and Florian Lepoigneur, "«Sniffing» allégué: pourquoi l'excuse Huawei avancée par Hurreeram est complètement bidon."

Brazilian Smart Cities: From Principles to Practice

44 Blenda Santos, "Smart cities and data protection," InternetLab, 26 July 2022, https://internetlab.org.br/en/news/smart-cities-and-data-protection-possible-routes/. (Full article only available in Portuguese).

45 José Roberto Amaral, "São José é certificada a primeira Cidade Inteligente do Brasil," Prefeitura São José dos Campos, 16 March 2022, www.sjc.sp.gov.br/noticias/2022/marco/16/sao-jose-e-certificada-a-primeira-cidade-inteligente-do-brasil/.

46 Minister Rogério Simonetti Marinho et al., "The Brazilian Charter for Smart Cities: Short Version," eds. Almir Mariano de Sousa Júnior et al., Brazilian Ministry of Regional Development, 2021, www.gov.br/mdr/pt-br/assuntos/desenvolvimento-urbano/carta-brasileira-para-cidades-inteligentes/The_Brazilian_Charter_for_SmartCities_Short_VersionFinal.pdf.

47 "Câmara aprova lei que regula proteção de dados do município," Câmara Municipal de Vinhedo (Estado de São Paolo), 12 June 2018, www.camaravinhedo.sp.gov.br/portal/noticias/0/3/22289/camara-aprova-lei-que-regula-protecao-de-dados-do-municipio/.

48 "Quem Somos?," ANDUS (Apoio à Agenda Nacional de Desenvolvimento Urbano Sustentável no Brasil), 11 November 2020, www.andusbrasil.org.br/sobre-o-andus/quem-somos; and "Seleção do Projeto," ANDUS, (originally put forth August, 2015), 14 November 2020, www.andusbrasil.org.br/sobre-o-andus/linha-do-tempo.

49 This finding was one of the key conclusions outlined in a 2022 InternetLab report on the emergency aid transfer implemented in Brazil during the COVID-19 pandemic. For more information, please see: Clarice Tavares et al., "Emergency Aid in Brazil: Challenges in the Implementation of a datafied social protection policy," Derechos Digitales América Latina, February 2022, www.derechosdigitales.org/wp-content/uploads/03_Informe-Brasil_Artificial-Intelligence-and-Inclusion_EN_22042022.pdf.

50 "Children's Right to Privacy: Obstacles and agenda for privacy protection and the development of informational self-determination of children in Brazil," Alana Institute and InternetLab, February 2021, https://internetlab.org.br/wp-content/uploads/2021/03/ilab-alana_childrens-privacy_EN_20210214-1.pdf.

51 For more information, please consult: Larry Hardesty, "Study finds gender and skin-type bias in commercial artificial-intelligence systems," MIT News, 11 February 2018, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212; Jesse Damiani, "New Research Reveals Facial Recognition Software Misclassifies Transgender, Non-Binary People," *Forbes*, www.forbes.com/sites/jessedamiani/2019/10/29/new-research-reveals-facial-recognition-software-misclassifies-transgender-non-binary-people/?sh=49924d41606b; and Tom Simonite, "The Best Algorithms Struggle to Recognize Black Faces Equally," *Wired*, 22 July 2019, www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/.

52 "[Metrô] TJSP mantém proibição do uso de reconhecimento facial no metrô paulista," InternetLab, 29 April 2022, https://internetlab.org.br/pt/semanario/29-04-2022/#19066.

53 For more information, please visit the "Tire meu rosto da sua mira" ("take my face out of your sight") campaign website: https://tiremeurostodasuamira.org.br/en/home-eng/.

54 One of the most famous of these rankings is the "Ranking Connected Smart Cities," launched in 2015 and led by companies that sell market intelligence solutions. For more information, please consult: https://ranking.connectedsmartcities.com.br/.

55 "Prefeitura fortalece parcerias com Organizações da Sociedade Civil," Prefeitura de Contagem, 29 April 2022, www.portal.contagem.mg.gov.br/portal/noticias/0/3/75181/prefeitura-fortalece-parcerias-com-organizacoes-da-sociedade-civil.

ACKNOWLEDGMENTS

The authors appreciate the contributions of the International Forum's staff and leadership, including Christopher Walker, John Glenn, Kevin Sheives, John Engelken, Rachelle Faust, Lily Sabol, and Joslyn Brodfuehrer, all of whom played important roles in the editing and publication of this report. Particular acknowledgment goes to Beth Kerley, whose support and vision for this project were vital to its completion.

In addition, Roukaya Kasenally would like to acknowledge the Hoover Institution and its ongoing China's Global Sharp Power Project for which she wrote a paper entitled, "The Trappings of the Mauritius Safe City." She has used some of the findings outlined in that paper in this report.

Finally, the Forum wishes to thank Factor3 Digital for their efforts and invaluable support in designing this report for publication.

PHOTO CREDITS

Cover image: Photo by Vasin Lee/Shutterstock

Page 3: Photo by Blue Planet Studio/Shutterstock

Page 5: Photo by Tanawat Chantradilokrat/Shutterstock

Page 8: Photo by metamorworks/Shutterstock

Page 10: Photo by Sanchit Khanna/*Hindustan Times*/Shutterstock

Page 11: Photo by agilard/Shutterstock

Page 14: Photo by Nataly Reinch/Shutterstock

Page 18: Photo by fredex/Shutterstock

Page 19: Photo by Arnika Ganten/Shutterstock

Page 21: Photo by Joa Souza/Shutterstock