SMART CITIES AND DEMOCRATIC VULNERABILITIES

// BETH KERLEY / ROUKAYA KASENALLY / BÁRBARA SIMÃO & BLENDA SANTOS

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

// REPORT / DECEMBER 2022

SMART CITIES AND DEMOCRATIC VULNERABILITIES

CONTENTS

NED | NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM | INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

EXECUTIVE SUMMARY

Through "smart city" projects, municipal officials around the world are deploying digital tools to collect data about urban life, analyze trends, and automate governance. Billed as cutting-edge solutions for connectivity and efficiency, these projects—which leverage new capacities created by **artificial intelligence (AI) and the Internet of Things (IoT)**—pose a range of risks to democracy if not implemented following democratic principles of transparency and accountability. If mismanaged, they could serve as vectors for malign authoritarian influence; undermine procedural norms of good governance; and raise the specter of mass surveillance. The **global trend toward democratic backsliding** may exacerbate and, in turn, be exacerbated by these dangers.

Smart city projects pose a range of risks to democracy if not implemented following democratic principles of transparency and accountability.

This collection, the second in our "Making Tech Transparent" series, surveys the democracy risks posed by smart cities and examines how they are taking shape in two countries affected by backsliding: **Mauritius and Brazil**. It addresses the critical importance of **embedding smart city projects in participatory processes** that reinforce democratic norms, and the obstacles that currently exist to realizing this vision. Key points include:

- Smart cities are ultimately one of many arenas in which democratic principles are colliding with a **technocratic authoritarian vision built on data collection**, one championed by but in no way limited to the People's Republic of China (PRC). In order to leverage municipal digitalization for democracy and ensure that emerging technologies serve the societies which deploy them, bolstering and expanding mechanisms for **oversight and stakeholder engagement** will be key.
- Vendors based in the PRC, such as Huawei, are prominent in global smart cities sales. The significant presence of Huawei and other PRC-based firms in this industry raises particular concerns around the intertwining of digitalization with PRC political influence, as well as the uses to which the **data collected from smart cities** will be put. Yet risks from the transfer of both governance functions and personal data to private companies extend beyond those cases in which PRC vendors are involved.

- Often viewed as tools to make governance more transparent, accountable, and inclusive, emerging technologies also present increasingly clear **opportunities for current and aspiring authoritarians**. The trajectory of *Mauritius*, a leading African democracy that has recently struggled with backsliding, illustrates how smart cities fit within a broader arc toward **enhanced digital surveillance capacities** that are ripe for abuse, absent robust checks on executive power.
- Even where democratic principles for the management of smart cities have been elaborated, as we see in *Brazil*, **hasty, opaque, and irregular processes** around the procurement and deployment of these systems continue to undermine adherence to those norms. Thus, innovative approaches are needed to **protect citizens' privacy, mitigate human rights risks, and facilitate public participation** in decision making.

Innovative approaches are needed to protect citizens' privacy, mitigate human rights risks, and facilitate public participation in decision making.

Around the globe, initiatives like "smart cities" are supplying ever more fodder for technocratic visions of absolute control, raising a plethora of risks to human rights, state accountability, and institutional integrity. In this context, embedding digitalization within the robust give-and-take of democratic politics may be the only path toward ensuring that digital data and the imperfect maps it creates serve the interests of the human societies they depict, rather than holding these societies hostage.

SMART CITIES AND DEMOCRATIC VULNERABILITIES

// **BETH KERLEY,** PROGRAM OFFICER, INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES, NATIONAL ENDOWMENT FOR DEMOCRACY

INTRODUCTION

From the most established democracies to the "digital totalitarian" setting of the People's Republic of China (PRC), **"smart city" projects are transforming municipal governance**. Definitions of this broad term for municipal-level digitalization vary widely, sometimes encompassing relatively simple projects such as launching digital portals for public agencies or offering free public Wi-Fi.

