

Warning signals:

Venezuela and the risk of Chinese AI-enabled digital authoritarianism

REPORT

Fergus Ryan, Bethany Allen, Nathan Attrill, Mariví Marín, Alex Colville, Shannon van Sant



About the authors

Fergus Ryan is Senior Analyst with ASPI's Cyber, Technology and Security Program.

Bethany Allen is Head of China Investigations and Analysis with ASPI's Cyber, Technology and Security Program.

Nathan Attrill is a China Analyst with ASPI's Cyber, Technology and Security Program.

Marivi Marín is an external contributor.

Alex Colville is a China Analyst with ASPI's Cyber, Technology and Security Program.

Shannon van Sant is an external contributor.

AI contributed no ideas to this report.

Acknowledgements

The authors would like to thank ASPI colleagues who worked on and reviewed this project, including James Corera, Bart Hogeveen, Gatra Priyandita and Justin Bassi. We would also like to thank our external reviewers Jared Alpert and especially Parsifal D'Sola Alvarado, who generously shared his expertise.

Funding for this report was provided by the Human Rights Foundation.

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

About Reports

Reports deliver original and deeply researched analysis and judgements on issues of strategic significance and ongoing importance. Reports aim to inform and influence national strategic choices with original, deeply researched analysis that surfaces implications, tests assumptions, and may consider future courses of action.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services.

© The Australian Strategic Policy Institute Limited 2026

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers. Notwithstanding the above, educational institutions (including schools, independent colleges, universities and TAFEs) are granted permission to make copies of copyrighted works strictly for educational purposes without explicit permission from ASPI and free of charge.

First published September 2026

Published in Australia by the Australian Strategic Policy Institute

ISSN: 3083-2853 (Online), 3083-2861 (Print)

ASPI

Level 2

40 Macquarie Street

Barton ACT 2600

Australia

Tel Canberra + 61 2 6270 5100

Email enquiries@aspi.org.au

www.aspi.org.au

www.aspistrategist.org.au



[Facebook.com/ASPI.org](https://www.facebook.com/ASPI.org)



[@ASPI_org](https://twitter.com/ASPI_org)

Cover image: Venezuela Vice President Delcy Rodríguez (left), President Nicolas Maduro (center) and Chinese Ambassador Lan Hu (right) appear together at the July 2025 China–Venezuela Expo in Caracas, at which Venezuela and China signed a series of technology and cooperation agreements, including the iFlytek AI agreement. Photo credit: Prensa Presidencial de Venezuela, [online](#).

Contents

Executive summary and key findings	2
Key findings	2
Recommendations	3
Introduction: Venezuela’s surveillance state and the Chinese Communist Party	4
Venezuela’s political system	4
The Venezuela–China relationship: authoritarian solidarity	5
Chapter 1: Chinese technology in Venezuela’s digital-surveillance infrastructure	6
1.1 What Venezuela has built	6
1.2 Three operationally important systems	8
1.3 Capabilities and limitations	10
1.4 How AI could augment existing systems	11
1.5 Emerging risk	13
Chapter 2: China’s AI-enabled surveillance as an export product	14
2.1 The Chinese Communist Party’s model of surveillance-based governance	14
2.2 China’s AI-powered surveillance and control systems	14
2.3 Case study: iFlytek	14
Chapter 3: Post-2023 AI signals and emerging risks	16
3.1 The diplomatic track: from infrastructure to AI	16
3.2 The national chamber: AI direction at scale	19
3.3 The data stack	20
3.4 Civil-rights risks: what the architecture enables	21
3.5 AI-powered surveillance: a warning, not a forecast	21
Conclusion: political uncertainty and a narrow opportunity in Venezuela	22
Notes	23
Acronyms and abbreviations	28

Executive summary and key findings

This report shows that Venezuela is in a position to quickly acquire Chinese artificial intelligence (AI)-enabled surveillance tools. Venezuela has signed an agreement to acquire them, and government officials have stated their intention to integrate them into Venezuela's current surveillance regime.

The Chinese Government is the globally recognised leader in deploying new AI systems, including large language models (LLMs), to deepen surveillance and repression within its own borders. Under President Nicolás Maduro's autocratic leadership, Venezuela emerged as one of the most advanced adopters of Chinese-made surveillance technology in the Western Hemisphere, embedding digital monitoring tools deep into the daily governance of the state.

Now Venezuela is primed to upgrade its surveillance technology. This report shows that, in the months before Maduro's capture by US forces in January 2026, the Venezuelan Government signed an agreement to adopt Chinese-built AI systems in an initiative led by Maduro's Vice President, Delcy Rodríguez, and signalled its intent to use Chinese AI to enhance existing state-sponsored surveillance.

The US has installed Rodríguez, who once supervised Venezuela's repressive intelligence agency, as the country's acting president. Under her leadership, the Venezuelan Government has neither liberalised nor dismantled the surveillance regime.

If Caracas continues to implement its plan to use Chinese AI for surveillance—and it has given no signal that it won't—Venezuela will become one of the first countries outside China to import China's new generation of LLM-based AI systems for surveillance and control, and the most advanced adopter in the Western Hemisphere.

This report finds that the state's laws and institutions have already been shaped to accommodate that ambition, and that leading Venezuelan politicians have stated it openly—both to enhance its domestic surveillance system and to counter weapons of Western 'cognitive warfare'. The report also carefully maps out how Chinese AI could enhance and more tightly integrate existing surveillance systems.

These findings serve as a call to action at a key turning point in Venezuela's trajectory. It's not too late to prevent the further entrenchment of technology-enabled surveillance there.

Key findings

1. Venezuela has signed an agreement to acquire Chinese AI technology to layer on top of its existing governance structures.

In July 2025, the Venezuelan Government signed a memorandum of understanding (MoU) with iFlytek, which is a Chinese firm on the US Entity List since 2019 and a supplier of LLM systems to China's own censorship and judicial-automation apparatus. It's Venezuela's

first known agreement for Chinese AI capability rather than Chinese hardware, and it was negotiated by Delcy Rodríguez, then Vice President and now the US-appointed acting president. After two decades of importing cameras, networks, identity systems and command centres, Caracas has contracted for the intelligence intended to run on top of them.

2. Venezuela's leaders have openly stated their explicit intent to use Chinese AI for surveillance and control.

A key step towards this effort was the establishment of a national command room in January 2025, intended to manage a confederated system of local data rooms, running on Chinese-made control systems built over the past decade, that collect information on citizen complaints, welfare distribution and grassroots political activity.

3. Venezuela is poised to go from just buying digital infrastructure, including for national-security purposes, to potentially importing the intelligence meant to run on top of it.

This is enabled by the gradual import of Chinese hardware, software and platform solutions that now constitute an integrated technology stack—the perfect landing place for next-generation AI-enabled surveillance and repression.

4. Acting president Delcy Rodríguez was instrumental in overseeing Venezuela's political surveillance apparatus. She supervised the domestic intelligence agency (SEBIN) and the expansion of the commune system, which became a key part of Venezuela's infrastructure of political surveillance and control.

Without outside pressure, specifically from the US, Rodríguez can't be expected to take any autonomous steps towards dismantling Venezuela's surveillance systems.

5. The AI layer is signalled but not yet built—indicating a narrow but crucial window of time to prevent further entrenchment of Venezuela's surveillance apparatus.

No public evidence shows Chinese AI systems operating inside Venezuela's surveillance apparatus today. But if the iFlytek agreement is implemented on top of the infrastructure that this report documents, AI would make Venezuela's repression cheaper, faster and harder to see—automating censorship, linking databases into individual risk profiles, and turning today's fragmented systems into an integrated instrument of political control. That escalation is preventable now. It will be far harder to reverse once built.

The current US control over Venezuela's government provides an opportunity to dismantle China's potential grip on Venezuela's digital infrastructure and surveillance systems.

Global implications

6. The policy toolkit built for equipment hasn't yet been adapted for AI.

Import controls, procurement rules and audit regimes were designed for things that can be counted, inspected and physically removed. But the component that determines political effect—an AI model's trained disposition about what's sensitive, threatening or refusible—is intangible and unauditable by the importer. Democratic governments presently have no settled method for assessing the political disposition of foreign-supplied models, and no disclosure standard tied to government procurement.

7. Venezuela is a test of whether democracies can act before such a system exists.

Responses to exported digital authoritarianism are typically remedial: sanctions after deployment, documentation after abuse, condemnation after entrenchment. But Venezuela presents an opportunity to act sooner—a signalled but unbuilt capability, in a state currently dependent on Washington, with a supplier identified. Whether that window is used will establish whether prevention can be a real instrument of policy. Governments now weighing the same purchase will read the answer as precedent, and so will vendors.

A note on confidence

This report has been compiled through open-source research, including government documents, company filings and media and research reports in English, Chinese and Spanish. Venezuela is largely closed to independent researchers, and there's little public documentation of how these systems are used in practice.

This report therefore grades every claim by the strength of the evidence behind it, so it's clear how much weight each one carries. This report distinguishes between:

- 1) confirmed deployment—systems documented in operation
- 2) signed agreements—such as the iFlytek MoU, which commit parties on paper without establishing that anything has been built
- 3) stated intent—official announcements and doctrine
- 4) plausible pathways—capabilities that existing infrastructure could support but that aren't documented
- 5) inferred risk—projections based on how similar systems have been used elsewhere.

Claims are framed accordingly throughout. Where a figure rests on official Venezuelan sources, it's flagged as such.

Recommendations

Recommendation 1: Support Venezuelan civil society.

This is a crucial moment for the international community to give maximum support to Venezuelan civil society, the democratic political opposition, journalists and digital-rights defenders. Not only are they primary targets of surveillance; they're also the change agents who could initiate a course correction. Timely support can help them to reassert their right to operate freely in Venezuela and to advocate for political reform from within.

Private foundations, multilateral human-rights bodies, and donor governments can:

- scale up grants that support threatened organisations and individuals in Venezuela, especially by providing digital-security support, physical security training, legal aid and emergency response; and to independent Venezuelan media and diaspora media outlets that need funding for mirror sites, legal defence, secure hosting and cross-border publishing
- fast-track humanitarian visas and other protection pathways for persecuted political opposition members, organisers, journalists and others targeted by the Venezuelan Government
- commission reports and organise public hearings focused on digital surveillance, repression during election seasons and attacks on journalists, through bodies such as the Special Follow-up Mechanism for Venezuela at the Inter-American Commission on Human Rights.

Recommendation 2: Make AI tools for countering authoritarianism freely available to Venezuelan civil society.

Tech companies can initiate free AI education and training programs for civil society and private-sector stakeholders in Venezuela, to show them how AI tools can be used to circumvent censorship and hide their activities from repressive government agencies.

Recommendation 3: The US should require Rodríguez to immediately cancel the memorandum of understanding with Chinese AI giant iFlytek.

The window of opportunity to prevent the entrenchment of deeper surveillance is now: Venezuela must formally cancel this agreement before iFlytek's AI-enabled platforms are fully integrated into Venezuela's surveillance systems.

Recommendation 4: Urge the US Secretary of State to pressure Rodríguez to end the current surveillance regime.

The current moment represents a narrow and contestable window for democratic allies and partners, multilateral organisations and civil-society groups to pressure the Venezuelan Government to dismantle its systems of surveillance and repression. The *New York Times* reported in July that Secretary of State Marco Rubio effectively runs the Venezuelan government and economy and communicates constantly with Rodríguez over WhatsApp.¹ Thus, the US remains the best lever of influence to pressure Venezuela's current leaders.

Secretary Rubio can push the current Venezuelan Government to:

- end the ‘Homeland Card’ (*Carnet de la patria*) system and delete its database of Venezuelan citizens; replace it with a more standard national ID system that doesn’t collect as much intrusive personal and political information
- require CANTV and all licensed telecommunications operators to comply with a defined, independently audited human-rights protocol for interception and metadata requests
- publish the full text of existing AI and surveillance agreements.

A stronger approach, although more difficult to achieve, would be for democratic governments to together create a coalition *démarche*, co-signed and accompanied by the preceding demands and a stated schedule of what compliance earns and what noncompliance costs.

Recommendation 5: Plan for liberal reform.

Even if dismantled, repressive surveillance systems could easily make a comeback unless democratic rights and institutions are restored in Venezuela. Conditions in Venezuela probably aren’t ripe for liberal political reform—yet. But civil-society organisations and like-minded governments can still prepare for a time in the future when that moment may come.

There should be detailed, transition-ready plans now so that surveillance rollback is feasible when political openings appear. This can come in the form of blueprints for a privacy law, surveillance-oversight architecture, telecom regulator independence, repeal plans for abusive measures, deletion/audit protocols for politicised databases, and rules for lawful access, transparency and remedy.

Civil society and governments can continue to call for the release of all political prisoners, dissolving the commune system and restoring the independence of the judiciary, so that any progress on rolling back surveillance can be maintained over the long term.

Recommendation 6: Sanction surveillance abuse and surveillance enablers.

- Expand targeted sanctions against Venezuelan officials directing digital repression.
- Coordinate stronger enforcement for procurement and import bans on companies providing surveillance technology or support to Venezuela.

Recommendation 7: Set security standards for foreign AI used by governments.

Standards bodies, national AI safety and security institutes and government procurement authorities should establish an assurance standard for foreign-supplied models deployed in state functions. Import controls, procurement rules and audit regimes were designed for equipment that can be counted, inspected and physically removed. The component that determines political effect—a model’s trained disposition about what’s sensitive, threatening or refusable—is intangible and unauditable by the importing state.

A disclosure standard should apply to models deployed in policing, justice, welfare administration and communications regulation, covering training-data provenance, refusal and filtering behaviour, update governance, and the identity of the party controlling finetuning. Independent evaluation against the standard should be a condition of procurement, and results should be published.

Introduction: Venezuela’s surveillance state and the Chinese Communist Party

Digital authoritarianism, even when augmented by imported technology, begins at home. This chapter provides a brief overview of Venezuela’s political system and traces the emergence of its surveillance ecosystem during the Maduro era. It demonstrates how surveillance technology builds on political structures, and how ultimately the path to further authoritarianism is a political decision. The chapter then explains why the Chinese Communist Party (CCP) helps other governments build high-tech surveillance states.

Finally, the chapter examines the figure now in charge. Delcy Rodríguez, Maduro’s Vice President and now the country’s acting president, was a senior official overseeing parts of Venezuela’s surveillance and repression regime, and a top interlocutor in the agreement with iFlytek. Her involvement makes it unlikely she would dismantle a surveillance state she supported. Without external pressure, the repression is likely to continue.

