EUI SCHOOL OF TRANSNATIONAL GOVERNANCE

STG Policy Papers

POLICY BRIEF

CHINA'S TECH SURVEILLANCE APPLICATIONS IN EUROPE AND LATIN AMERICA: ANALYSING THE IMPACT ON DEMOCRATIC GOVERNANCE

Authors:
Ronald Sáenz Leandro, Carlos Saura García

ISSUE 2024/17
JULY 2024

Florence School of Transnational Governance

EXECUTIVE SUMMARY

This policy brief explores the extensive deployment of Chinese AI and machine learning technologies across Europe and Latin America in social surveillance. Over the past decade, these technologies have become deeply integrated into the security frameworks of numerous nations, enhancing capabilities in image classification, facial recognition, video analysis, and voice identification. As one of the world's leading providers, China's big tech companies equip governments with sophisticated tools that facilitate unprecedented monitoring and data collection. The analysis presents contrasting contexts of the application of surveillance structures, taking two cases from Europe and another two cases from Latin American countries to highlight the spread and the use of these types of technologies in different geographical scenarios. In the report's final section, we summarise some challenges posed by China's surveillance technologies and elaborate on some recommendations for policymakers, civil society organisations, government officials, and researchers to study and address the negative impacts of these structures on democratic governance.

Authors:

Ronald Sáenz Leandro | Visiting Fellow, Chair in Artificial Intelligence and Democracy, Florence School of Transnational Governance (STG), EUI

Carlos Saura García | Visiting Fellow, Chair in Artificial Intelligence and Democracy, Florence School of Transnational Governance (STG), EUI

1. INTRODUCTION

The technologies of massive social surveillance based on artificial intelligence (AI) and machine learning (ML) have matured and rapidly expanded worldwide over the past five years. The increasing integration of AI into urban infrastructure has transformed cities into more digitised environments, significantly contributing to resource management and urban security.

In recent times, there has been a proliferation of surveillance systems, which have been employed to monitor compliance with social distancing measures during the COVID-19 pandemic. These systems have been designed to mitigate the spread of the virus. Additionally, there have been attempts to utilise AI in traffic management and public transportation to optimise mobility and road safety.

Nevertheless, **the extensive utilisation of these instruments has also prompted ethical concerns, particularly about privacy and citizen surveillance.** Despite their efficacy, it has been postulated that digital tracking measures necessitate a balance between innovation and responsible conduct to prevent the infringement of individuals' privacy and to guarantee the protection of civil rights.

In 2019, over 40% of countries worldwide were already utilising AI-linked technologies for extensive social surveillance based on image classification, facial recognition, video analysis, or voice identification by creating biometric systems for human facial analysis. **It is important to highlight that within this group of countries there are more democratic governments than authoritarian regimes**. Establishing smart or safe cities with thousands of sensors and cameras transmitting real-time data and images is a further example of using AI-linked technologies. Similarly, the application of intelligent policies in areas such as justice, crime prosecution and prediction, or investigations, and the monitoring of social platforms to analyse and control communications on the network are further examples of the use of AI-linked technologies.

In the context of the broader ecosystem of social surveillance technologies, it is crucial to acknowledge that China, through its major technology corporations, is the primary global supplier of tools enabling other governments and public institutions to carry out surveillance practices at all levels. This fact presents both significant opportunities and challenges for democratic governance.

This policy brief explores the extensive deployment of Chinese AI and machine learning technologies across Europe and Latin America in social surveillance. To reach this goal, our analysis presents two European case studies and another two from Latin American countries to examine their implications, summarise the most critical challenges posed by China's surveillance technologies, and elaborate recommendations for policymakers, civil society organisations, government officials, and researchers to study and address the negative impacts of these structures on democratic governance.

2. CASES: CHINA'S AI SURVEILLANCE TECHNOLOGY IN EUROPE AND LATIN AMERICA

2.1. EUROPE

2.1.1. The case of Serbia

Serbia and China's economic and political ties have become more robust over the past two decades. Initially, in 2009, a strategic collaboration agreement was signed between the two countries' governments.

Subsequently, in 2015, memorandums were signed for Serbia's entry into the Belt and Road Initiative (BRI), a global initiative promoted by the Chinese government. In 2017, the Serbian government reached a strategic agreement with the Chinese technology corporation Huawei to create and manage a social surveillance system in Serbia, particularly in Belgrade. This system, known as the "Safe Society" project, was designed to monitor and control public spaces' activities and increase citizens' security.