Many smart city initiatives, however, **leverage the capacity of the Internet of Things (IoT) and artificial intelligence (AI)–powered analytics tools to monitor trends in urban life, identify challenges, and inform or even automate the provision of services**—from heating and waste management to public safety. Such initiatives promise increased efficiency and could even provide new opportunities for public engagement in municipal governance. Yet current approaches to these projects may be sidelining democratic deliberation and fueling authoritarian practices instead.[1]

Most current smart city projects promise in some way to streamline urban governance through the ongoing **collection and analysis of large volumes of data**. In an experimental "Smart Village" in South Korea, residents are sharing data collected by smart watches and smart home devices in exchange for rent-free living.[2] Saudi Arabia has been touting its plans for a vertically stacked city

called "The Line" that will draw on "residents' smartphones, their homes, facial recognition cameras, and a host of other sensors" to "feed information back to the city and help it predict user needs."[3] In the PRC—which as of January 2020 is already home to more than eight-hundred smart city projects—the U.S.-China Economic and Security Review Commission has observed, "[It] is clear . . . that the CCP [Chinese Communist Party] intends to use multiple smart city technologies to substantially augment and even revolutionize its mass surveillance capabilities."[4] In more democratic settings, the surveillance potential of smart cities can lead to pushback: a planned Sidewalk Labs initiative in Toronto featuring heated streets and computer vision-enabled cameras was cancelled in 2020 amid both economic woes and a lawsuit over "data surveillance."[5]

DEFINING THE CHALLENGE

Smart cities are a sometimes underappreciated part of a broader narrative in which digital tools once expected to put political participation within easy reach are also proving to be powerful instruments of manipulation and control. They underscore that this trajectory involves not only the sphere of online discourse but also governance processes and the physical world.

Digital tools once expected to put political participation within easy reach are also proving to be powerful instruments of manipulation and control.

The democracy risks around smart cities span multiple fronts and include the *authoritarian actors* frequently involved in their design and operation; the *opaque and irregular processes* by which they come into being; and the *data-collection capacities* they create. Both individually and in combination, these risks threaten to erode rule-of-law norms. They also produce privacy hazards with the potential to fuel discrimination, enable political manipulation, and chill civic participation. On all these fronts, risks can be exacerbated by pre-existing illiberal trends or weaknesses in oversight institutions.

Although the PRC's development and export of "smart city" tools together with the Sidewalk Labs case may have received the greatest share of attention, smart cities are a global phenomenon. In particular, these projects are a major presence in what Steven Feldstein described in a recent report for the International Forum for Democratic Studies as **"swing states"**: "partly open political settings where key liberal-democratic guardrails are weakened or absent in ways that could heighten the appeal of authoritarian digital models."[6] These and other political settings marked by democratic backsliding are fertile grounds for the development of the authoritarian potential inherent in technologies that involve an unprecedented monitoring of daily life.

Autocratic actors

With regard to *actors*, the PRC's leading role in smart city exports has alarmed democracy advocates. **China has made smart cities-related technologies (including cloud computing, big data, and IoT) a top-level priority** and exported such tools to more than a hundred countries.[7] At home, these projects

A Huawei CCTV camera installed in Suvarnabhumi Airport in Bangkok, Thailand.

fit within a wider web of technical and institutional practices for **integrating information from different sources in the service of social control**.[8] As Samantha Hoffman relates, smart city projects can fuse "the everyday provision of basic publics goods" with "the projection of authoritarian power." She explains, "[F]or instance, a smart electricity meter can improve the accuracy, transparency, and reliability of readings, to the benefit of the utility and its customers. For police, the data from that same meter can help to detect 'abnormal' behaviors indicative of 'illegal' gatherings."[9]

Thus, one major question around PRC-sponsored smart city projects concerns whether, when other governments purchase these technologies from vendors such as Huawei, the digital authoritarian model will come along for the ride. On this front, it is noteworthy that **Huawei "Safe Cities"—a security-focused spinoff of the smart cities concept** that features surveillance systems such as "command centers, CCTV cameras, intelligent video surveillance, facial and license plate recognition technology, crowd monitoring, situational awareness detection, noise monitoring or detection, abandoned object detection, and social media monitoring"—are spreading globally, particularly in countries classified as "Not Free" or "Partly Free" by Freedom House.[10]

Even if the PRC's surveillance systems end up working somewhat differently outside the highly specific social and institutional authoritarian frameworks in which they are embedded at home,[11] they may still end up strengthening autocrats or undermining democratic governance in a range of other ways.