Venezuela’s political system

For decades, Venezuela functioned as a democratic system despite persistent institutional weaknesses. Hugo Chávez, a former army officer who had led a failed coup attempt in 1992, was elected President in 1998 on a platform promising profound political and social transformation.²

Over the following years, Chávez weakened the country’s system of checks and balances, expanded state control over the economy, ended the Central Bank’s autonomy, curtailed independent media, and intimidated political opponents.³ His government also promoted the creation of communal councils and communes as part of a broader project to build a ‘communal state’. Although implementation remained uneven, those organisations became important channels for political mobilisation, local governance and the distribution of state resources.⁴

Nicolás Maduro won the 2013 presidential election and oversaw a period of unprecedented political oppression and violence in Venezuela, reshaping it into one of the world's most authoritarian regimes.⁵ Maduro developed and expanded the mechanisms of repression that had begun under Chávez. His government increasingly relied on a combination of party organisations, community networks and social-welfare programs to strengthen political control, while linking access to some state benefits to mechanisms such as the *Carnet de la Patria*—a digital identification system introduced in 2017. The system became an important instrument for administering social programs and reinforcing political loyalty.

The role of security and intelligence agencies—including the Special Action Forces unit of the Bolivarian National Police (FAES), the Bolivarian National Intelligence Service (SEBIN) and the General Directorate of Military Counterintelligence (DGCIM), among others—in suppressing dissent also grew during this time. United Nations investigations have documented widespread arbitrary detention, torture and extrajudicial executions committed by several of those bodies.⁶

The International Criminal Court began an investigation into crimes against humanity in Venezuela in 2021—its first in the Americas—documenting political persecution, severe deprivation of physical liberty, and torture committed by Venezuelan authorities.⁷

In 2024, Venezuela became a virtual pariah state after Maduro claimed victory after the opposition won the presidential election.⁸ Subsequent protests spurred a crackdown, resulting in at least 25 deaths and the arbitrary detention of about 2,000 people.⁹

One-third of Venezuelans are now experiencing food insecurity, and economic hardship has forced the exodus of nearly 25% of the population, or 7.7 million people.¹⁰

The Venezuela–China relationship: authoritarian solidarity

Venezuela has obtained political, economic and technological support from numerous countries, but the especially close relationship between China and Venezuela under Chávez, and for part of Maduro's tenure, helped pave the way for Venezuela's adoption of Chinese surveillance technology, and thus the deepening of its repression and the construction of its surveillance state.

Venezuela's repressive apparatus rests on numerous domestic structures: Venezuela's premier state security agency SEBIN, the DGCIM, military intelligence, the Bolivarian National Police, the Bolivarian National Guard, *colectivos*, the attorney general's office, judicial persecution, censorship and media control. But Chinese companies helped enable the system by building some of the tools within this complex state-driven apparatus of surveillance and coercion.

For Venezuela, Chinese finance, technology and political support probably lowered the costs of authoritarian consolidation. For

Beijing, this wasn't just a commercial investment for Chinese tech champions. To China's leaders, the more countries that adopt China's techno-authoritarianism, the more legitimate the CCP's governance model becomes.¹¹

Chávez began courting Beijing soon after taking office in 1999, seeking a counterweight to the US, which was a top purchaser of Venezuelan oil and long a major influence on the region. The relationship blossomed, and the two countries forged hundreds of agreements under Chávez's rule. The two sides launched the China–Venezuela High Level Joint Commission to steer the countries' political and economic relationship, the China–Venezuela Joint Fund, which swapped China-backed loans for Venezuela's oil, and other deals across mining, infrastructure and technology transfer.¹²

Chávez admired various aspects of China's development trajectory and sought technological cooperation in multiple sectors, including telecommunications, satellites, the national ID system and infrastructure. In 2008, Chávez sent Justice Ministry officials to Shenzhen to study China's national identity card program.¹³

Maduro continued to seek out Chinese expertise and technology as he built and modernised his surveillance state. He announced the '*carnet de la patria*' or 'Homeland Card' system in December 2016, with rollout beginning in early 2017, based in part on China's national identity card program.¹⁴ Chinese telecom company ZTE helped to build the Homeland Card system, which includes a mobile payment system and national ID card technology.¹⁵

Millions of Venezuelans now use the Homeland Card system to access social benefits. Human-rights activists have described the system as a mechanism of social control, through which the Venezuelan state distributes economic benefits while simultaneously strengthening political dependence on government-controlled structures.¹⁶

Other Chinese companies, including Huawei and CEIEC, built telecommunications infrastructure and other systems used to monitor and censor online political activity and to record citizens' political affiliations, social-media presence and electoral participation.

Bilateral ties weakened substantially between 2013 and 2018 due in part to economic collapse in Venezuela, and to Venezuela's failure to complete some major China-funded projects amid widespread corruption, leaving Chinese creditors in the lurch.¹⁷

But the relationship underwent a diplomatic and economic renewal after 2019, when Maduro illegally claimed the presidency in a disputed election and the US and other nations imposed sweeping sanctions on a wide swathe of Venezuelan industries, including its oil industry.¹⁸ Maduro turned to China. Beijing gave Caracas cover on the international stage, blocking UN Security Council resolutions condemning Maduro and opposing international sanctions.¹⁹

In 2023 Beijing and Venezuela jointly declared that they had formed an 'all-weather strategic partnership'—a term reserved for China's closest partners, such as Pakistan and Belarus.²⁰ After 2019 and until the January 2026 US intervention, China purchased most of Venezuela's exported oil; traders used shadow-fleet tankers,

ship-to-ship transfers and false documentation to conceal much of the trade.²¹ Venezuela, in turn, was the largest purchaser of military equipment from China in Latin America.²² In 2025, China was Venezuela's second-largest trading partner.²³ Hours before the military strikes began and his own capture, Maduro was meeting with Qiu Xiaoyi, China's Special Envoy for Latin American Affairs, to discuss rising tensions with the US.²⁴

Delcy Rodríguez and authoritarian continuity

After seizing Maduro, the Trump administration assessed that Maduro loyalists were better positioned than the democratic opposition to lead the government and maintain stability.²⁵ The US chose Maduro's vice president Delcy Rodríguez to serve as the country's acting president, in part because of her role overseeing the country's oil and energy industries.

Rodríguez is no liberal reformist. Under Maduro, she helped oversee Venezuela's political surveillance. From 2018 until she became acting president in January 2026, Rodríguez served as Executive Vice President, which is an influential position within Venezuela's state structure. In that role, she became the highest civilian authority with formal oversight over the SEBIN, the country's principal civilian intelligence agency and a central pillar of Venezuela's repressive apparatus.²⁶

As Executive Vice President, Rodríguez was also directly involved with the Homeland Card system. The Fundación Patria, or 'Homeland Foundation', manages the Homeland Card system, and is formally attached to the office of the Executive Vice President.²⁷ And she also oversaw an expansion of the commune system—the

territorial structures that independent monitors have documented conducting street-level surveillance of government critics, and that now staff the national command-room network activated under her authority in February 2025 (see Chapter 3).²⁸

Since Rodríguez became acting president, there's strong indication that Venezuela's regime of surveillance and repression remains alive and well. In March 2026, UN investigators said they had documented dozens of politically motivated detentions since Maduro's removal.²⁹ A March 2026 report by the Atlantic Council's Digital Forensic Research Lab found that Venezuela's surveillance infrastructure remained 'fully operational' after Maduro's removal.³⁰ The report's authors concluded that 'technological capabilities and institutional frameworks for authoritarian control transcend individual leadership and require deliberate dismantling rather than mere regime leadership change.' In April 2026, the Venezuelan human rights group Foro Penal said hundreds of political prisoners had been released since January, but that 473 remained behind bars.³¹

Rodríguez has also played a leading role in managing the Venezuela–China relationship. In 2023, she was appointed Venezuelan chair of the China–Venezuela High-Level Joint Commission, the main mechanism through which both governments coordinate strategic bilateral cooperation.³² She led the high-level dialogues that deepened the relationship after the 2023 'all-weather strategic partnership' upgrade. She personally negotiated and signed an agreement with Chinese tech giant iFlytek in July 2025 in which the Venezuelan Government agreed to incorporate iFlytek's AI systems and to jointly pursue the development of sovereign AI.

Chapter 1: Chinese technology in Venezuela's digital-surveillance infrastructure

Venezuela's digital-surveillance infrastructure wasn't designed as a single, integrated system. It emerged incrementally through separate investments in telecommunications, digital identity, public-security monitoring and internet control, supported by Chinese firms and other foreign partners, particularly Cuba in the security and intelligence sphere. Many countries have invested in Venezuela's digital infrastructure, but Chinese technology has been especially consequential because it has strengthened institutions already used for political control.

The resulting architecture is fragmented, unevenly deployed and technically constrained. Nevertheless, its components can reinforce one another: identity systems can connect citizens to state services, command centres can support public-order operations, telecommunications networks provide information choke-points, and internet controls can restrict politically sensitive communications. The risk is therefore not that Venezuela has reproduced China's surveillance state, but that Chinese

technology—and increasingly AI—could make the existing Venezuelan system of coercion more effective.

This chapter provides a selective, evidence-based account of the principal Chinese-supported technological systems identified in open sources; it isn't an exhaustive inventory of every Chinese company or technology operating in Venezuela.

1.1 What Venezuela has built

Venezuela's digital-surveillance architecture isn't a single platform, but a layered technological ecosystem spanning six interconnected areas: telecommunications infrastructure; digital identity and registration systems; central databases and data-integration platforms; surveillance and monitoring networks; emerging analytics and AI capabilities; and internet control and content-management systems.³³

Those technological layers operate within a much broader apparatus of political control. Venezuela also relies on intelligence and counterintelligence agencies, military and police institutions, party and community networks, informant systems and administrative coercion. Many of those structures pre-date the Chinese technology examined in this chapter and have been shaped by domestic *Chavista* institutional development and longstanding Cuban security assistance.³⁴ They fall outside the chapter's principal technological focus but are essential to understanding how digital systems are used and converted into political action.

Several of the digital-control systems examined in this chapter were introduced or expanded between 2013 and 2020 under President Nicolás Maduro, although some of the underlying telecommunications infrastructure and foreign technology relationships pre-dated that period.³⁵ They were publicly framed as tools for welfare delivery, crime prevention, emergency response and digital modernisation. In practice, they also expanded the state's capacity to identify citizens, monitor public space, manage access to services and restrict the online information environment.³⁶

Chinese firms became embedded across several layers of this architecture before AI became a prominent part of Venezuela's public technology agenda. CEIEC was involved in the expansion of VEN911, associated command centres and CCTV networks—Venezuela's national emergency-response and command-and-control system, which allows the state to monitor incidents and coordinate security responses in real time—as well as CCTV networks and command centres associated with CEIEC. ZTE has reportedly had a role in building systems connected to

the biometric identity database underpinning the Homeland Card.³⁷ Huawei, Hikvision, Dahua and other Chinese firms have also contributed to the telecommunications, connectivity and visual-surveillance layers of the wider ecosystem (Table 1).

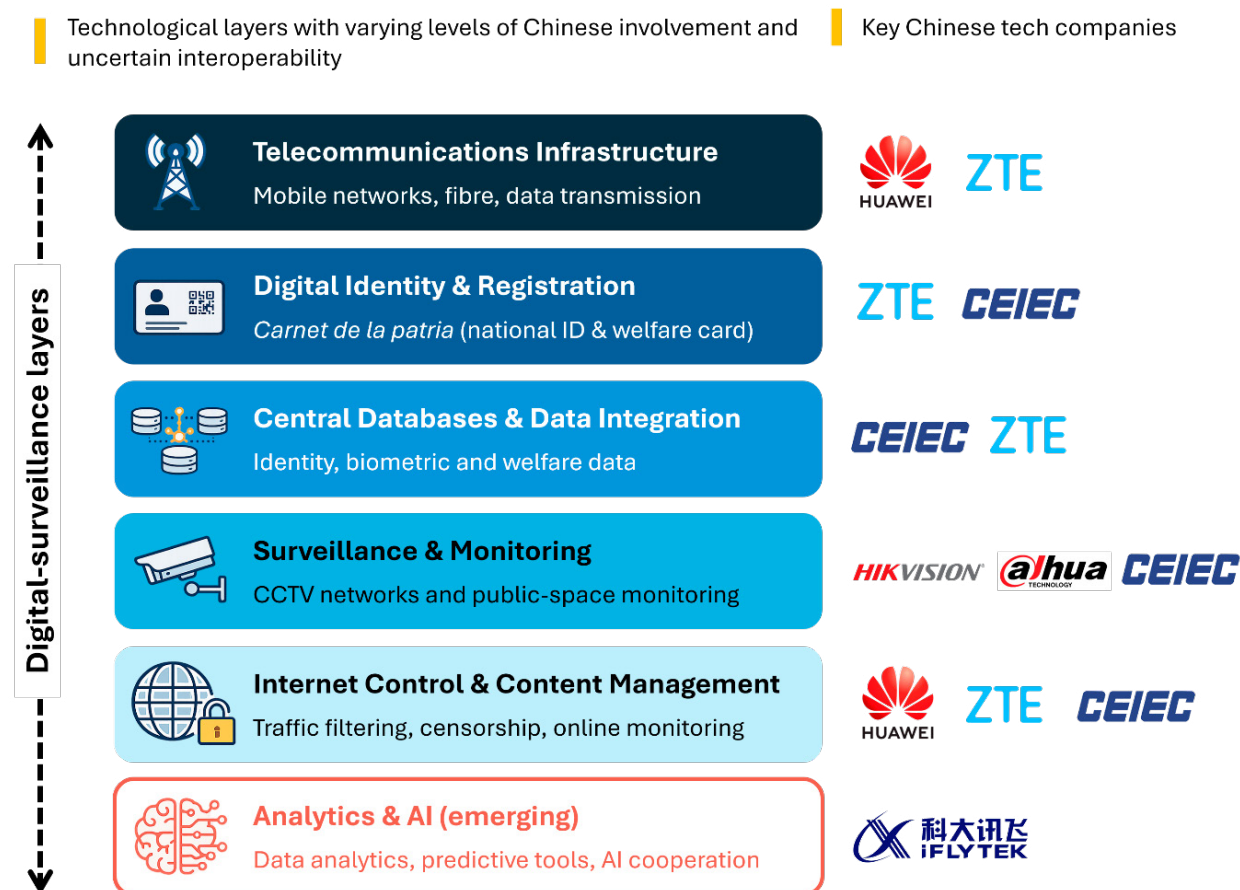
Taken together, these systems show that Venezuela's technological relationship with China is not only about infrastructure. Individual projects—cameras, command centres, telecommunications systems and digital-governance platforms—were often presented as discrete modernisation initiatives. Collectively, however, they have created a layered technological ecosystem that we judge capable of collecting, organising and potentially analysing substantial volumes of citizen data, even though its components remain unevenly deployed and only partially interoperable.