In the project's first phase, 100 video surveillance cameras were installed in 61 different locations in Belgrade. The surveillance infrastructure implemented in this phase implemented video cameras with advanced technologies that enable them to detect, analyse and search for faces, objects and behaviours continuously and uninterruptedly, and also created a data and connection centre of the Serbian Ministry of Interior, managed by Huawei, where all video, images, information and data from the cameras are stored, shared and analysed. In a second phase, starting in 2019, the number of video cameras increased to 1,000 in 800 locations in Belgrade and its surroundings and the Huawei 5G network infrastructure was installed on the streets. In the next few years, video cameras will be gradually increased, enhanced, and introduced in the vehicles and suits of the country's security forces.

2.1.2. The case of Sardinia (Italy)

In 2019, the Italian government joined China's BRI, which led to an increase in economic and political relations between institutions and companies of both countries, especially in infrastructure and connectivity projects. However, it is essential to note that Italy withdrew from the project in 2023.

Before this initiative, there were some interactions between Italian and Chinese institutions, in particular agreements between the government of Sardinian region and the Chinese technology company Huawei, signed in 2016, to develop an intelligent region across the island of Sardinia with Huawei technology, launch various safe cities (including the town of Cagliari) and establish a data storage and processing centre on the island.

The implementation of the Safe City in Cagliari has involved the creation of a digital infrastructure based on the placement of sensors and surveillance cameras in various locations throughout the city, as well as drones flying over the city, all connected to the data centre. This digital infrastructure aims to continuously and uninterruptedly monitor weather conditions, traffic movements, and people's behaviour in the city. Introducing new technologies for massive social surveillance in the sensors and cameras, such as facial recognition, number plate recognition, intruder detection or behavioural and emotional analysis, has allowed the development of invasive techniques for detecting, analysing, and searching for specific elements or individuals.

2.2. LATIN AMERICA

2.2.1. The case of Ecuador

In recent years, Ecuador has taken significant steps towards integrating technology into its emergency response systems. A critical development in this area is the ECU 911 project, an emergency response system that utilises technology for surveillance and rapid response coordination. This initiative began in 2012 and is part of a broader effort to improve public safety and emergency management across Ecuador.
The ECU 911 project has strong ties to China, with the China National Electronics

Import and Export Corp playing a pivotal role in its development. This collaboration is similar to China's other technology-based partnerships with countries worldwide, reflecting the influence of China's BRI on global infrastructure and technology.

The initial implementation of ECU 911 involved integrating emergency services under a unified platform, facilitating coordinated responses to emergencies. The system includes extensive video surveillance and a centralised command centre where emergency services such as police, fire, and medical units can coordinate their activities.

The extensive data collection and surveillance capabilities of the ECU 911 system have raised questions about protecting personal information and the potential for misuse of surveillance data. Ecuador's reliance on Chinese technology concerns data security and geopolitical implications. Given China's reputation for using technology to exert influence, some fear that the ECU 911 system could be used for unauthorised surveillance or political control. Despite the above, recent evidence considers it essential to incorporate the agency of Latin American States when incorporating and adapting Chinese technologies since this can help better understand the design, implementation, and evaluation of surveillance technologies.

2.2.2. The case of Colombia

Introducing Chinese surveillance technology in Colombia has mirrored adopting similar systems in other countries through the BRI. Like Ecuador, Colombia has embraced various surveillance technologies, incorporating biometric data and mass surveillance systems into its broader law enforcement strategy. The goal is to combat crime and increase public safety. Still, the extent to which these systems collect and use personal data raises critical questions about privacy rights and data protection.

These surveillance technologies can be deployed in traffic cameras, facial recognition systems, and integration with emergency response networks, such as in the ECU 911 Project. However, Colombia's reliance on Chinese technology and the close relationship between Chinese companies and the Chinese government creates concerns about unauthorised surveillance and the potential for political influence. China's control over the companies that provide these surveillance tools allows it to influence Colombia's use of technology.

A key challenge for this country is implementing a robust legal framework that ensures these technologies are not abused. Strong data protection policies, transparency, and accountability are essential to maintain public trust and safeguard individual rights. These technologies should be subject to strict oversight to prevent misuse and unauthorised access to personal information.

As Colombia continues to expand its surveillance infrastructure, it must navigate these challenges carefully to balance public safety with individual rights. The risks of over-reliance on Chinese surveillance technology and the lack of oversight mechanisms are significant concerns that require thoughtful policy and regulatory solutions to protect personal freedoms and data security.

3. DEMOCRATIC GOVERNANCE IMPLICATIONS

Chinese surveillance technology raises significant concerns in different aspects of democratic governance in the four cases analysed. **The most critical implications**

revolve around the lack of transparency, China's technological corporation's accountability, the potential misuse for political purposes, government accountability, external political influence and control, and undermining of political integrity.