Authorities in Beijing may gain access to sensitive host country data through **surreptitious "backdoors,"** as recently observed in a law enforcement database in Pakistan.[12] Even "legitimately" collected data could **help PRC state entities to hone their propaganda** and other tools for manipulating foreign societies, as Samantha Hoffman has persuasively argued.[13] Security-centric smart city projects together with PRC know-how could encourage governments in closed or semi-closed settings to **intensify their monitoring of political opponents**; Huawei technicians were found to have assisted with such activity in Uganda and Zambia.[14] Finally, growing dependence on PRC digital infrastructure could in turn provide Beijing with new and dangerous **leverage over the politics of importing countries**.[15]

Good governance hazards

At the same time, it bears noting that some *procedural concerns* are common to both PRC smart city projects and those involving vendors based in democracies. In the essays that follow, Roukaya Kasenally—scrutinizing a Huawei Safe City project in Mauritius—and Bárbara Simão and Blenda Santos—examining the multi-vendor smart city landscape in Brazil—similarly stress the challenge of opacity. Authorities are frequently disinclined to disclose information about the contracts through which they procure smart city technologies. This reluctance is particularly worrisome when those contracts involve high-level deals with PRC vendors that **circumvent standard public procurement procedures**, as we observe in cases from Mauritius to Serbia.[16] But the problem is not exclusive to these cases.

Authorities are frequently disinclined to disclose information about the contracts through which they procure smart city technologies.

Opacity can also be linked to a **failure to solicit community input** or conduct appropriate human rights impact assessments for smart city projects, as Simão and Santos document. If officials commissioning these projects do not prioritize input from below, the package deals offered by private vendors can instead end up setting public agendas. In such circumstances, these projects can amount, in Bianca Wylie's words, to "the outsourcing of public governance to a for-profit actor."[17]

The specter of mass surveillance

These procedural shortcomings are particularly concerning because smart city projects create new *capacities*, especially in the surveillance domain, that could **amplify unaccountable government and corporate power** at the expense of public engagement. Many smart city projects include controversial facial recognition tools overtly designed for surveillance, nominally to fight crime. Yet as Simão and Santos note, smart city initiatives in fields such as education or connectivity also tend to involve the **collection, or provision to vendors, of large volumes of personal data**.

Where frameworks to guide the handling of this data are absent or inadequate, there is little guarantee that it will not be leveraged in ways that are discriminatory or enable political manipulation. As Kasenally observes

in Mauritius, even when data protection frameworks are formally in place, national-security clauses may give executive branch officials considerable unilateral discretion over data handling. In backsliding democracies where those same officials have a record of engaging in practices that violate civil liberties or trample on checks and balances, this situation is cause for concern.

Moreover, data collection in smart cities presents something more serious than simply the series of independent, project-level risks associated with each new smart streetlight or energy meter. In the PRC, we can already observe how **digital platforms for "data fusion"** enable the integration of different data streams—drawn from both digital spaces such as WeChat accounts and physical ones such as streets monitored by facial-recognition cameras—to monitor individuals and predict social trends.[18] Such practices are used to their most devastating effect in the Integrated Joint Operations Platform that flags potentially "dangerous" individuals to police in Xinjiang.[19]

Across all three fronts, **underlying weaknesses in democratic institutions aggravate the risks of smart city projects**. Where checks and balances are weak and decisions are made behind closed doors by a small circle of elites, officials may be likelier to underestimate—or simply discount—the dangers of entanglement with vendors based in autocracies. They may also have fewer incentives to assess the human rights impacts of projects at the design stage or implement appropriate data protection safeguards. Feldstein's research on digital repression has shown "a strong relationship between curtailments of political liberties and subsequent government abuse of surveillance technologies." This tendency could produce a vicious feedback loop linking smart city risks to democratic backsliding.[20]

Underlying weaknesses in democratic institutions aggravate the risks of smart city projects.

DIGITALIZATION AT A CROSSROADS

The PRC's dystopian practices underscore that smart cities are one of the many arenas in which **democratic societies are colliding with a digitally powered vision that threatens to corrode their basic normative fabric**. That vision involves not only bolstering state capacities for surveillance and control, but also cutting out the messy (albeit necessary) feedback mechanisms of open societies.