For analytical purposes, this report groups Venezuela's digital-surveillance capabilities into six functional layers. The framework is constructed for this report, drawing on established analyses of digital-authoritarian and smart-city systems, but adapted to the technologies documented in Venezuela. These categories resemble components found in China's digital-governance architecture, but they're used here as a functional taxonomy rather than evidence that Venezuela copied a Chinese blueprint. Venezuela demonstrates how components associated with this system can be accumulated selectively and incorporated into an existing political system. It isn't a full replica of China's domestic model and doesn't appear to operate as a single integrated platform. It has assembled enough layers to make the system politically useful, even though it remains technically incomplete. Figure 1 shows the contribution of Chinese technology across Venezuela's digital survey system.

Table 1: Key Chinese technology companies in Venezuela's digital-surveillance ecosystem

Company	Role in Venezuela	Confidence level	Relevance to surveillance system
	Homeland Card infrastructure ³⁸	High	Identity, databases, welfare-linked social control
	SIMA/VEN911, command centres, internet-control support ³⁹	High	Systems integration, command-and-control, censorship
	CCTV hardware observed in Caracas ⁴⁰	Medium	Visual surveillance layer
	CCTV hardware observed in Caracas ⁴¹	Medium	Visual surveillance layer
	Telecoms/connectivity backbone ⁴²	Medium	Network infrastructure enabling data transmission

Figure 1: Chinese technology contributions across Venezuela's digital-surveillance layers



Graphic: ASPI.

The key point is interoperability rather than perfect integration. Public evidence doesn't show that Venezuela has built a single unified surveillance platform linking every database, camera network and internet-control mechanism, but those systems don't need to be fully integrated to expand state capacity or acquire political utility. The Homeland Card links identity and welfare records, including, in some reported cases, politically sensitive information; safe-city networks enable monitoring of selected public spaces; telecommunications infrastructure supports data transmission and provides potential network choke-points; and internet-control mechanisms allow the state to restrict digital communications during politically sensitive periods.

The comparison with China is therefore important but has limitations. China's digital governance system is more institutionalised, more deeply integrated and supported by a strong domestic technology sector.⁴³ Venezuela's model is narrower, more *ad hoc* and more dependent on external providers, especially Chinese firms. Its primary uses are narrower: subsidy distribution, welfare administration, public-order management, information control and the reinforcement of political dependence. The result is a fragmented Venezuelan digital-control system that incorporates several technological components also found in China's digital-governance architecture, but applies them through different institutions, under different constraints and for Venezuelan political purposes.

1.2 Three operationally important systems

Venezuela's surveillance architecture rests on three core systems:

- the Homeland Card—the national digital identity system
- safe-city monitoring and communication systems—a collection of CCTV and command-and-control systems used for public safety and security operations
- the infrastructure related to internet control and censorship.

Each system performs a different function, but together they give the state the ability to identify citizens, monitor public space, restrict digital information flows and link access to services with political control.

System 1: The Homeland Card

The Homeland Card (*carnet de la patria*) is the identity layer of Venezuela's surveillance ecosystem. Introduced in 2016 during Venezuela's deepening economic crisis, it was officially presented as a welfare and service-delivery platform.⁴⁴ In practice, it evolved into a centralised digital identity system connecting citizens to subsidised food, fuel, health care, pensions and state cash transfers.⁴⁵ According to the official Homeland Card website (now offline), the platform had 21.8 million registered users in January

2023⁴⁶—equivalent to roughly three-quarters of Venezuela’s population⁴⁷—and served 14.2 million people each month.⁴⁸

The card contains a personalised QR code linked to a central database. Through registration and use of the card, citizens provide extensive personal information, including household composition, employment status, health conditions, state benefits received and, in some cases, political affiliation or voting behaviour. That allows government agencies to retrieve individual records and eligibility information through linked digital systems.⁴⁹

The system’s significance lies in the way it links identity, welfare and administrative data. Access to essential goods and services became increasingly tied to participation in a state-managed digital platform. That expanded the government’s capacity to profile beneficiaries, administer social programs, reinforce dependence on state institutions and support politically significant mobilisation. Reporting has also indicated that politically sensitive information, including voting-related data, could be associated with individual records. Public evidence does not, however, establish that the system continuously or systematically monitors citizens’ political loyalty.⁵⁰

ZTE played a significant role in building the systems connected to the Homeland Card and the wider *Patria* platform, including its database, QR-code system and payment app. From 2016 to at least 2018, ZTE personnel reportedly worked inside Venezuela with government agencies and the state telecommunications provider *Compañía Anónima Nacional Teléfonos de Venezuela* (CANTV) to configure databases, address performance issues and train Venezuelan personnel.⁵¹

Public evidence of ZTE’s recent operational role is limited. There’s strong reporting on its role in the system’s creation and early operation, but less public evidence showing whether ZTE continues to manage or upgrade the platform. What can be said with greater confidence is that the *Patria* platform has remained an important mechanism for administering social benefits and selected citizen–state transactions. Its current technical condition, operational reach, vendor support and upgrade pathways remain opaque.⁵² The available evidence therefore supports claims about its historical importance and administrative function more strongly than claims about its present technical capabilities.

The Homeland Card matters for future AI adoption because it provides the identity anchor for the wider surveillance ecosystem. AI tools could make it easier to search, link and analyse citizen records, identify welfare recipients, detect alleged fraud, correlate administrative records, generate risk indicators or support politically discriminatory decisions.

System 2: Safe-city projects: CCTV and command centres

Venezuela’s safe-city projects form part of the public-space monitoring layer of its digital-surveillance ecosystem. They include VEN911 and Integrated Monitoring and Assistance System (*Sistema Integrado de Monitoreo y Asistencia*, SIMA) command centres, CCTV

installations, emergency-response systems, police-dispatch tools and communications platforms deployed in selected locations.⁵³

When SIMA was announced in 2013, the government stated that the project would install 30,000 cameras in public spaces, operate nationally and connect local operational hubs to a central situation room in Caracas.⁵⁴ These figures describe the program’s stated ambition rather than its documented implementation. Available open-source evidence doesn’t show that the camera target or nationwide coverage was achieved.

Implementation appears to have been partial and geographically uneven. Broader constraints affecting the Venezuelan state—including funding shortages, corruption, equipment maintenance, electricity and connectivity problems, and limited institutional capacity—are likely to have restricted the scale and reliability of the deployment.

Where operational, these systems can collect and centralise information from cameras, emergency-response networks and public-security infrastructure. Command centres allow authorities to monitor urban spaces in real time, coordinate security responses and integrate data from multiple public-security sources.

Safe-city systems can give authorities greater visibility over protests, public gatherings and security incidents by connecting cameras, communications systems and command centres. They turn monitoring into an operational surveillance capability by allowing authorities to identify events, direct security forces and manage public order from centralised locations.⁵⁵ In Venezuela, the documented scale and operational consistency of those capabilities remain uncertain.

Chinese firms have played different roles within this layer. CEIEC was the most important systems integrator, with links to SIMA, VEN911, command-and-control architecture, public-security analytics, dispatch systems and emergency-response platforms. CEIEC is a Chinese state-owned defence-electronics and systems-integration company. Unlike camera manufacturers that principally supply sensors, CEIEC’s reported role in Venezuela included combining hardware, communications, software, command centres, dispatch functions and technical support into operational public-security systems. This makes its role potentially more consequential than the provision of individual cameras, although the precise configuration and current condition of the systems it supplied remain unclear.

The SIMA and VEN911 projects were designed to install command-and-control centres, security cameras and alarm buttons across multiple Venezuelan localities, with CEIEC as the principal provider. Where deployed and operational, this can give authorities a platform for monitoring urban spaces, assessing incidents and coordinating security responses from centralised command centres.⁵⁶ Hikvision’s and Dahua’s roles were less as architects of the overall system and more as providers of the visual-surveillance hardware that feeds data into Venezuela’s command centres.

The evidence base varies across those companies. CEIEC's role is the best documented. The public evidence for Hikvision and Dahua is more limited, resting largely on field observations, local market presence and later reporting identifying their equipment in Venezuela's surveillance ecosystem. This indicates that Hikvision and Dahua equipment forms part of the visual-surveillance layer, although the scale of their deployment and commercial role remain unclear.

This distinction matters because safe-city projects are layered by design. CEIEC appears to have provided the integration layer: platforms, command centres, dispatch tools and public-security systems. Hikvision and Dahua appear to have contributed to the sensor layer: Hikvision cameras have been identified in Caracas, and most publicly visible CCTV appears to come from Chinese vendors—particularly CEIEC, Hikvision and Dahua—making them dominant in Venezuela's CCTV supply chain.⁵⁷ Together, these firms illustrate how Chinese surveillance exports often combine systems integration, telecommunications infrastructure and hardware supply rather than relying on a single vendor.

The planned SIMA and VEN911 architectures are some of the most obvious targets for AI enhancement. Computer vision, facial or vehicle re-identification, crowd analytics, natural-language video search and automated incident reporting could make existing CCTV and command-centre systems faster, more searchable and more operationally useful.

System 3: Internet access, control and censorship

Venezuela's internet-control capabilities rest on the interaction of network concentration, regulatory authority and technical intervention. The regulatory system, network architecture and technical control related to the internet in Venezuela allow the state to impose selective restrictions on access to independent media, opposition communications, social-media platforms and politically sensitive online content.⁵⁸

As the state-controlled telecommunications company and largest internet service provider, CANTV is the central linchpin in Venezuela's internet and information control system.⁵⁹ The *Comisión Nacional de Telecomunicaciones* (CONATEL) is the regulatory authority governing the actions of providers. CEIEC is reported to have supplied technology, training and expertise that strengthened the state's ability to restrict internet access and conduct digital surveillance.⁶⁰

Internet control allows the Venezuelan state to restrict both online content and access to communications infrastructure. Measures have included website and platform blocking, throttling or disruption of connectivity during politically sensitive periods, and restrictions affecting tools used to circumvent censorship.⁶¹

CEIEC is the clearest Chinese actor linked to this layer. The US Treasury sanctioned CEIEC in 2020 for supporting the Maduro government's efforts to restrict internet service, conduct digital surveillance and carry out cyber operations.⁶² Huawei's role appears to sit mainly in the telecommunications and connectivity layer: reporting reveals that CANTV depended on agreements

with Huawei and ZTE to supply equipment and staff, making Huawei part of the network infrastructure on which Venezuela's digital-control systems depend.⁶³ Huawei's documented role in telecommunications infrastructure doesn't, by itself, demonstrate that Huawei equipment is used for censorship or political surveillance.

Internet-control systems could be strengthened by LLM-based content moderation, automated translation and triage, circumvention-tool detection, network-traffic analysis and automated takedown escalation. Those tools could make censorship more scalable, adaptive and easier to operate across large volumes of online content.

1.3 Capabilities and limitations

Venezuela's digital-surveillance systems are best understood as a collection of partially connected capabilities rather than a coherent national architecture. Their rollout has been constrained by weak infrastructure, limited maintenance, institutional fragmentation and uneven operational capacity. Those limitations reduce the government's ability to use the systems continuously or at national scale. They don't, however, eliminate their political utility: identity databases, telecommunications choke-points, selected camera networks and internet controls can still be used separately—or connected on an *ad hoc* basis—against particular individuals, locations or moments of political contention.

The system begins with identity. The Homeland Card provides a potential identity anchor connecting citizens to the state. By linking individuals to welfare benefits, fuel subsidies, healthcare services, pensions and other government programs, it creates a persistent digital record through which people can be identified, profiled and categorised. Unlike CCTV or internet monitoring, which observe behaviour in specific contexts, the Homeland Card provides a mechanism for tying information back to identifiable individuals. That makes identity the foundation on which other forms of surveillance can potentially be layered.

Safe-city infrastructure can provide operational visibility where it's deployed and functional. VEN911 and SIMA command centres, emergency-response networks and police-dispatch systems give authorities visibility over public space and can coordinate responses in real time. Those systems allow the state to observe activity, but they also help to turn observation into action. Cameras, communications systems and command centres allow authorities to identify events, direct security forces and manage public order from centralised locations.

Telecommunications infrastructure creates potential choke-points. CANTV and other network systems carry the data, communications and connectivity on which digital identity platforms, command centres and internet controls depend. That makes telecommunications infrastructure more than a neutral backbone. It gives the state choke-points through which information can be transmitted, monitored, slowed or disrupted.

Internet-control mechanisms support selective and episodic intervention. Through CANTV's position as the principal state-controlled internet provider, CONATEL's regulatory authority, targeted technical restrictions and broader pressure on media and telecommunications companies, the state can block particular websites and platforms, throttle services and disrupt politically sensitive communications. CEIEC has been publicly accused by the US Government of supplying software, training and technical expertise used for internet restriction and digital surveillance, but the specific systems involved, their present operation and their importance relative to domestically controlled regulatory and network mechanisms remain unclear.

Venezuela shouldn't be understood as operating an integrated internet-governance system comparable to China's Great Firewall. Its censorship regime is more fragmented, selective and reactive, and remains constrained by weak infrastructure and limited state capacity. Those limitations don't make it politically irrelevant: targeted restrictions can still impede opposition communication and access to independent information during elections, protests and crises.

Those layers don't need to be perfectly integrated to be politically effective. Public evidence doesn't show that Venezuela has built a single unified database linking every surveillance platform, identity system, camera network and internet-control mechanism. Nor does it show that Venezuelan authorities possess a China-style system capable of seamlessly combining all available data sources in real time. But coercive power doesn't depend on perfect technical integration. Even partial interoperability between identity systems, command centres, telecommunications networks and state agencies can expand the state's ability to monitor citizens and influence behaviour.

This is especially important for understanding the future role of AI. New AI doesn't require Venezuela to build a new surveillance architecture from scratch. It can increase the value of systems already in place by making fragmented data easier to search, summarise, correlate and act upon. Identity records, CCTV footage, network data and internet-control information don't need to sit in one perfectly integrated platform to become more politically useful. New AI tools could help officials extract patterns from partial datasets, connect people to events or organisations, generate alerts and turn existing information into operational decisions.