In the case of Serbia, the lack of transparency in the implementation of the extensive social surveillance system and its objectives, the confidentiality of contracts between the government and Huawei, the absence of regulation and legal framework regarding social surveillance, and the difficulty in monitoring Huawei's activities within and beyond the country's borders present a significant risk to civil liberties and democratic governance. These circumstances have the potential to impact democratic governance negatively, with the possibility of government critics and political opponents being monitored, intimidated, and suppressed, individuals' privacy and freedom being violated, and human rights abuses occurring. Furthermore, there is a risk of the loss of sovereignty and an increase in China's influence due to Serbian data being stored on servers outside Serbia.

In the case of Sardinia and the city of Cagliari, there is greater regulation and legal framework regarding the use of massive social surveillance technologies through European Union (EU) legislation and more transparency regarding the objectives of the collaboration between public institutions and Huawei. However, it is essential to note that the regional government and the municipality of Cagliari continue to use Huawei technologies despite new surveillance technologies regulations and warnings from the EU about the risks of working with some Chinese technological companies. This case of technological surveillance entails problems of democratic governance related to the increasing influence of China, violation of citizens' privacy, and loss of institutional sovereignty due to technological dependency, the export, storage, and exploitation of data, and the lack of accountability regarding these activities.

In Latin America, the ECU 911 Project in Ecuador aims to centralise emergency response systems by incorporating surveillance technology to enhance public safety. However, the project's extensive surveillance and data collection capabilities raise concerns about democratic governance. Ecuador's reliance on Chinese technology presents risks related to the potential misuse of surveillance data and unauthorised monitoring.

On the other hand, Colombia's adoption of Chinese surveillance technology, like Ecuador's, aligns with China's broader strategy to expand its technology footprint through the BRI. In Colombia, surveillance technology, including biometric and mass surveillance, aims to bolster law enforcement and improve public safety. However, the extent to which these technologies collect and use personal data calls into question individual privacy and democratic governance.

In all four cases, the implications for democratic governance are profound. Surveillance technology can lead to centralised control, reducing the space for democratic participation and oversight. Concerns about data security and political influence challenge the integrity of democratic institutions and threaten individual freedoms. **To address these challenges, countries need robust legal frameworks that ensure transparency, accountability, and the protection of individual rights. Policies should be in place to regulate the use of surveillance technology, ensuring that it is used for its intended purpose (enhancing public safety) without infringing on democratic principles.** Strict oversight mechanisms are

essential to maintain public trust and protect against potential government or external economic and political power abuse.

4. RECOMMENDATIONS

To address the democratic governance concerns arising from using surveillance technology around the discussed cases, particularly those of Chinese origin, we propose recommendations for policymakers, civil society organisations, government officials, and researchers.

For Government Officials

- **Implement robust oversight mechanisms:** Create independent bodies responsible for overseeing surveillance technology use. These bodies should be able to audit and investigate potential abuses and ensure transparency in surveillance systems' operations.
- **Improve transparency and accountability of Chinese technological companies' activities:** The warnings issued by EU and USA institutions, on the one hand, regarding the espionage and security risks posed by the use of technologies from big tech Chinese corporations and, on the other hand, regarding their strong ties to the Chinese government and the Communist Party of China (CCP), necessitate increased oversight and accountability to try to minimise the risks of projects carried out by Chinese technology corporations about democratic governance and citizens' freedom.
- **Compliance with the legislation:** Government officials should work closely with legal experts to ensure proper understanding and application of surveillance technology legislation that complies with domestic and international human rights and privacy laws.

For Policymakers and Civil Society Organizations

- **Ensure the ethical use of AI and biometric data:** Implement ethical guidelines for using AI and biometric data in surveillance technology. These guidelines should address concerns about discrimination, profiling, and unauthorised surveillance.
- **Create social platforms to report social surveillance technologies:** Creating platforms and collectives in civil society to denounce, sabotage, and reverse the infrastructure of massive social surveillance technologies is a counter-power to the governments that implement and use them. In this area, some actions and movements of counter-power stand out, such as digital activism, data activism, ethical hacking, or whistleblowing.
- **Promote specific legislation in the field of AI and social surveillance:** The rapid advancement of AI, its application in the field of massive social surveillance, and the disruptive risks this poses to citizens necessitate the development of specific legislation in this area and ongoing updates to adapt to the exponential evolution of this field. A clear example to follow is the AI Act developed by the EU over the past years.