As digital systems with authoritarian affordances come to be more widely available, this model is becoming a dangerous temptation for democracies and "swing states" as well. Although appearing in the guise of hyper-efficient "solutions" to optimize good governance for a modern state, digital projects that follow this vision can also be a means for illiberal actors to install **new levers of social manipulation** at the public's expense. Ultimately, they may intensify such potent challenges to democracy as popular alienation from governance systems and the erosion of institutional accountability.

Writing in *Foreign Affairs*, Henry Farrell, Abraham Newman, and Jeremy Wallace argued that authoritarians will **see AI tools as an alternative to popular political participation**—a system that can tip authorities off to potential problems and "tell rulers whether their subjects like what they are doing without the hassle of surveys or the political risks of open debates and elections."[21] PRC smart city projects that use a web of sensors and "city brains" to handle local governance challenges fit neatly within this rubric. Down to the most local level, authorities "use data integration platforms to decide whether local challenges are best resolved via service provision or via more coercive forms of demobilization."[22]

But the aspiration for automated tools that can obviate the need for democratic feedback is by no means limited to autocratic settings. It is, rather, the logical endpoint of a technocratic impulse present in all too many democratic polities. In *The Smart Enough City*, Ben Green has described how smart city projects can reflect and encourage a prioritization of technical means over social ends. In other words, municipal authorities presume that their main responsibility is identifying the best technological tool for achieving what they presume to be an uncontroversial goal—often described in terms of "efficiency"—rather than engaging the pluralistic societies they govern to achieve a better understanding of what their goals should be. In such instances, **putative technological fixes can serve as a distraction from addressing underlying social issues**.[23] As our colleagues at the National Democratic Institute have argued, "Obsession with innovative technologies can overshadow better, less technical solutions."[24]

In today's unstable, ever-shifting social and economic landscape, governments may take comfort in a digital vision that elides unpredictable, fraught, and contentious processes of popular consultation. The preceding reflections and the essays that follow nonetheless underscore the **crucial importance of both formal and informal democratic institutions** to sound decision making about smart cities. They are vital not only to protecting civil liberties, but also to ensuring basic good governance. Farrell, Newman, and Wallace argue that authoritarians' aspiration to make data a substitute for dialogue is likely to backfire:

> *Although ubiquitous state surveillance could prove effective in the short term, the danger is that authoritarian states will be undermined by the forms of self-reinforcing bias that machine learning facilitates. As a state employs machine learning widely, the leader's ideology will shape how machine learning is used, the objectives around which it is optimized, and how it interprets results. The data that emerge through this process will likely reflect the leader's prejudices right back at him. . . . Instead of good policy, this will lead to increasing pathologies, social dysfunction, resentment, and, eventually, unrest and instability.*[25]

In this context, repressive digital systems aimed at maintaining "social stability" while denying the public a voice may instead end up exacerbating the governance challenges facing societies worldwide, as citizens grow increasingly alienated from distant, opaque, and unresponsive institutions.

Repressive digital systems aimed at maintaining "social stability" may instead exacerbate the governance challenges facing societies worldwide.

LOOKING FORWARD

Because the complex issues surrounding personal data collection and relationships with smart city vendors are challenging for even the most established democracies to manage, identifying promising, participatory models in this space is perhaps more difficult than naming the risks. It is, however, worth noting that inspiration on this front may come from the ranks of younger democracies and other "swing states." Simão and Santos note that **Brazil**, for all its recent political struggles, has issued **national-level policies that propose important democratic norms for municipal digitalization**, including a Charter for Smart Cities that was itself developed through wide consultation with civil society. These guidelines address issues such as respect for rights, stakeholder engagement, and mindfulness of how new digital projects intersect with socioeconomic inequalities. Building on joint research from Internet Lab, Article 19, and LAPIN, Simão and Santos also propose that cities consider alternate pathways for smart city development, such as **collaborations with social collectives or universities** rather than traditional vendors.

Digital advances are further facilitating technocratic visions of absolute control. In this context, understanding the limits of data-driven technologies and opening up space for input from civil society, accountability institutions, and the broader public is crucial to guarding against both human rights risks and cross-border authoritarian influence. At the same time, **embedding digitalization within the robust give-and-take of democratic politics** may be the only path toward re-establishing an even more fundamental form of control: the power to ensure that digital data and the imperfect maps it creates serve the interests of the human societies they depict, rather than holding these societies hostage.