1.4 How AI could augment existing systems

The significance of this existing architecture is that the most plausible pathway for future AI adoption in Venezuela is cumulative rather than disruptive. The Venezuelan Government doesn't need to build a new surveillance system to benefit from advances in generative AI, computer vision or automated analytics. It can layer those capabilities onto telecommunications networks, identity databases, CCTV systems, command centres and internet-control mechanisms that already exist (see box).

Potential interoperability advantages

Existing reliance on Chinese technology could reduce some barriers to adopting additional Chinese AI capabilities. A vendor upgrading its own command-centre, video-management, telecommunications or database products may already understand the system architecture, data formats, interfaces and maintenance environment. Existing procurement relationships, staff training and technical support channels could also make vendor-native upgrades easier than introducing an entirely new provider.

Those advantages shouldn't be overstated. Chinese national origin doesn't guarantee technical interoperability. Systems supplied by Huawei, ZTE, CEIEC, Hikvision and Dahua may use different architectures, proprietary standards and interfaces, and many were deployed at different times without evidence of common technical design. Poor data quality, ageing equipment, connectivity problems and the absence of application-programming interfaces may further limit integration. Interoperability must therefore be assessed at the product and system level rather than assumed across a supposedly unified Chinese-built system.

Post-2023 advances in AI could make those systems faster, more automated and easier to use. Surveillance no longer depends only on fixed rules or human review of video feeds. New tools can support video search, automated summaries, prompt-based alerts, multilingual transcription and translation, anomaly detection, adaptive content moderation and AI-assisted analysis of network traffic.

Table 2 maps those AI advances against the six layers of Venezuela's surveillance architecture. The core point is simple: Venezuela doesn't need a complete rebuild to benefit from the AI wave. In most cases, the likely path is incremental upgrade: new software, analytics tools and replacement appliances layered onto systems already in place. The Venezuelan entities listed below should be understood as the most plausible operators, beneficiaries or institutional users of each layer, based on their known functions and public reporting. In many cases, the precise technical interfaces, contracts and data-sharing arrangements between agencies aren't publicly visible.

Table 2: How AI could upgrade Venezuela's existing digital-surveillance architecture

Existing layer	Main Venezuelan entity or operator	Plausible new AI upgrades	Human rights implications
Telecommunications infrastructure 	CANTV / Movilnet as state telecoms operators; CONATEL as the telecommunications regulator. Relevant security-sector users may include SEBIN, DGCIM, FANB, CESPA and CCDFANB.	Subject to access to relevant network metadata and traffic-analysis infrastructure, AI tools could help to classify traffic by application type, identify unusual communication patterns and assist staff in developing blocking rules.	The state could monitor digital traffic more efficiently, detect politically sensitive surges in communication and disrupt access to communications platforms more quickly during protests, elections or moments of crisis.
Digital identity and registration 	SAIME, CNE, SAREN, Banco de Venezuela / BiopagoBDV, SUDEBAN and Sistema Patria hold or operate key identity, biometric, electoral, registry, banking and citizen-service datasets.	Where databases are technically accessible and legally or administratively available to the same operators, AI could assist with record matching across biometric, welfare and registration datasets.	The state could profile citizens more easily, identify welfare recipients or politically sensitive groups, and make access to benefits more conditional on behaviour, loyalty or compliance.
Central databases and data integration 	Sistema Patria, VenApp, Sistema 1x10 del Buen Gobierno and VEN911 appear to be the main state data-integration platforms, with likely access or use by SEBIN, DGCIM, CESPA and other executive-branch agencies.	New AI could improve cross-database search, summarise large volumes of records, map relationships between individuals and organisations, flag patterns across welfare, communications or security data, and support analyst workflows across fragmented datasets.	Fragmented datasets could become more politically useful by allowing officials to link people, organisations, locations and behaviours across systems that may not be fully integrated.
Surveillance and monitoring 	VEN911, state command-and-control centres, municipal surveillance networks, PNB, SEBIN, DGCIM and CICPC operate or use public-space monitoring, incident-response and investigative systems.	Where camera quality, coverage and video-management compatibility permit, computer-vision systems could assist with person or vehicle re-identification across selected cameras.	Authorities could monitor protests, public gatherings and movement through urban spaces at greater scale, reducing the need for manual review and allowing faster deployment of security forces.
Internet control and content management 	CONATEL, CANTV / Movilnet and MIPPCI are the main actors for internet regulation, telecoms control and information/content management; SEBIN, DGCIM, FANB, CESPA and CCDFANB may be relevant security users.	LLMs and classification models could help to identify sensitive political content, translate and triage online material, prioritise content for blocking or takedown, identify patterns potentially associated with circumvention tools, subject to encryption and platform-access constraints.	Censorship could become more adaptive and scalable, allowing the state to restrict opposition messaging, independent media, civil-society organising and cross-border information flows with greater speed and precision.
Emerging analytics and AI 	MINCYT, CNTI and state AI programs are the main civilian technology-development actors; potential operational users include SEBIN, DGCIM, CICPC, PNB, FANB, CESPA and the Executive Branch.	New AI platforms could combine text, image, audio, video and network data into dashboards, generate predictive alerts, support multi-step investigative workflows, and help officials produce automated reports or risk assessments from existing state data.	Existing surveillance data could be converted into operational decisions, alerts and risk assessments, giving officials a stronger basis for pre-emptive intervention, targeted monitoring or resource allocation.

Note: Risk model, not evidence of deployment: the Venezuelan entities listed are plausible operators or users based on known functions, not confirmed data-sharing.

Table 3 provides the institutional names for the acronyms listed in Table 2.

Table 3: Acronyms and institutional names

Acronym	Full name
BDV	Banco de Venezuela / Bank of Venezuela
BiopagoBDV	Banco de Venezuela Biometric Payment System
CANTV	Compañía Anónima Nacional Teléfonos de Venezuela / National Telephone Company of Venezuela
CCDFANB	Comando de Defensa Aeroespacial Integral de la FANB / Comprehensive Aerospace Defense Command of the Bolivarian National Armed Forces
CESPA	Centro Estratégico de Seguridad y Protección de la Patria / Strategic Center for Homeland Security and Protection
CETYDIP	Centro de Estudios y Desarrollo para las Tecnologías de la Información y la Comunicación en la Administración de Justicia / Center for ICT Studies and Development in the Administration of Justice
CICPC	Cuerpo de Investigaciones Científicas, Penales y Criminalísticas / Corps of Scientific, Criminal and Forensic Investigations
CNE	Consejo Nacional Electoral / National Electoral Council
CNTI	Centro Nacional de Tecnologías de Información / National Information Technologies Center
CONATEL	Comisión Nacional de Telecomunicaciones / National Telecommunications Commission
DGCIM	Dirección General de Contrainteligencia Militar / General Directorate of Military Counterintelligence
FANB	Fuerza Armada Nacional Bolivariana / Bolivarian National Armed Forces
MINCYT	Ministerio del Poder Popular para Ciencia y Tecnología / Ministry of Science and Technology
MIPPCI	Ministerio del Poder Popular para la Comunicación e Información / Ministry of Communication and Information
Movilnet	State mobile telecommunications operator of CANTV
PNB	Policía Nacional Bolivariana / Bolivarian National Police
PSUV	Partido Socialista Unido de Venezuela / United Socialist Party of Venezuela
SAIME	Servicio Administrativo de Identificación, Migración y Extranjería / Administrative Service for Identification, Migration and Foreigners
SAREN	Servicio Autónomo de Registros y Notarías / Autonomous Service of Registries and Notaries
SEBIN	Servicio Bolivariano de Inteligencia Nacional / Bolivarian National Intelligence Service
SUDEBAN	Superintendencia de las Instituciones del Sector Bancario / Superintendency of Banking Sector Institutions
VEN911	Sistema Integrado de Emergencias VEN911 / VEN911 Integrated Emergency System

1.5 Emerging risk

Venezuela's surveillance and coercive institutions aren't a replica of China's domestic digital-governance system. Their political logic and institutional foundations are principally Venezuelan, emerging from decisions made under Chavismo and from institutions that predate much of the Chinese technological involvement examined in this chapter. They have also been shaped by other external relationships, most notably longstanding Cuban assistance in intelligence, counterintelligence, security-sector organisation and methods of political control.

China's contribution has been narrower but still significant. Chinese firms have supplied or supported important technological components: ZTE helped develop systems associated with digital identity and welfare administration; CEIEC contributed to command-centre and internet-control capabilities; Hikvision and Dahua equipment has appeared within the visual-surveillance layer; and Huawei and ZTE have supported telecommunications infrastructure. Those contributions expanded particular state

capabilities, but they didn't create Venezuela's wider authoritarian apparatus or determine its political objectives.

The result is a fragmented and uneven digital-surveillance ecosystem rather than a single integrated Chinese-built platform. Its political utility lies in the cumulative interaction between digital identity systems, welfare administration, telecommunications choke-points, selected public-space monitoring and state security institutions. Even where those systems are technically limited or only partially interoperable, they can reinforce existing mechanisms of coercion and political control.

The emerging risk is therefore one of augmentation rather than wholesale model transfer. Generative AI, computer vision and automated analytics could make some existing systems more searchable, scalable and operationally useful. The central concern isn't that Venezuela will suddenly reproduce China's surveillance state, but that Chinese or other AI tools could strengthen a domestically directed apparatus already used to manage dissent, restrict information and preserve political power.

Chapter 2: China's AI-enabled surveillance as an export product

The CCP has developed and deployed the world's most advanced tech-powered surveillance state, built in part by companies that are providing similar technology to Venezuela. The full-stack model that China has deployed isn't possible in Venezuela, which lacks the infrastructure and technological capability. The danger of AI integration in Venezuela, rather, is that it makes the existing more piecemeal infrastructure more fearsome.

By examining how the Chinese Government has deployed AI for surveillance—and how iFlytek has worked closely with the government to enhance that surveillance—this chapter shows what Venezuela could possibly do with plausible AI upgrades gleaned from a company that shaped its products to serve China's model.

2.1 The Chinese Communist Party's model of surveillance-based governance

Surveillance isn't just something the Chinese Government does; it's a core feature of its governance model. That model knows no limits on state intrusion and always seeks to maximise the use of emerging technologies for ever greater surveillance and control. After years of on-the-ground reporting on how China adopted techno-authoritarianism, *Wall Street Journal* reporters Josh Chin and Liza Lin have asserted that surveillance-based governance is the CCP's alternative to democracy.

'By mining insight from surveillance data,' they wrote in 2022, the CCP 'believes it can predict what people want without having to give them a vote or a voice. By solving social problems before they occur and quashing dissent before it spills out onto the streets, it believes it can strangle opposition in the crib.'⁶⁴

This means that, when the CCP exports surveillance systems, it isn't just exporting technology and equipment; it's exporting a specific model of governance. It's a model top Venezuelan officials have said they find appealing. Rodríguez told Chinese Vice-President Han Zheng during a December 2024 visit to China that Venezuela was 'ready to learn from China's successful experience in governance'.⁶⁵ She signed an agreement with iFlytek less than a year later, pledging to incorporate its AI technology across Venezuela's government.⁶⁶

For the time being, China is Venezuela's only major option for obtaining advanced AI technology. Broad US sanctions against the Venezuelan Government and numerous state-owned companies mean that it's illegal for US AI companies to provide them with most products and services.⁶⁷ China's economic and technological support for sanctioned authoritarian governments also means that US and Western sanctions are less effective.

2.2 China's AI-powered surveillance and control systems

After the LLM revolution that began in 2023, the Chinese Government acted swiftly to promote the deployment of AI across the economy and throughout every level of governance, enshrining this goal in its 'AI+' initiative and most recently in its 15th Five-year Plan.⁶⁸

That deployment has already made China's repression more efficient, scalable and cost-effective. LLM-powered technologies are allowing the Chinese Government to connect and integrate existing surveillance systems, and to make better use of the mass data that it already collects.

Online censorship, once conducted by armies of tens of thousands of 'online content managers' employed in-house by companies, is now conducted largely by AI. China's strict censorship laws created a market demand for cheaper, less time-intensive censorship solutions, and Chinese tech giants responded to that demand by developing LLM-powered censorship software available for sale.⁶⁹

There's now a flourishing market in China for AI-based authoritarian innovation. Companies are competing fiercely for government contracts to build surveillance systems that integrate mass data from facial-recognition camera systems, credit and digital payments, transportation data and border control. Audio, visual and text-based LLMs make it possible for local public-security bureaus to monitor live communications at scale—and in dozens of languages.

As market competition in China becomes fierce, Chinese AI companies—working hand in hand with the Chinese Government—are now seeking to sell their full suite of products in foreign markets.

The post-2023 LLM layer described in this section matters for Venezuela because it's precisely this layer—not the legacy hardware—that the MoU with iFlytek, if implemented, could bolt onto Caracas's existing infrastructure.

2.3 Case study: iFlytek

Chinese tech giant iFlytek exemplifies how the CCP's regulatory framework incentivises the development and marketing of products that enable censorship and embed political control into commercial AI products.

Founded in Hefei, China, in 1999, iFlytek has grown into a global pioneer in speech recognition, language processing and machine learning, providing real-time text transcription, translation and generative language models for clients.⁷⁰ Its AI-powered voice-recognition technology has been used to develop a pilot surveillance system for the Ministry of Public Security that can

automatically identify targeted voices in phone conversations. iFlytek has sold products to China's Ministry of Public Security, where it built an AI laboratory and national voice-recognition database, which has been used in police investigations in Anhui, Xinjiang, Tibet and Gansu.⁷¹ Its AI technology, with increasingly granular tools for monitoring and controlling public opinion, has become deeply embedded in China's judicial, censorship and governance systems.

iFlytek has now also begun to sell products and services internationally, signing agreements in countries in Southeast Asia and the Middle East.⁷²

The US Department of Commerce placed iFlytek on the US Entity List in 2019 for its role in China's surveillance and repression of Muslim minority groups in Xinjiang.⁷³

Commercial censorship products

iFlytek, like other Chinese tech giants including Tencent and Alibaba, has created AI-powered digital censorship platforms that it licenses to other companies and entities.