For Researchers

- **Explore local adaptations and actors' agency:** Scholars should focus on the agency of developing states in adapting Chinese-origin surveillance technology for specific purposes. This approach involves examining how local actors tailor technology to their unique contexts and how these adaptations reflect indigenous concepts of security and governance.
- **Develop more qualitative studies on the integration of surveillance systems:** Given the success of China's Tech Surveillance Applications in Europe and Latin America, scholars should study the empirical evidence of how these technologies are designed, implemented, and used in practice. This approach can

include focus groups, interviews with government officials and stakeholders, and analysis of how these systems contribute to public safety and emergency response without compromising democratic values.

- **Analyse connections between Chinese technological corporations and CCP:** To analyse the connections and interests of the CCP with major Chinese technology corporations, delve into phenomena such as digital expansionism and digital authoritarianism, and examine their potential impacts on democratic governance and how they can be mitigated.

5. CONCLUSIONS

Integrating China's AI and machine learning surveillance technologies into Europe and Latin America's societies has enhanced public safety in some respects, however it has raised serious worries regarding democratic governance. The four case studies in this policy brief illustrate the complex relationship between technology, public safety, and individual rights.

On the one hand, in Serbia and Sardinia (Italy), the extensive use of surveillance technology has improved public safety to some extent but at the expense of transparency and citizen privacy. The close ties between the technology providers and the Chinese government underscore the risks of external political influence and the erosion of sovereignty. These cases highlight the need for robust oversight mechanisms and greater accountability to protect democratic values.

Secondly, in Latin America, the ECU 911 project in Ecuador and similar recent initiatives in Colombia illustrate the rapid adoption of Chinese surveillance technologies, driven partly by China's BRI. While these systems aim to enhance emergency response and public safety, the potential misuse of surveillance data and the influence of Chinese corporations remain significant risks.

To preserve democratic governance, governments, policymakers, civil society, and researchers must work collaboratively to establish robust legal frameworks, ethical guidelines, and strict oversight mechanisms. These measures should balance public safety and individual rights, ensuring surveillance technologies are used responsibly and transparently worldwide in the current context of technological acceleration.

COMPLEMENTARY BIBLIOGRAPHY

Ellis, Robert Evan. "China's Digital Advance in Latin America." *Revista Seguridad y Poder Terrestre*, vol. 1, n.º 1, June 2022, pp. 15–39. https://doi.org/10.56221/spt.v1i1.5.

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

Ragazzi, Francesco, et al. *Biometric & Behavioural Mass Surveillance in EU Member States*. The Greens/EFA in the European Parliament, 2021. https://extranet.greens-efa.eu/public/media/file/1/7297.

Saura García, Carlos. "Digital Expansionism and Big Tech Companies: Consequences in Democracies of the European Union." *Humanities and Social Sciences Communications*, vol. 11, n.º 448, 2024, pp. 1-8. https://doi.org/10.1057/s41599-024-02924-7.

The Florence School of Transnational Governance (STG) delivers teaching and high-level training in the methods, knowledge, skills and practice of governance beyond the State. Based within the European University Institute (EUI) in Florence, the School brings the worlds of academia and policy-making together in an effort to navigate a context, both inside and outside Europe, where policy-making increasingly transcends national borders.

The School offers Executive Training Seminars for experienced professionals and a Policy Leaders Fellowship for early- and mid-career innovators. The School also hosts expert Policy Dialogues and distinguished lectures from transnational leaders (to include the STG's Leaders Beyond the State series which recorded the experiences of former European Institution presidents, and the Giorgio La Pira Lecture series which focuses on building bridges between Africa and Europe). In September 2020, the School launched its Master-of-Arts in Transnational Governance (MTnG), which will educate and train a new breed of policy leader able to navigate the unprecedented issues our world will face during the next decade and beyond.

The STG Policy Papers Collection aims to further the EUI School of Transnational Governance's goal in creating a bridge between academia and policy and provide actionable knowledge for policy-making. The collection includes Policy Points (providing information at-a-glance), Policy Briefs (concise summaries of issues and recommended policy options), and Policy Analyses (in-depth analysis of particular issues). The contributions provide topical and policy-oriented perspectives on a diverse range of issues relevant to transnational governance. They are authored by STG staff and guest authors invited to contribute on particular topics.

Florence School of Transnational Governance
European University Institute
Via Camillo Cavour 65, Firenze, FI 50129
Email: stg.publications@eui.eu

www.eui.eu/stg

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

DOI: 10.2870/097533
ISBN: 978-92-9466-513-3
ISSN: 2600-271X
QM-BA-24-017-EN-N