Drones being used to get surveillance inside a Polling booth in New Delhi, India.

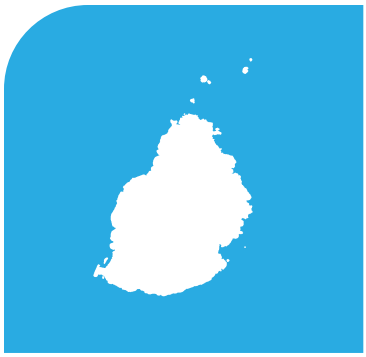
IS DIGITALIZATION ENDANGERING DEMOCRACY IN MAURITIUS?

// **ROUKAYA KASENALLY,** ASSOCIATE PROFESSOR, UNIVERSITY OF MAURITIUS

Digitalization has long been a prestige project for the government of Mauritius. In this regard, **the 2019 launch of a Safe City—a security-focused digitalization initiative using Huawei equipment and funding from the PRC—on this small island state fit within a well-oiled public rhetoric promising economic growth, global connectivity, and innovation**. Yet it is one of several recent projects in the digital sphere that could hasten the erosion of Mauritian democracy.

Reflecting a vision pursued by successive governments over the last thirty years, Mauritius boasts a well-developed ICT infrastructure. In the past decade, authorities have implemented **connectivity and e-governance initiatives** including the National Smart ID Card (2013), Open Data Mauritius (2015), the provision of 350 free Wi-Fi hotspots across the island (2017), the launch of a Citizen Support Portal (2017), the Mauritius Safe City Project, or MSCP (2019), and the rollout of 5G across the island (since 2021). The current focus is on achieving the goals set out in **"Digital Mauritius 2030,"** a policy blueprint that emphasizes digital government, ICT infrastructure, innovation, talent management, and cybersecurity.[26] Recently, however, this impressive technological trajectory has proceeded in tandem with a worrying political downturn.

Over the last five years, Mauritius has experienced significant democratic backsliding. It was classified by the V-Dem institute last year as among the "ten most rapidly autocratizing countries in the world,"[27] and only 32 percent of respondents in the most recent Afrobarometer public opinion survey expressed satisfaction with "the way democracy works in Mauritius."[28] Worrying trends include arbitrary arrests of journalists and other citizens, amendments to broadcasting and digital legislation, closures of certain private radio stations, the political weaponization of the police, and the weakening of key oversight institutions. This state of affairs can be attributed to a leader-centric political culture in which decision-making power is increasingly concentrated in the hands of one person. Over the last decade, these trends have intensified, giving rise to entrenched impunity, sycophantic behavior toward the country's leadership, and money-driven politics.



Mauritius is one of the "ten most rapidly autocratizing countries in the world"

At the very least, Mauritius's trajectory challenges any lingering assumptions that going digital automatically translates into greater transparency, accountability, and inclusion. But two recent initiatives suggest that the challenge runs deeper. **Together with a recent proposal by the country's Information and Communication Technologies Authority (ICTA) for regulating social media, the MSCP illustrates how the country's burgeoning digital ecosystem is offering both domestic and foreign actors alarming new powers through control over data.** These projects underscore the dangers of digital development in the absence of firm democratic guardrails; the difficulty of determining when projects launched in the name of enhancing public safety are actually tools for political surveillance; and the threats that opaque cross-border digital entanglements, particularly with authoritarian powers, can pose to democracy.

THE PUSHBACK AGAINST ONLINE SURVEILLANCE

In Mauritius's online sphere, an **attempted "authoritarian power grab"[29] involving new digital capabilities** was rebuffed last year amid massive local and international pushback. Although the proposal was put on hold, the debate around it illustrated how digital advances can enable or hasten democratic backsliding—in this case, one toward closing civic space online.

In April 2021, the ICTA released a consultation paper on "regulating the use and addressing the abuse and misuse of social media."[30] Its stated purpose was setting out a strategy to address "harmful and illegal online content" that would not depend on international social media companies. To this end, the paper proposed introducing a new decision-making body on online content, a technical enforcement unit, and a technical toolset.

The toolset, the provision that sparked the greatest outrage, would have served to separate social media data out from the broader flow of internet traffic in and out of Mauritius. After this division, **social media data would be routed through a government proxy server and "decrypted, re-encrypted and archived for inspection purposes as and when required."** ICTA justified the proposals as in sync with measures proposed or adopted to regulate online content in other democracies, such as Germany, the U.K., France, and India.