On its webpage, iFlytek says its 'content moderation solution' can monitor live-stream videos; 'detect risks such as political content, violations, and sensitive words in texts' for media publishers; and analyse product images, reviews and Q&A for e-commerce sites. iFlytek also notes that its distinctive speech-recognition technology can detect 'over a hundred types of politically sensitive audio content' in social voice messages, including references to 'political figures, political events, reactionary and separatist activities, and terrorism'.⁷⁴

Use of iFlytek in China's procuratorial and judicial system

iFlytek's integration into China's judicial and procuratorial system is one example of how the company's technology is integrated in government mechanisms of repression. In 2016, iFlytek formed a partnership with the Supreme People's Court to advance the application of AI in courts.⁷⁵ iFlytek's Spark Legal LLM technology has since been deployed in 89 different judicial organs, including 28 courts, in the country.⁷⁶ The company's voice-recognition technology has been installed in more than 4,200 courtrooms across 31 provincial-level regions.⁷⁷ iFlytek's technology spans an entire prosecutorial workflow, from police surveillance to courts and prisons, providing prosecutors with a distinct advantage and limiting defence counsel's visibility into the processes helping to determine their clients' fate.⁷⁸

On 3 April 2025, the Anhui Provincial People's Procuratorate launched the first province-wide AI-assisted case-handling system for Chinese procuratorial organs, jointly built on iFlytek's Spark Legal LLM and domestic computing platform.⁷⁹ China's procuratorates are the state bodies tasked with both the investigation and the prosecution of crimes.⁸⁰

International expansion

iFlytek is in the process of expanding internationally, with Hong Kong as its international headquarters.⁸¹ It has agreements with state and institutional partners in Hungary, Laos, Malaysia, Kazakhstan, Saudi Arabia, the United Arab Emirates and Qatar. iFlytek says its voice and AI technology supports real-time translation in more than 60 languages covering nearly 200 countries and regions.⁸²

iFlytek also launched the Spark ASEAN Multilingual Foundation Model covering Burmese, Lao, Tamil, Javanese, Indonesian, Thai, Vietnamese and Filipino in 2025, building a global infrastructure of languages that could support the same speech-recognition and content-moderation capabilities that iFlytek offers domestically in China.⁸³

Chapter 3: Post-2023 AI signals and emerging risks

This chapter examines new AI-related cooperation between China and Venezuela since 2023 and assesses how AI-enabled tools are being layered onto the surveillance architecture documented in Chapter 1.

Those developments involve rights that Venezuela's government already routinely violates, including the right to privacy under Article 17 of the International Covenant on Civil and Political Rights, the right to freedom of expression under Article 19, and the right to liberty and security of person under Article 9.⁸⁴ The addition of AI to an already mature repression infrastructure risks making those violations more systematic, more scalable, and harder to evade or challenge.

A Venezuelan citizen who attracts the attention of the state may now find their movements tracked through a camera network installed by Huawei, CEIEC and ZTE; their identity cross-referenced against *Sistema Patria* (the Patria System), the government benefits database that functions as a political compliance mechanism; their neighbourhood monitored through a local command room fed by a community organiser using the SEGEN app; and all of that data aggregated into the *Sala Nacional de Autogobierno Popular* (the National Popular Self-Government Chamber), which then President Nicolás Maduro said is 'directed with new Artificial Intelligence technologies together with China'.⁸⁵

This chapter draws on open-source material from both governments: Venezuelan presidential broadcasts, official ministry announcements, state media, and official legal instruments published in the *Gaceta Oficial*, and government web portals and technical manuals, including the *Sistema de Gobierno Popular y Comunal* portal and the SEGEN application user manual—alongside reporting from independent Venezuelan outlets and the civil-society monitors VE sin Filtro and DFRLab. On the Chinese side, it draws on iFlytek's own announcements, Chinese state media coverage of MoUs with the Venezuelan Government and diplomatic readouts from China's Ministry of Foreign Affairs. We treat the opacity of Venezuelan procurement as analytically significant. Because full MoU texts aren't public and vendor contracts for national-level systems aren't disclosed, the chapter is explicit throughout about what's confirmed, what can be credibly inferred, and where the evidence trail goes cold.

What's changed since 2023 is the explicit AI layer being added on top of the infrastructure that Chapter 1 documents. That shift has been formalised through sustained high-level diplomatic engagement and has culminated in the national chamber—the most concrete evidence to date of Chinese AI being integrated into Venezuela's political monitoring system.

This pursuit comes with an ideology. The same government acquiring the technology has set out, in its own publications, a doctrine that treats the information space as a battlefield. A 2025 book issued by the Science Ministry and prologued by its minister, the official who also leads Venezuela's AI cooperation with

China, describes 'cognitive warfare' waged by the West, through a domestic opposition it brands as spreading 'false information', to capture the minds of Venezuelans. The book condemns AI, algorithms and digital networks as instruments of surveillance and manipulation, without explaining why those same instruments become acceptable when imported from Beijing.⁸⁶

The vigorous pursuit of AI-enabled governance begun under the Maduro government and now continued under the Delcy Rodríguez-led interim government poses serious human-rights concerns in a context in which judicial independence doesn't exist, political dissent is criminalised and existing surveillance systems are already documented to have been used against opposition figures, journalists and ordinary citizens. Adding AI to that architecture doesn't create the repression. It scales the repression up and makes it harder to see.

3.1 The diplomatic track: from infrastructure to AI

In September 2023, Nicolás Maduro travelled to China for the state visit during which the two governments elevated their relationship to an 'all-weather strategic partnership' (the first such designation for a Latin American country) and signed a package of cooperation agreements spanning energy, finance, telecommunications and the digital economy. The agreements included a digital-economy cooperation memorandum, big-data and remote-sensing cooperation with a Chinese Academy of Sciences institute, a cooperation memorandum between China Media Group and Venezuela's Communications Ministry, and separate Huawei agreements with CANTV and Movilnet.⁸⁷ Maduro hailed the visit as the start of a 'fifth splendid stage' of the China–Venezuela relationship.⁸⁸

During the trip, Maduro toured Shanghai's Zhangjiang AI Island, where Venezuelan Science Minister Gabriela Jiménez Ramírez praised the facility as a model for AI research, industrial application and training, noting that its algorithms could help 'integrate security systems'.⁸⁹

The Zhangjiang visit was followed in April 2024 by a more formal institutional link between the two countries' technology ecosystems. Venezuela's +Ciencia Science and Technology Park signed an MoU and joint declaration with China's NeoBay Technology Park to develop joint research and innovation projects. Venezuelan officials framed the agreement as a direct outcome of Maduro's 2023 meeting with Xi, and identified AI, big data, deep learning, bioagriculture, industrialisation and robotics as priority areas for cooperation.⁹⁰

By late 2024, the domestic and bilateral tracks were converging. In November 2024, Venezuela published a law approving its bilateral investment-promotion and protection agreement with China—the negotiations for which had been completed

during Maduro's September 2023 state visit to China.⁹¹ In the same month, Venezuela's National Assembly approved a draft Artificial Intelligence Law in its first reading, presenting AI as a tool to strengthen national technical and scientific capacities and 'sovereign' productive development, while calling for the 'supervision, control and promotion' of AI across areas including education and local development. The Bill also contemplated participation by the communes, placing AI policy within Venezuela's territorial and political structures rather than treating it as a purely technical matter.⁹² This legislative groundwork was laid during one of the most repressive stretches in Venezuela's recent history: the months following the disputed July 2024 election, in which around 2,000 people were arbitrarily detained.⁹³

In December 2024, Chinese Vice President Han Zheng met Delcy Rodríguez during a visit framed around reviewing and strengthening the China–Venezuela cooperation map established after Maduro's 2023 state visit, including in politics, energy, the economy, finance and technology.⁹⁴ According to the Chinese Foreign Ministry's readout, Rodríguez said that Venezuela was 'ready to learn from China's successful experience in governance'.⁹⁵

Those diplomatic and legal developments helped set the stage for more specific corporate engagement in 2025. In April, Maduro launched a new telecommunications and technology policy 'motor' (a Venezuelan Government term for a priority sectoral engine) and called for 'exponential' growth in 5G networks, sovereign satellite capacity, remote-area connectivity and technologies linked to AI. This wasn't yet a China-specific AI agreement, but it placed AI inside the broader infrastructure agenda into which later China-linked corporate engagement could fit.⁹⁶ That same month, Rodríguez visited the Beijing facilities of Chinese AI company iFlytek to explore cooperation in AI for the hydrocarbons, health and education sectors, stating that 'only China' could ensure that the global South had access to AI 'for development and not for domination'.⁹⁷

The engagement deepened over the following weeks. In May 2025, Venezuela's Science Ministry announced that 25 Venezuelan scientists would travel to China for a month-long AI training program.⁹⁸ In June, Chinese Ambassador Lan Hu met Science Minister Gabriela Jiménez; the embassy readout identified science, health, human-resource training, space and AI cooperation as part of the agenda.⁹⁹

The follow-up in Caracas showed that this engagement was being widened into a cross-government agenda. In early July, Gabriela Jiménez Ramírez met iFlytek executive Jin Lin at Venezuela's Science Ministry, alongside officials from the ministries responsible for ecosocialism, health, hydrocarbons, defence, education, university education, and communication and information. Jiménez described the meeting as the beginning of Venezuela's AI cooperation agenda with China, while emphasising the use of technological tools to strengthen government capacity in 'wellbeing, peace and security' and national stability. Jin, in turn, reportedly highlighted the use of AI and related technologies to detect false information, guarantee cybersecurity and improve the effectiveness of governance.¹⁰⁰

The clearest corporate expression of this trajectory came the following day, during the Gran Expo China–Venezuela in Caracas, when a package of agreements covering water resources, economic and technical cooperation, and the development of 'sovereign' AI technologies involving iFlytek was signed by Executive Vice President Delcy Rodríguez and Chinese Ambassador Lan Hu.¹⁰¹ Maduro declared that 'Venezuela is through the front door into the vanguard of AI development,' naming tourism, agriculture, hydrocarbons, health research, education and telecommunications as target areas.¹⁰²

The diplomatic follow-up continued the next month. In August 2025, Lan Hu met Venezuela's oil and gas ministry's vice minister responsible for AI affairs. According to the Chinese Embassy readout, Lan said China was willing to deepen AI cooperation with Venezuela and promote AI development in a 'beneficial, safe and fair' direction. The Venezuelan side said it wanted to learn from China's AI development experience, expand cooperation and use AI to support economic and social development.¹⁰³

The most recent signal came in July 2026. On 16 July, on the eve of the World Artificial Intelligence Conference in Shanghai, Venezuela was among 29 states that signed the founding agreement of the World Artificial Intelligence Cooperation Organization, a China-initiated intergovernmental body to be headquartered in Shanghai with China as the treaty's depositary.¹⁰⁴ Venezuela was represented by Isabel Iturria, the sectoral vice-president for science, technology, education and health.¹⁰⁵ The agreement commits signatories to cooperation on AI capacity-building, technical standards, open-source ecosystems and supply–demand matching among member states, and expressly confines the organisation's functions to the civilian domain of AI. The agreement is subject to ratification and takes effect once a third instrument of ratification, acceptance or approval is deposited.¹⁰⁶ Venezuela's signature therefore places no new Chinese system inside the country. What it does is extend the trajectory that this chapter traces. A relationship that began with imported hardware is now being written into the multilateral architecture through which Beijing seeks to shape AI development and governance across the global South.¹⁰⁷

Throughout this sequence of events, China–Venezuela AI cooperation was mostly publicly framed as being about development, research and industrial modernisation. But the security logic was visible from the start, evidenced by Jiménez's comment about 'integrating security systems' as well as later references to false-information detection, cybersecurity, governance effectiveness and national stability.¹⁰⁸ In Venezuela's political context, that points to the risk that AI won't just modernise the state, but strengthen its capacity for censorship, surveillance and control.

A sceptic might note that China signs AI MoUs with dozens of governments, most of which never progress past the signing ceremony. Three things distinguish this one. First, it lands on an already assembled surveillance base rather than a blank slate. The identity, camera and command-room layers that an

inference layer would need are built and operating.¹⁰⁹ Second, the Sala Nacional rollout (Section 3.2) shows the state actively expanding the political-monitoring architecture that the MoU would enhance.¹¹⁰ Third, Venezuela's leadership has articulated its ambition for AI-enabled governance in its own words. The MoU may yet lapse, but the conditions that usually leave such agreements inert are absent here.

Maduro's capture by US forces in January 2026 didn't erase this trajectory so much as complicate it. The interim government of acting president Delcy Rodríguez inherits the AI and communal-governance architecture built under Maduro, even as it faces intense US pressure to open the oil sector to foreign investment and distance Venezuela from China, Russia, Iran and Cuba, while also releasing political prisoners.¹¹¹ The result isn't a clean break from the Maduro-era technology state but an unresolved transition, in which US pressure pulls the interim government one way, while the Chinese-built systems embedded in its governing infrastructure, and the officials who procured them, pull the other.

What the minister wrote

Venezuela's pursuit of Chinese AI was led by Delcy Rodríguez, then Maduro's Vice President and now the country's acting president, but she isn't its only architect. Gabriela Jiménez-Ramírez, the Science Minister whose meetings and signatures also recur through this chapter, has lent her name to a book-length argument against the technology she is helping to bring in. In 2025, she prologued a volume published by her own ministry.¹¹² The book casts AI, alongside social media and 'Industry 4.0', as a weapon the West uses to wage 'cognitive warfare' on Venezuela: to 'poison the consciousness' of free peoples and capture their capacity for critical thought.¹¹³ Its quarrel isn't that the technology is foreign but that it surveils, profiles and manipulates by nature.

The book is a window into how the government thinks. It treats the information space as a domain of war the state must hold. One contributor argues that communications should be designated a field of 'integral national defence', citing a general's view that the media are 'a threat to the security of the nation'; the government's own Plan de la Patria 2025–2031 treats cyberspace as a matter of sovereignty and national security and calls for 'social oversight' (*contraloría social*) of the media: organised community monitoring of the press and online speech, framed as grassroots citizen oversight rather than state censorship.¹¹⁴ And it names the enemy at home—the book brands opposition figures as 'mercenaries' and 'delinquents' who spread 'false information' as proxies of the imperial assault, citing, among other examples, opposition claims that state-produced petrol made cars explode.¹¹⁵ Where the book's philosophical chapters reject AI outright, the ministry's public statement of the doctrine reaches for it: 'cognitive resilience', it argues, demands not only critical-thinking education and limits on big tech's use of data, but 'artificial intelligence tools that detect patterns of manipulation in real time'.¹¹⁶

That's the doctrine behind the deals, and at its core is a claim about sovereignty: AI in foreign hands is a weapon of domination; in the state's own, a tool of defence. The information space is a battlefield, its control a matter of national security, and the speech of critics is enemy manipulation to be detected and countered. The government wants the means to do that, and the Chinese AI documented in this chapter is how it intends to get them: a sovereign defence against foreign domination, sourced from a foreign power.

Venezuela's sovereign AI system: intentions versus capabilities

Venezuela's government aims to develop AI that's both innovative and sovereign, and hopes iFlytek can deliver that.¹¹⁷ But the country's limited AI capacity, combined with the nature of iFlytek's products, means Venezuela would have little agency itself, and would instead become dependent on Chinese AI frameworks, chips and models, including the built-in political biases.

In their MoU, iFlytek and the Venezuelan Government stated their intention to jointly develop an AI ecosystem that's both innovative and sovereign.¹¹⁸ As governments around the world seek to develop domestic AI capabilities, the desire among national stakeholders for jurisdiction over every part of the AI supply chain has led to a demand for 'sovereign AI'—a loose term that aspires to give a national government sovereign control over as many parts of the AI supply chain as possible, including control over sensitive data, control over infrastructure such as cloud servers, and control over the actions of an AI model.

Venezuela currently lacks the capability to ensure multiple areas of AI sovereignty. It has recently begun to set up specialised government departments for AI oversight, but there's no evidence that the country contains the specialised data centres necessary to undertake AI work processes within its borders.¹¹⁹ The country ranked 145 out of 195 countries evaluated by the Government AI Readiness Index for 2025, and is effectively barred from accessing cutting-edge AI chips as part of longstanding US trade embargoes.¹²⁰ Perhaps even more significantly, both AI inference and training require substantial and uninterrupted supplies of electricity, but Venezuela has long suffered from chronic instability in its supply and is prone to sudden power cuts.¹²¹

The MoU includes integrating AI into specific fields, including agriculture, education, telecommunications and the country's hydrocarbons industry. Yet many of the deliverables advertised in those fields by iFlytek require a well laid out AI stack, including stable electricity supplies, sufficient AI computing and adequate data storage.¹²²

The current infrastructure problems in Venezuela give iFlytek an advantage. It can leverage its position to make the country dependent on Chinese AI systems, making those the foundations of any future AI development. iFlytek currently offers customers multiple options for AI services that require external computing, in which a company's or government's data is sent to cloud services

for processing. Those cloud providers are likely to be Huawei Cloud, which listed iFlytek as using its computing infrastructure during their 2026 conference on Latin America.¹²³ Huawei Cloud's data-location documentation currently lists three 'cloud service regions' in Latin America—Mexico City, São Paulo and Santiago—none of them in Venezuela.¹²⁴ Such an arrangement would give overwhelming control of any Venezuelan AI processes to Chinese companies, with sensitive data hosted on Chinese-built servers located outside Venezuela's borders.

Alternatively, Venezuela's government could preserve a greater degree of control by using a different iFlytek product, known as an 'all-in-one server'. This is a small server, equipped with specialised chips, that's installed within a customer's premises. iFlytek advertises this product as providing 'secure, controllable intelligence' for clients.¹²⁵ iFlytek claims the servers aren't connected to the internet and are capable of both AI training and inference, creating a system that can be customised to individual business needs while hosting all data locally to maintain information security.¹²⁶ Such a solution would solve the sovereignty concerns of hosting sensitive data in Chinese-owned cloud servers outside Venezuela.

But using those local servers would bring difficulties of their own. While Venezuelan companies could install AI models of their choice on these all-in-one servers, some may conclude it would be easiest to use the server's pre-installed models: iFlytek's own 'Spark' (星火) models and DeepSeek models. It's possible that iFlytek could help Venezuela finetune those models to fit the country's needs and any future AI laws that may be adopted in Venezuela, but the automatic inclusion of Spark and DeepSeek models on those servers raises concerns about built-in information controls. Both have been registered for use within China by the Cyberspace Administration of China, meaning they've been aligned with CCP information guidance requirements.¹²⁷

There are several technical methods that can work around the information controls encoded within those models, but it's unclear how effective they are. It could be possible to attach the model to a RAG (retrieval-augmented generation) pipeline, which allows the model to tailor its answers based on additional data it's been given access to. Developers could also adapt a model's responses through a system prompt—a fixed set of instructions attached to any question posed by a user, acting as a set of guidelines for how the model can and can't respond.¹²⁸ However, it's unclear whether either of those solutions would be enough to override the model's original training. Finetuning is a more substantial change, whereby a model itself is given additional training. But it has proved difficult for developers from a variety of different countries to thoroughly remove CCP propaganda from a variety of models finetuned from Chinese originals.¹²⁹ Any institution that used these deployments as a chatbot for information searches would risk exposing the country to viewpoints built for China's information flows, not Venezuela's.

Venezuela can't use those servers to train new sovereign AI models, and that could lead to dependency on Huawei AI chips. While the

servers would provide enough computing power to run tasks on a pre-existing AI model, they wouldn't have enough power to train new models from scratch. Trying to work around this, for example by buying up hundreds of all-in-one servers and cannibalising them for chips, also wouldn't work for training a new model. iFlytek doesn't mention what GPUs or CPUs the server contains, but it's most likely Huawei Ascend chips, given iFlytek's acknowledgement of their 'close partnership' in their 2025 annual report, and extensive reliance on Huawei's chips for its own AI training.¹³⁰ iFlytek's management publicly complained at their 2026 earnings conference of the 'major difficulties' the company has faced when trying to train new models on Huawei chips.¹³¹ iFlytek also doesn't make public what computing capability these servers have, or their electricity consumption, so it's difficult to determine how they would fare in Venezuela's patchy electricity grid.

These pre-existing infrastructure issues are compounded by the devastating effects of two earthquakes of magnitude 7.2 and 7.5 that struck the country in late June 2026.¹³²

3.2 The national chamber: AI direction at scale

On 27 January 2025, Nicolás Maduro announced the creation of a *Sala Nacional de Autogobierno Popular* (National Popular Self-Government Chamber)—a national command room that would centralise information from across Venezuela's communal governance structures—and a 90-day directive to install 5,334 local counterparts, one for every commune or communal circuit in the country. The chamber, he said, would operate with AI and 'Chinese technology, which is cutting-edge technology that is leading the world, secure technology'.¹³³ No vendor was named; nor was any technical detail offered. But, as a statement of intent, it was the most explicit connection any Venezuelan official had drawn between the country's political monitoring architecture, AI and China.

The announcement placed the new chamber above an existing reporting architecture rather than creating a system from scratch. The 1x10 del Buen Gobierno system had been operating since 2022 as a geo-referenced case-management platform through which citizens could report public-service problems via VenApp's 'Línea 58' channel or the *Sistema Patria* platform. Later official accounts describe the system as covering areas including water, electricity, health, gas, education and telecommunications.¹³⁴

Reports are linked to the citizen's personal data and location, tracked through standardised case statuses, and routed to the responsible ministry or local authority by what official documentation calls an 'intelligent system', with human operators stepping in when the software can't classify a case.¹³⁵ Below the software sits a territorial layer of organised communal and party-state structures. Official accounts describe the 1x10 system as operating through roughly 49,000 communal councils and 5,334 communal circuits, alongside communes, Local Committees for Supply and Production (CLAP) food-distribution committees,

street and community leaders, local groups related to Venezuela's ruling party and other social movements; participation is organised from the community and family levels.¹³⁶ The *salas de autogobierno* were designed as the oversight layer for this system; physical rooms use government information platforms to monitor 1x10 complaints, CLAP movements, matters related to Venezuela's state oil and gas company, communal financing and other territorial policies, reporting upwards to the national chamber. The 'T3' Maduro invoked at the launch refers to the third of the seven transformations in Venezuela's 2025–2031 national plan: citizen security; defence; unity and territorial integrity.¹³⁷ The chamber was announced, in other words, not as a service-delivery tool but as part of the security pillar of the state's planning framework.

The rollout was fast and, by the government's own telling, nationwide. The *Sala Nacional* was activated on 7 February 2025 from the Executive Vice Presidency, then held by Delcy Rodríguez, and was described as connected 24 hours a day to the 5,334 communes and communal circuits, centralising territorial information 'with the use of Chinese technology and Artificial Intelligence'.¹³⁸

A formal installation and operating guide followed on 20 February.¹³⁹ By late April, official reporting put the local network at roughly 80% operational, and Maduro ordered full consolidation within 30 days. The municipality of Guaicaipuro reported the delivery of technology kits to each of its 43 *salas* the same week.¹⁴⁰ By late June, the official *Sala de Autogobierno* portal reported that more than 94% of communal circuits had activated *salas*.¹⁴¹ On 20 October 2025, Maduro announced the milestone figure: 'We now have 99.83% of the popular self-government *salas* installed across the national territory, 5,327 *salas*.'¹⁴² By December, government-aligned reporting said the 1x10 system had resolved 88.07% of reports received through VenApp, and described 5,336 communal self-government rooms as articulated to the national chamber for reporting and activating responses to community complaints.¹⁴³ Every figure in this account is the government's own. No independent verification of the network's true size or functionality exists.

Who runs the rooms matters as much as what they contain. The staffing model isn't a civil service. The *salas* are run by *voceros* (spokespersons) of the local communal councils, each holding a portfolio mapped to one of the seven transformations, alongside a locally elected justice of the peace and a commune parliamentarian.¹⁴⁴ The territorial structures that feed them are formally party infrastructure. European Union asylum-agency country reporting has documented that appointment as a street chief requires PSUV (*Partido Socialista Unido de Venezuela* / United Socialist Party of Venezuela) membership, and the *Patria* platform that carries the system's data is registered not to any state agency but to the party itself: the *patria.org.ve* domain is held in the PSUV's name.¹⁴⁵ The *salas* also bypass the elected layer of the Venezuelan state. They create a parallel reporting channel from directly the commune to the national chamber that can bypass mayors and governors as intermediaries, while also monitoring and subordinating their participation. The clearest evidence for what

happens inside the rooms concerns the SEGEN app. A user manual published on the government's *Sistema de Gobierno Popular y Comunal* portal requires an Android phone, location access and a dedicated reporting form named 'SALAS DE AUTOGOBIERNO'. State-aligned reporting in March 2026 confirmed that the app was in use on devices inside the *salas* to register territorial risk events with precise coordinates as part of a community-risk information system integrated with state geo-referencing platforms.¹⁴⁶ A commissioned technical assessment suggested the possible use of Huawei AirEngine access points and CEIEC-style dashboard infrastructure, but those claims rest on inference from the companies' documented histories with the Venezuelan state, not on procurement records, contracts or photographs of equipment installed in the *salas*. They should therefore be treated as analytical leads rather than established findings.¹⁴⁷

The chamber also didn't arrive in a vacuum of intent. Through 2025, Interior Minister Diosdado Cabello repeatedly described the state's monitoring capabilities in openly punitive terms: he warned opposition protesters that 'there are cameras everywhere, so behave yourselves, they're watching you'; directed mayors to pressure private businesses into pointing cameras toward public streets; and by December said VEN911 already had more than 7,000 cameras. None of this places those systems inside the *Sala Nacional*. It establishes the disposition of the officials who built it.¹⁴⁸

The available evidence supports a clear conclusion that Venezuela has built a nationwide, geo-referenced case-management and dashboard architecture that aggregates citizen-level data from household-level structures up to a national command room. The system keeps humans in the loop, operates through party-fused communal structures, and remained active in March 2026, when the communal minister put the network at 5,336 *salas* while acknowledging that not all had dedicated physical premises.¹⁴⁹

The least documented part of the system is the one Maduro emphasised most: AI. Maduro's own framing made AI and Chinese technology a defining feature of the chamber, yet the public installation guide is an organisational manual rather than a technical specification. It doesn't identify an AI system, vendor, model, procurement process, software architecture or concrete AI function; nor has this research identified any other public document that does so.¹⁵⁰

What remains unproven is the more specific claim that iFlytek, or any other named Chinese company, supplies the *Sala Nacional* or local *salas*, or that predictive algorithms alleged in Venezuelan commentary are deployed inside the chamber itself.¹⁵¹

3.3 The data stack

Venezuela has built the lower reaches of an AI system with a citizen-level dataset that's collected through the country's communal and surveillance structures and then aggregated into a single national command room that the government says runs 'with the use of Chinese technology and Artificial Intelligence'.¹⁵² But collecting data and acting on it intelligently are different

problems. A working AI capability is a stack with raw data at the base, then the storage and computers that hold and process it, then the models that interpret it, then the applications that put the output in an official's hands. Venezuela has assembled the base, but everything its AI announcements promise sits in the layers above.

Those upper layers are the least documented part of the system and the most consequential. Two factors decide whether Venezuela's 'sovereign' AI would be sovereign in any meaningful sense: where the aggregated data physically lives, and what processes it. Neither has a confirmed answer in the public record, and both plausible paths run through China. The data can be sent to Chinese cloud infrastructure for processing or held on Chinese-built servers and chips installed inside Venezuela. Either way, the storage, computers and models that would turn the dataset into a working capability would be supplied, and to a significant degree controlled, by Chinese companies. A stack built on those terms is sovereign only at its base.

The government's ambitions for the top of that stack run well ahead of what it can build there on its own.

3.4 Civil-rights risks: what the architecture enables

Venezuela's surveillance architecture doesn't need AI to violate civil rights. The government has been breaching them with the same systems for years, including the right to privacy under Article 17 of the International Covenant on Civil and Political Rights, the right to freedom of expression under Article 19, and the right to liberty and security of person under Article 9.¹⁵³ What an AI layer changes isn't the kind of abuse but its scale, speed and opacity. It would industrialise practices the state now does by hand.

The clearest risk to civil rights is in identification. Today, a Venezuelan attracts the state's attention mostly by doing something that draws a human eye, such as joining a protest, posting the wrong thing or being named by a neighbour. An analytical layer on top of the aggregated data would loosen that constraint. Facial recognition run across the camera network, voiceprint matching applied to a telecommunications system the state already owns, and automated cross-referencing against the *Patria* identity register would let the government identify, locate and rank people without waiting for any of them to act. Voiceprint identification isn't a hypothetical capability for the company Venezuela has partnered with. iFlytek sells a voiceprint-recognition service that enrolls voices into a database and matches a speaker against it one to one or one to many—the technical basis for picking a single person out of a population by sound.¹⁵⁴ The same speech and voice technology underpins the surveillance systems iFlytek has supplied to public-security agencies in Xinjiang, for which it was added to a US trade blacklist.¹⁵⁵

Enhanced identification could then feed further detentions. In the months after the disputed July 2024 election, the government arbitrarily detained around 2,000 people, using the architecture as

it then stood.¹⁵⁶ The same architecture with prediction layered on top would let the state build target lists from patterns rather than incidents, flagging association, movement or online sentiment before anyone reaches the street. That shifts a reactive security apparatus towards an anticipatory one and raises the prospect of detention based on what a system forecasts a person might do rather than anything they have done.