Although these countries have introduced requirements for social media platforms to take down certain categories of content, none of them have deployed a "technical toolset" allowing government officials to directly intercept and remove such content. The proposed measures also contravened rights enshrined in the Mauritian Constitution, which guarantees "freedom to . . . receive and impart ideas and information without interference."[31]

These intrusive proposals present particular concerns given a recent **trend toward suppression of civic activity online**, which has intensified since the most recent general election, held in 2019. Acts of repression have included the arrests of citizens who posted "anti-government comments," "routine" blocks on opposition politicians' social media accounts, and removal of these politicians' posts criticizing the government.[32] **Such incidents add force to concerns that the ICTA proposal was, in fact, aimed at suppressing dissent** on social media platforms, which have become extremely popular civic fora for politicians, CSOs, and ordinary citizens.

In this context, channelling social media traffic through government-controlled servers could fundamentally change the conditions for civic expression. Moreover, international precedents exist—most notably in the PRC—for the integration of social media data with data collected via offline surveillance in order to track individuals and intensify social control.[33]

The ICTA recommendations acted as a wake-up call for Mauritian citizens. ICTA received **more than 1,500 citizen submissions** concerning the document, civil society groups forcefully condemned the proposals, and sectors of the media decried the tactics used to advance them. This outcry ultimately caught the attention of international advocacy groups, which released a "joint civil society statement" asking the Mauritian Government and ICTA to "retract the consultation paper which proposes radically disproportionate measures to counter offensive speech on social media and presents a threat to human rights."[34] Observers believe that this **concerted approach by both local and international civil society** was a determining factor in shelving the proposal.

Channeling Mauritius's social media traffic through government-controlled servers could fundamentally change the conditions for civic expression.

Huawei advertising in Accra, Ghana.

THE QUIET SPREAD OF OFFLINE SURVEILLANCE

As with the ICTA proposals, Mauritius's democratic backsliding provides important context for the launch of the **Mauritius Safe City Project (MSCP)**. The Safe City Project emerged through an opaque, irregular process that evinces further erosion of the country's democratic guardrails. At the same time, broader political trends in Mauritius lend extra credence to concerns about the ends to which the MSCP's data collection capacities will ultimately be put. Yet in contrast to the outcry that followed ICTA's social media proposals, the installation of surveillance systems in Mauritius's physical public square has proceeded with remarkably little debate. Citizens have little to no understanding of the project. The only resistance to this initiative came from opposition parliamentarians who regularly questioned the MSCP, raising concerns about its financing, the absence of a legal or regulatory framework, and other accountability gaps. Subsequently, some media outlets started covering the MSCP. Amid this scrutiny, **the government hid behind the confidentiality clauses signed between the different parties involved in the project: the Mauritian police, the Mauritius Telecom, and Huawei**.

First announced in 2016, the MSCP is **one of more than twenty Huawei-backed smart or "Safe" city projects across the African continent**.[35] "Safe Cities" technologies are a relatively new feature of the African digital ecosystem. For this reason, there has not been much in-depth research into their impact on local political, economic, and social dynamics. The case of Mauritius, however, suggests cause for concern.

One of the MSCP's core justifications has been safety and security, and this focus is reflected in the project's technical makeup. As of its official launch in December 2019, the project entailed the installation of **four-thousand cameras with facial recognition and license plate recognition capabilities**, of which 2,760 are now fully operational, in addition to "a command and control centre and seven subcommand centres . . . cloud computing services, data centres, intelligent road surveillance and emerging communications equipment and services."[36] Tellingly, however, various interlocutors (including parliamentarians) have informed this author that they have on different occasions gone to the police to ask for the retrieval of images from the Safe City cameras pertaining to crimes committed in their constituencies but were told the cameras were not working or that they did not have access to the images. Moreover, the country's Safe City cameras allegedly failed to capture any information pertaining to the suspicious death (suspected murder) of a ruling party political agent in 2020.