On expression, the risk begins with how the government talks about it. In January 2026, the Science Ministry published a paper on 'cognitive warfare', defining it as a form of conflict the aim of which 'is not the physical destruction of the enemy, but the nullification of his capacity for critical thought', waged continuously through social networks, media and entertainment platforms. Its proposed remedy was to use 'artificial intelligence tools that detect patterns of manipulation in real time'.¹⁵⁷

3.5 AI-powered surveillance: a warning, not a forecast

What this chapter has traced is a shift, since 2023, from infrastructure to intelligence. The surveillance systems China helped build in Venezuela were already extensive; what's new is the deliberate move to layer AI on top of them, formalised through sustained high-level diplomacy and made concrete in the iFlytek agreement, the national command chamber and the data stack that feeds it.

The capability isn't yet complete. Venezuela depends on China for the computers, the chips and the models, and the distance between what the government has announced and what it can field remains wide. But the direction is unambiguous, and it's set down in the state's own words. The government treats the information space as a domain of war, the control of which is a matter of national security, and it has named the tool that it wants: AI to detect, in real time, the speech it casts as enemy manipulation. The data has already been collected, linked and aggregated to a single point of command. What remains is integration.

That's what makes this a warning rather than a forecast. Adding AI to Venezuela's surveillance architecture doesn't create the repression; it industrialises it, rendering it more systematic, more scalable and harder to see or contest. The architecture is largely built. What isn't yet settled is whether it will be completed or taken apart.

Conclusion: political uncertainty and a narrow opportunity in Venezuela

The surveillance regime in Venezuela is alive and well. Despite Maduro's fall, political detentions and the use of the surveillance system for repression are ongoing. Although Venezuela isn't capable of recreating China's full-stack surveillance apparatus, there's still a distinct possibility that AI will be used to enhance Venezuela's own oppressive surveillance.

However, the current Venezuelan leadership's heavy dependence on the US represents an opportunity. Democratic nations and international civil society have a rare opening to push Delcy Rodríguez and other top officials to rip out the country's surveillance equipment, scrap the agreement with iFlytek and liberalise the country's political system to ensure that those changes last.

Beijing for its part recognises this opening, and the risk it poses to Chinese companies and China's political influence there. China's leaders appear to understand that assets and investments of its national champions are at risk in Venezuela. Beijing's approach seems to be, in part, strengthening oversight of state-owned assets abroad to assist in risk protection and management.¹⁵⁸

This opening might not last. There's still time to ensure that Venezuela doesn't strengthen its surveillance apparatus—and its ties to Beijing—by integrating Chinese AI into its systems.

Notes

- 1 Tyler Pager, Anatoly Kurmanaev, 'How Marco Rubio is running Venezuela from afar', *New York Times*, 13 July 2026, [online](#).
- 2 Council on Foreign Relations, 'US–Venezuelan relations', 18 November 2005; 'Observation of the 1998 Venezuelan elections', The Carter Center, February 1999, 22, [online](#).
- 3 Brianna Lee, Kevin Lizarazo, Jeremy Sherlick, *Venezuela's Chavez era*, Council on Foreign Relations, updated 1 May 2017, [online](#); Associated Press, 'Chávez to nationalise Venezuelan companies', *CBS News*, 8 January 2007, [online](#); Carlos Lauría, Sauro González Rodríguez, 'Static in Venezuela', Committee to Protect Journalists, 24 April 2007, [online](#); 'A decade under Chávez: political intolerance and lost opportunities for advancing human rights in Venezuela', *Human Rights Watch (HRW)*, 18 September 2008, [online](#).
- 4 Manuel Casique Herrera, 'Communes and crisis: a Venezuelan migrant replies to Geo Maher', *Spectre Journal*, 23 March 2026, [online](#).
- 5 Michael McCarthy, Jennifer McCoy, 'The limits of legacy: the post-Chávez challenge and electoral legitimacy', *Americas Quarterly*, 24 July 2013, [online](#); 'China–Venezuela fact sheet: a short primer on the relationship', US–China Economic and Security Review Commission, 13 January 2026, [online](#).
- 6 Audie Cornish, 'UN report reveals "shockingly high" number of extrajudicial killings in Venezuela', *NPR*, 5 July 2019, [online](#).
- 7 'Situation in the Bolivarian Republic of Venezuela I', International Criminal Court, [online](#); 'Venezuela: ICC investigation opens', *HRW*, 4 November 2021, [online](#).
- 8 Gabriela Sá Pessoa et al., 'US recognises Venezuela's opposition candidate as winner of disputed presidential election', *PBS NewsHour*, 2 August 2024, [online](#); Vanessa Buschschlüter, 'Venezuela's Maduro declared winner in disputed vote', *BBC News*, 29 July 2024, [online](#).
- 9 'Punished for seeking change: killings, enforced disappearances and arbitrary detention following Venezuela's 2024 election', *HRW*, 30 April 2025, [online](#); Firstpost, 'Venezuela: Opposition leader Gonzalez forced into exile amid election turmoil | Firstpost America', *YouTube*, [online](#).
- 10 Ana Lonova, 'Venezuela Gallup poll food insecurity', *New York Times*, 8 January 2026, [online](#); State Department, 'Venezuela: a democratic crisis', US Government, 30 October 2020, [online](#); 'Venezuelan humanitarian and refugee crisis', Centre for Disaster Philanthropy, last updated 8 January 2026, [online](#).
- 11 Elizabeth C Economy, 'Exporting the China model', prepared statement to the US–China Economic and Security Review Commission hearing on 'A "China model?" Beijing's promotion of alternative global norms and standards', 13 March 2020, [online](#).
- 12 Oshin Pandey, Pavan Raghavendra, 'How China's oil-backed lending in Venezuela fell into distress—and what might come next', *AidData*, 23 January 2026, [online](#).
- 13 Angus Berwick, 'How ZTE helps Venezuela create China-style social control', *Reuters*, 14 November 2018, [online](#).
- 14 Florantonia Singer, 'Sistema Patria: a new digital tool for social control in Venezuela', *EL PAÍS English*, 24 April 2021, [online](#).
- 15 Berwick, 'How ZTE helps Venezuela create China-style social control'; Office of Senator Chris Van Hollen, 'Van Hollen, Rubio urge administration to investigate ZTE business with Venezuelan Government', US Senate, 28 November 2018, [online](#).
- 16 Singer, 'Sistema Patria: a new digital tool for social control in Venezuela'.
- 17 Alejandro Peña Esclusa, 'China tightening its grip on Latin America', *GIS Reports Online*, 5 February 2026, [online](#).
- 18 Benjamin Creutzfeldt, Parsifal D'Sola Alvarado, 'Venezuela, the state that refuses to collapse', *Stimson*, no date, [online](#).
- 19 David Wainer, 'Russia, China veto UN resolution seeking Venezuela elections', *Bloomberg*, 28 February 2019, [online](#).
- 20 'China, Venezuela upgrade ties to "all-weather strategic partnership"—state media', *Reuters*, 13 September 2023, [online](#).
- 21 'US intercepts oil tanker off Venezuelan coast, officials say', *Reuters*, 21 December 2025, [online](#).
- 22 Diana Roy, 'China's growing influence in Latin America', Council on Foreign Relations, 6 June 2025, [online](#).
- 23 Carlos Eduardo Piña, 'Venezuela', *The People's Map of Global China*, updated 24 October 2025, [online](#).
- 24 James Palmer, 'What the Venezuela attack means for China', *Foreign Policy*, 6 January 2026, [online](#); Cate Cadell, 'China condemns US strike in Venezuela, hours after diplomat met with Maduro', *Washington Post*, updated 3 January 2026, [online](#).
- 25 Alexander Ward et al., 'CIA concluded regime loyalists were best placed to lead Venezuela after Maduro', *Wall Street Journal*, 6 January 2026, [online](#).
- 26 Office of the United Nations High Commissioner for Human Rights, 'Independent international fact-finding mission on the Bolivarian Republic of Venezuela', United Nations, [online](#); 'Venezuela: Enforced disappearances amount to crimes against humanity', Amnesty International, 15 July 2025, [online](#); 'Punished for seeking change: killings, enforced disappearances and arbitrary detention following Venezuela's 2024 election', *HRW*, 30 April 2025, [online](#).
- 27 'Reglamento Interno de Organización y Funcionamiento de la Fundación Patria', *Gaceta Oficial de la República Bolivariana de Venezuela*, 23 September 2019, 41(722):448, [online](#).
- 28 'Venezuela: country focus', European Union Agency for Asylum, November 2023, [online](#); Iria Puyosa, Andrés Azpúrua, 'Watch the watchers: surveillance technologies for political control in Venezuela', *Digital Forensic Research Lab*, 26 March 2026, [online](#).
- 29 'Venezuela's repressive state apparatus "intact" despite leadership change', *UN News*, 12 March 2026, [online](#).
- 30 Puyosa & Azpúrua, 'Watch the watchers: surveillance technologies for political control in Venezuela'.
- 31 Aleks Phillips, 'Rights groups critical as Venezuela prisoner release scheme "coming to an end"', *BBC News*, 25 April 2026, [online](#).
- 32 Embassy of the People's Republic of China in Georgia, 'Wang Yi meets with Venezuelan Vice President Delcy Eloy Rodríguez Gómez', PRC Government, 7 September 2023, [online](#).
- 33 Puyosa & Azpúrua, 'Watch the watchers: surveillance technologies for political control in Venezuela'.
- 34 Jose Miguel Alonso-Trabanco, 'Cuba's intelligence masterstroke in Venezuela', *Geopolitical Monitor*, 9 August 2019, [online](#); Angus Berwick, Sarah Kinoshian, Vivian Sequera, 'Special report: How Cuba taught Venezuela to quell military dissent', *Reuters*, 14 December 2019, [online](#).
- 35 Diana Roy et al., 'Venezuela: the rise and fall of a petrostate', Council on Foreign Relations, updated 31 July 2024, [online](#); Ron MacCammon, 'The countdown to Venezuela's digital-AI authoritarian future: two clocks in a strategic race', *Small Wars Journal*, 2 September 2025, [online](#).
- 36 'Sistemas de videovigilancia y atención de emergencias en Venezuela' [Video surveillance and emergency response systems in Venezuela], *Transparencia Venezuela*, 2021, [online](#); Research Directorate, 'Venezuela: Requirements and procedures to obtain the Homeland Card (Carnet de la Patria); content, appearance, and security features; social services available for holders; availability of documentation to prove that a person does not possess the card; sample (2020–January 2022)', Immigration and Refugee Board of Canada, Canadian Government, 28 January 2022, [online](#); Department of the Treasury, 'Treasury sanctions CEIEC for supporting the illegitimate Maduro regime's efforts to undermine Venezuelan democracy', US Government, 30 November 2020, [online](#).
- 37 'Sistemas de videovigilancia y atención de emergencias en Venezuela' [Video surveillance and emergency response systems in Venezuela], *Transparencia Venezuela*, 2021, [online](#).
- 38 Berwick, 'How ZTE helps Venezuela create China-style social control'.
- 39 'Sistemas de videovigilancia y atención de emergencias en Venezuela', *Transparencia Venezuela*, January 2022, [online](#); Department of the Treasury, 'Treasury sanctions CEIEC for supporting the illegitimate Maduro regime's efforts to undermine Venezuelan democracy'.
- 40 Puyosa & Azpúrua, 'Watch the watchers: surveillance technologies for political control in Venezuela'.
- 41 Puyosa & Azpúrua, 'Watch the watchers: surveillance technologies for political control in Venezuela'.