The real intent behind the MSCP, which runs a total cost of US$455 million—financed by a loan from the Export-Import Bank of China—remains unclear. The project was casually announced in the Mauritian National Assembly during the national budget discussion and has "succeeded" in evading all forms of oversight ever since. **Confidentiality clauses** obscure the contracts among the key stakeholders involved. Furthermore, officials decided to **waive a competitive bidding requirement** for public procurements in order to select Mauritius Telecom to operate and maintain the MSCP. Some question whether this company's status as a para-statal body **outside the financial scrutiny of parliament and the government's own auditors** leaves the public largely in the dark about the project's actual cost.

Critical questions about how the MSCP will affect Mauritian politics against the backdrop of the country's recent democratic backsliding are also unanswered. Specifically, will data collected by MSCP cameras that are pumping images on a 24/7 basis serve to advantage or undermine particular political actors? Also, what safeguards are in place to ensure that these images will be secure from manipulation or misuse? It is believed that Mauritius has one of the best data protection laws in Africa; however, there is a **clause that authorizes the prime minister to override data protection safeguards in the interest of "national security, defence or public security**."[37]

Particularly in light of the island's recent shift toward authoritarianism, observers have voiced concerns that this concentration of personal power could enable political interference in data handling, including the abuse of Mauritius's new surveillance tools to control, manipulate, or intimidate opponents. These concerns are exacerbated by **opacity regarding the division of responsibilities among the different players involved—the Mauritian Police, Mauritius Telecom,[38] and Huawei**[39]—which makes it difficult to say who "owns" the data from the MSCP.

A final "red flag" concerns the role of Huawei within the MSCP. **Huawei is the main promoter of the "Safe Cities" across Africa and beyond.** Scant information has been disclosed about the exact nature of the controversial PRC company's role in conceiving and managing the MSCP. What can be ascertained so far is that Huawei approached the Government of Mauritius in early 2015 with an **unsolicited bid for setting up the MSCP**. Why was that so? Why did the Government of Mauritius respond positively? And whose model of safety or surveillance is being realized—one bounded by democratic norms and safeguards, or one premised on the pervasive government monitoring that underpins PRC digital authoritarianism?

A final "red flag" concerns the role of Huawei within the MSCP.

BETWEEN DEMOCRATIC BACKSLIDING AND FOREIGN DIGITAL ENTANGLEMENT

Like many backsliding democracies, Mauritius is now the site of a high-budget urban digitalization project that is transforming where and how authorities can surveil citizens. This project has been shrouded in secrecy, unfurling in a way that has **subverted democratic norms around government transparency, competitive procurement, and institutional accountability**—and potential malfeasance by local authorities is not the only cause for concern.

Huawei's role in the MSCP illustrates the particular risks that **engagement with foreign tech vendors** can present in the context of democratic backsliding. These kinds of projects present opportunities for politically influenced deals that subvert good governance norms, the import of undemocratic digital models from actors like the PRC, and the collection of sensitive data that could enable Beijing to further hone its tools of political influence.[40]

In its quest for greater digital connectivity and security, Mauritius has relied heavily on two foreign countries: the PRC and India. Both powers have aggressively expanded their footprint on the island over the last decade. In addition to its role in the MSCP, **Huawei has been instrumental in developing Mauritius's internet infrastructure**, including 3G (2004), 4G (2012), and 5G networks (2021), as well as the Mauritius Rodrigues Submarine fiberoptic cable (MARS). The current Chinese Ambassador to Mauritius has touted Huawei's role in enabling Mauritius to take its place "among the key contenders in the region."[41]

A Mauritian government minister recently took a dimmer view of the matter, publicly declaring that "the ex-CEO of Mauritius Telecom has surrendered our country completely to Huawei."[42] In addition to these concerns, it was recently disclosed that India—with Mauritian government permission—had used special equipment to "sniff" (intercept and retain) traffic on one of the submarine cables carrying internet data into and out of Mauritius, an action prompted by concerns about PRC digital espionage using Huawei infrastructure. These disclosures have triggered political scandal and a diplomatic mess for the island state.[43]

So, it is fitting to ask: Who is digitalization really benefitting? Will Mauritius's democratic institutions have control over the country's digital trajectory, or will that trajectory instead be shaped by opaque deals, growing concentrations of power, and unaccountable foreign actors? Mauritius sits amid a geopolitical battleground, the Indian Ocean, where key contenders—the U.S., the U.K., France, and India—have already secured a strategic foothold and where Beijing is desperately trying to mark its presence. It seems that data could be the most sought after resource. **In the MSCP, foreign digital influence and next-generation surveillance powers have converged with remarkably little public debate, let alone oversight.** If these key accountability mechanisms are not re-engaged, the flow of digital data could deal a further blow to Mauritian democracy.

If key accountability mechanisms are not re-engaged, the flow of digital data could deal a further blow to Mauritian democracy.

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.

ABOUT THE CONTRIBUTORS

ABOUT THE CONTRIBUTORS

Beth Kerley is a program officer with the research and conferences section of the National Endowment for Democracy's International Forum for Democratic Studies. She manages the Forum's emerging technologies portfolio, which covers the challenges and opportunities for democracy as technological advances such as machine learning, the Internet of Things, and big-data analytics supply new tools of politics and governance. She was previously associate editor of the *Journal of Democracy*, and holds a PhD in History from Harvard University and a Bachelor of Science in Foreign Service from Georgetown University.

Roukaya Kasenally is a democracy scholar and associate professor at the University of Mauritius. She is associated with several institutions, as the Chair of the Electoral Institute for Sustainable Democracy in Africa (EISA), a member of the International Advisory Board of the Electoral Integrity Project (EIP), and Series Editor of 'Small State Studies' (Routledge). Kasenally has researched and published in the area of democratic and media governance. Her most recent work has been on the cost of politics (2020), elite accountability in Africa (2021), and intrusive technology in Africa (2022). She was also a Reagan-Fascell Fellow at the National Endowment for Democracy and held another fellowship at Stanford University. Kasenally has a PhD from University of Sheffield, U.K.

Bárbara Simão is the head of research for privacy and surveillance at InternetLab. She previously worked as a digital rights researcher at the Brazilian Institute for Consumers Defense (IDEC) between 2017 and 2020. She was also a project advisor on "Data Protection in Digital Health Services" at Fiocruz. She earned a Master's degree in Law and Development from Fundação Getúlio Vargas (FGV) and a Bachelor's degree at the Law School of the University of São Paulo (FDUSP). Follow her on Twitter: @psbarbara.

Blenda Santos is a researcher for privacy and surveillance at InternetLab. She is also a researcher at the Research Group on Interpretations of Brazil and Discrimination Markers in a Global Perspective project affiliated with the Federal University of Bahia (UFBA) and the Brazilian National Council for Scientific and Technological Development (CNPq) since 2020. She was previously a researcher at the Research Group on Human Rights, Right to Health and Family initiative affiliated with the Catholic University of Salvador (UCSal) and CNPq (2016-2018) and the Research Group on Crime in Latin America UCSal (2017). She earned a Master's degree in International Relations from the Federal University of Bahia and a Bachelor's Degree in Law from the Catholic University of Salvador (UCSal).

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

The International Forum for Democratic Studies at the National Endowment for Democracy (NED) is a leading center for analysis and discussion of the theory and practice of democracy around the world. The Forum complements NED's core mission—assisting civil society groups abroad in their efforts to foster and strengthen democracy—by linking the academic community with activists from across the globe. Through its multifaceted activities, the Forum responds to challenges facing countries around the world by analyzing opportunities for democratic transition, reform, and consolidation. The Forum pursues its goals through several interrelated initiatives: publishing the *Journal of Democracy*, the world's leading publication on the theory and practice of democracy; hosting fellowship programs for international democracy activists, journalists, and scholars; coordinating a global network of think tanks; and undertaking a diverse range of analytical initiatives to explore critical themes relating to democratic development.

The National Endowment for Democracy (NED) is a private, nonprofit foundation dedicated to the growth and strengthening of democratic institutions around the world. Each year, NED makes more than 1,700 grants to support the projects of nongovernmental groups abroad who are working for democratic goals in more than 90 countries. Since its founding in 1983, the Endowment has remained on the leading edge of democratic struggles everywhere, while evolving into a multifaceted institution that is a hub of activity, resources, and intellectual exchange for activists, practitioners, and scholars of democracy the world over.

1201 Pennsylvania Avenue, NW
Suite 1100
Washington, DC 20004
(202) 378-9700
ned.org


@thinkdemocracy


ThinkDemocracy