- 42 Carlos M Baldo et al., 'Huawei in Venezuela: a review of 2006–2019', *Revista de Gestão*, 2021, 28(4):358–375, [online](#).
- 43 Committee staff, 'The new Big Brother: China and digital authoritarianism', US Senate Committee on Foreign Relations, 21 July 2020, [online](#).
- 44 Committee staff, 'The new Big Brother: China and digital authoritarianism'.
- 45 Berwick, 'Special report: How ZTE helps Venezuela create China-style social control'; Daphne Psalidakis, 'US imposes sanctions on Chinese firm accused of undermining democracy in Venezuela', *Reuters*, 1 December 2020, [online](#); Lorenzo Franceschi-Bicchieri, 'Venezuela's president thinks American spies can't hack Huawei phones', *TechCrunch*, 3 September 2025, [online](#).
- 46 Rebecca Arcesati, 'China's rise in digital governance: deploying technology to deliver public goods at home and abroad', *MERICS*, March 2022, [online](#).
- 47 Research Directorate, 'Venezuela: Requirements and procedures to obtain the Homeland Card (Carnet de la Patria); content, appearance, and security features; social services available for holders; availability of documentation to prove that a person does not possess the card; sample (2020–January 2022)'; Laura Vidal, translated by Alexis Faber, 'Venezuelans shudder at news of biometric ID deal with Chinese tech giant', *The World from PRX*, 28 December 2018, [online](#).
- 48 Jordan Flores, 'Carnet de la patria y sistema patria: cuatro preguntas para entender sus diferencias y alcance' [Homeland Card and Homeland System: four questions to understand their differences and scope], *El Diario*, 10 April 2021, [online](#).
- 49 'Patria', *Plataforma Patria*, archived home page, 7 February 2026, [online](#).
- 50 Hanna Duggal, AJLabs, 'Venezuela explained in 10 maps and charts', *al-Jazeera*, 28 November 2025, [online](#).
- 51 'Patria', *Plataforma Patria*, archived home page, 7 February 2026, [online](#).
- 52 Berwick, 'How ZTE helps Venezuela create China-style social control'.
- 53 Laura Vidal, Jillian C York, 'Desvelando la represión en Venezuela: un legado de vigilancia y control estatal' [Unveiling repression in Venezuela: a legacy of state surveillance and control], Electronic Frontier Foundation, 18 September 2024, [online](#).
- 54 Berwick, 'How ZTE helps Venezuela create China-style social control'.
- 55 Committee staff, 'The new Big Brother: China and digital authoritarianism'.
- 56 'Sistemas de videovigilancia y atención de emergencias en Venezuela', *Transparencia Venezuela*, January 2022, [online](#).
- 57 Ryan Mallett-Outtrim, '30,000 more security cameras and 17,000 less guns on Venezuelan streets', *Venezuelanalysis*, 27 November 2013, [online](#).
- 58 Jonathan E Hillman, Maesea McCalpin, 'Watching Huawei's "safe cities"', Center for Strategic and International Studies, 4 November 2019, [online](#); Maya Wang, 'China's techno-authoritarianism has gone global', *HRW*, 8 April 2021, [online](#); Katherine Atha, Jason Callahan, John Chen et al., 'China's smart cities development', US–China Economic and Security Review Commission, January 2020, [online](#).
- 59 'Sistemas de videovigilancia y atención de emergencias en Venezuela' [Video surveillance and emergency response systems in Venezuela], *Transparencia Venezuela*, January 2022, [online](#).
- 60 Puyosa & Azpúrua, 'Watch the watchers: surveillance technologies for political control in Venezuela'.
- 61 'Venezuela: Freedom on the Net 2025 Country Report', Freedom House, 2025, [online](#).
- 62 Department of the Treasury, 'Treasury sanctions CEIEC for supporting the illegitimate Maduro regime's efforts to undermine Venezuelan democracy'.
- 63 Ángela Alarcón, 'Venezuela's many means of surveillance and control', *Access Now*, 29 August 2024, [online](#); Department of the Treasury, 'Treasury sanctions CEIEC for supporting the illegitimate Maduro regime's efforts to undermine Venezuelan democracy'.
- 64 'Maduro must #KeepItOn in times of protest and unrest', *Access Now*, 27 August 2024, updated 3 September 2024, [online](#); 'Venezuela: Freedom on the Net 2025 Country Report', Freedom House, 2025, [online](#).
- 65 Department of the Treasury, 'Treasury sanctions CEIEC for supporting the illegitimate Maduro regime's efforts to undermine Venezuelan democracy'.
- 66 Angus Berwick, 'Service? Don't rely on Venezuela's state telecoms firm CANTV', *Reuters*, 22 November 2018, [online](#); Erin Horrigan et al., 'China's growing 5G presence in South America poses potential security threats to the region', *Tearline*, 8 May 2023, [online](#); Carlos M Baldo et al., 'Huawei in Venezuela: a review of 2006–2019', *Revista de Gestão*, 2021, 28(4):358–375, [online](#).
- 67 Josh Chin, Liza Lin, *Surveillance state: inside China's quest to launch a new era of social control*, Macmillan, 2022, [online](#).
- 68 'Han Zheng meets with Venezuelan Vice President Delcy Eoina Rodriguez Gomez', Embassy of the PRC in the Islamic Republic of Iran, 5 December 2024, [online](#).
- 69 Yorman Gámez, 'Venezuela y China profundizan cooperación estratégica con firma de acuerdos clave en la Expo China–Venezuela' [Venezuela and China deepen strategic cooperation with the signing of key agreements at the China–Venezuela Expo], Ministerio del Poder Popular para Relaciones Exteriores [Ministry of People's Power for Foreign Affairs], 4 July 2025, [online](#).
- 70 Rod J Rosenstein, Jesús A Dávila, Ronald Evans et al., 'Doing business in Venezuela: what companies need to know', *Sanctions News*, 4 March 2026, [online](#).
- 71 Bethany Allen, Nathan Attrill, Fergus Ryan, 'China's plan to scale its way to AI dominance', *ASPI*, Canberra, 18 March 2026, [online](#).
- 72 Fergus Ryan, Bethany Allen, Shelly Shih et al., *The party's AI: How China's new AI systems are reshaping human rights*, *ASPI*, Canberra, December 2025, [online](#).
- 73 'China's voice recognition champion iFlytek gets US\$407 million', *South China Morning Post*, 17 July 2019, [online](#); 'iFlytek', *Beijing Review*, July 2025, [online](#); 'About us', iFlytek, [online](#).
- 74 'China: voice biometric collection threatens privacy', *HRW*, 22 October 2017, [online](#); 'Police officers identified suspects by listening to their voices despite lack of evidence; voice technology has solved more than 20 cases in three years', *iFeng Anhui*, 9 December 2015, [online](#).
- 75 'iFLYTEK showcases multi-scene AI applications at GITEX Global 2024, powering AI development in the Middle East', iFLYTEK, 24 October 2024, [online](#); 'iFLYTEK consumer-end products available in Malaysia, further solidifying its presence in Southeast Asia', iFLYTEK, 7 May 2024, [online](#).
- 76 Bureau of Industry and Security, 'Addition of certain entities to the Entity List', Department of Commerce, US Government, *Federal Register*, 9 October 2019, [online](#).
- 77 'Content moderation solution: digital content risk control' [内容审核解决方案 数字内容风控], *iFlytek Open Platform*, no date, [online](#).
- 78 'iFlytek developing AI-enabled system for legal purposes', Supreme People's Court of the People's Republic of China, 7 March 2018, [online](#).
- 79 Ryan et al., *The party's AI: How China's new AI systems are reshaping human rights*.
- 80 'Achievements and prospects of artificial intelligence judicature in China', Scientific Research Publishing, 28 September 2022, [online](#); 'China's e-justice revolution', *Judicature*, Duke University School of Law, 2021, 105(1), [online](#).
- 81 Ryan et al., *The party's AI: How China's new AI systems are reshaping human rights*.
- 82 'iFlytek helps build Anhui Procuratorate's AI-assisted case-handling system', *iFlytek Education* [科大讯飞教育], 8 April 2025, [online](#).
- 83 Ryan et al., *The party's AI: How China's new AI systems are reshaping human rights*.
- 84 'AI giant iFlytek to invest HK\$400 million in Hong Kong, opens international headquarters', *South China Morning Post*, 5 July 2024, [online](#); 'Contact', iFlytek Middle East, [online](#).
- 85 'Smart Translator: FAQ', iFlytek, [online](#).
- 86 'China's AI powers ASEAN expo: iFlytek leads push for smarter connectivity', *Manila Times*, 25 September 2025, [online](#).
- 87 UN General Assembly, 'International Covenant on Civil and Political Rights', adopted 16 December 1966, entered into force 23 March 1976, United Nations, [online](#).
- 88 La Noticia VTV, 'Pdte. Maduro da inicio a la 2T productiva con la inspección del teleférico Macuto-Warairarepano' [President Maduro kicks off the 'Productive 2T' phase by inspecting the Macuto-Warairarepano cable car], *YouTube*, at 48:23, 27 January 2025, [online](#).
- 89 Gabriela Jiménez Ramírez, 'Guerra cognitiva: la conquista del silencio interior' [Cognitive warfare: the conquest of inner silence], Ministerio del Poder Popular para Ciencia y Tecnología [Ministry of People's Power for Science and Technology], 16 January 2026, [online](#).
- 90 Ministry of Foreign Affairs, '中华人民共和国和委内瑞拉玻利瓦尔共和国关于建立全天候战略合作伙伴关系的联合声明 (全文)' [Joint statement between the People's Republic of China and the Bolivarian Republic of Venezuela on establishing an all-weather strategic partnership], PRC Government, 14 September 2023, [online](#); 'Xi, Maduro announce elevation

- of China-Venezuela ties', *Xinhua*, 14 September 2023, [online](#); 'Venezuela y China firman 31 nuevos acuerdos para elevar cooperación bilateral a toda prueba' ['Venezuela and China sign 31 new agreements to elevate bilateral cooperation to an all-weather level'], Fondo Nacional de Ciencia, Tecnología e Innovación [National Fund for Science, Technology and Innovation], 14 September 2023, [online](#); 'EN CLAVES | China y Venezuela suscriben instrumentos de cooperación en el contexto de la XVII CMAN' ['Key points | China and Venezuela sign cooperation instruments in the context of the 17th High-Level Joint Commission'], Ministerio del Poder Popular de Economía y Finanzas [Ministry of People's Power for Economy and Finance], 13 September 2023, [online](#); 'Venezuela y China firman acuerdo de Big Data para el uso intensivo de la percepción remota' ['Venezuela and China sign Big Data agreement for the intensive use of remote sensing'], Fondo Nacional de Ciencia, Tecnología e Innovación [National Fund for Science, Technology and Innovation], 8 September 2023, [online](#); '中央广播电视总台与委内瑞拉新闻通讯部签署合作备忘录' ['China Media Group and Venezuela's Ministry of Communication and Information sign cooperation memorandum'], CCTV, 13 September 2023, [online](#).
- 91 'Presidente Maduro: 17^o Comisión Mixta China-Venezuela ha sido la mejor para afianzar cooperación' [President Maduro: 17th China-Venezuela Joint Commission has been the best for strengthening cooperation], Ministerio del Poder Popular del Despacho de la Presidencia y Seguimiento de la Gestión de Gobierno [Ministry of the People's Power for the Office of the Presidency and Government Management Monitoring], 13 September 2023, [online](#).
- 92 'Ministra Gabriela Jiménez Ramírez destaca eficiencia del Centro Experimental de Inteligencia Artificial en China' [Minister Gabriela Jiménez Ramírez highlights the efficiency of the Experimental Centre for Artificial Intelligence in China], FONACIT, 12 September 2023, [online](#).
- 93 'Venezuela y China firman memorándum de entendimiento para desarrollo de proyectos conjuntos en parques científicos tecnológicos' ['Venezuela and China sign memorandum of understanding to develop joint projects in science and technology parks'], ONCTI, 28 April 2024, [online](#).
- 94 'Ley Aprobatoria del "Acuerdo entre el Gobierno de la República Bolivariana de Venezuela y el Gobierno de la República Popular China relativo a la Promoción y Protección de Inversiones"' [Law approving the "Agreement between the Government of the Bolivarian Republic of Venezuela and the Government of the People's Republic of China on the Promotion and Protection of Investments"], no. 6,852 Extraordinary, *Gaceta Oficial de la República Bolivariana de Venezuela*, 13 November 2024, [online](#); 'Texto íntegro de la Declaración Conjunta entre la República Popular China y la República Bolivariana de Venezuela' ['Full text of the joint declaration between the People's Republic of China and the Bolivarian Republic of Venezuela'], *Xinhua*, 13 September 2023, [online](#).
- 95 'AN aprueba en primera discusión Proyecto de Ley de Inteligencia Artificial' ['National Assembly approves Artificial Intelligence Bill in first reading'], Asamblea Nacional de la República Bolivariana de Venezuela [National Assembly of the Bolivarian Republic of Venezuela], 19 November 2024, [online](#).
- 96 'Punished for seeking change: killings, enforced disappearances and arbitrary detention following Venezuela's 2024 election', *HRW*, 30 April 2025, [online](#).
- 97 Andreína Chávez Alava, 'Venezuelan VP travels to China to strengthen "all-weather strategic partnership"', *Venezuelanalysis*, 5 December 2024, [online](#).
- 98 Ministry of Foreign Affairs, 'Han Zheng meets with Venezuelan Vice President Delcy Eoloína Rodríguez Gomez', PRC Government, 5 December 2024, [online](#).
- 99 'Presidente Maduro prioriza la eliminación de zonas sin conectividad a las telecomunicaciones' ['President Maduro prioritises eliminating areas without telecommunications connectivity'], Comisión Nacional de Telecomunicaciones [National Telecommunications Commission], 9 April 2025, [online](#); 'Presidente Maduro activa los motores de Telecomunicaciones y Nuevas Tecnologías' ['President Maduro activates the Telecommunications and New Technologies engines'], *Correo del Orinoco*, 8 April 2025, [online](#).
- 100 'Vicepresidenta Delcy Rodríguez visitó la empresa iFlytek para explorar áreas de cooperación en materia de inteligencia artificial' ['Vice President Delcy Rodríguez visited iFlytek to explore areas of cooperation on artificial intelligence'], Ministerio del Poder Popular de Hidrocarburos [Ministry of People's Power for Hydrocarbons], 26 April 2025, [online \(archived\)](#).
- 101 'Científicos venezolanos viajarán a China para formarse en materia de Inteligencia Artificial' ['Venezuelan scientists will travel to China to train in artificial intelligence'], Ministerio del Poder Popular para Ciencia y Tecnología [Ministry of People's Power for Science and Technology], 30 May 2025, [online](#).
- 102 '蓝虎大使会见委内瑞拉科技部长希门尼斯' ['Ambassador Lan Hu meets Venezuelan Science and Technology Minister Jiménez'], Embassy of the People's Republic of China in the Bolivarian Republic of Venezuela, 19 June 2025, [online](#).
- 103 'Venezuela y China dan un nuevo paso significativo en tecnología y cooperación estratégica' ['Venezuela and China take a significant new step in technology and strategic cooperation'], *Radio Nacional de Venezuela*, 4 July 2025, [online \(archived\)](#).
- 104 Gámez, 'Venezuela y China profundizan cooperación estratégica con firma de acuerdos clave en la Expo China-Venezuela' [Venezuela and China deepen strategic cooperation with the signing of key agreements at the China-Venezuela Expo]; 'Venezuela and China take a significant new step in technology and strategic cooperation', *Radio Nacional de Venezuela*, 7 July 2025, [online](#).
- 105 'Venezuela firma un memorando de entendimiento con empresa china para el desarrollo de IA' [Venezuela signs a memorandum of understanding with a Chinese company for AI development], *EFE*, republished by *SWI swissinfo.ch*, 5 July 2025, [online](#).
- 106 '驻委内瑞拉大使蓝虎会见委油气部副部长希尔' [Ambassador Lan Hu meets Venezuelan Vice Minister of Oil and Gas Hill], Embassy of the People's Republic of China in the Bolivarian Republic of Venezuela, 6 August 2025, [online](#).
- 107 Ministry of Foreign Affairs, 'Signing ceremony of the Agreement on the Establishment of the World Artificial Intelligence Cooperation Organization held in Shanghai', PRC Government, 16 July 2026, [online](#); Ministry of Communication and Digital Affairs, 'Indonesia Perkuat Peran dalam Tata Kelola AI Global Bersama 29 Negara Pendiir World Artificial Intelligence Cooperation Organization (WAICO)' [Indonesia strengthens its role in global AI governance alongside 29 founding nations of the World Artificial Intelligence Cooperation Organization (WAICO)], Indonesian Government, 17 July 2026, [online](#).
- 108 'Venezuela participa en encuentro global sobre inteligencia artificial' [Venezuela participates in a global meeting on artificial intelligence], *Ciudad CCS*, 17 July 2026, [online](#); 'Ciudad CCS', *Gaceta Oficial de la República Bolivariana de Venezuela*, 10 July 2026, no. 43,413, [online](#).
- 109 'Agreement on the Establishment of the World Artificial Intelligence Cooperation Organization', *Geneva Internet Platform*, July 2026, [online](#).
- 110 Laurie Chen, Casey Hall, Eduardo Baptista, 'Xi pitches China as leader of new global AI order, challenging US dominance', *Reuters*, 17 July 2026, [online](#); Ministry of Foreign Affairs, '2026 World Artificial Intelligence Conference and High-Level Meeting on Global AI Governance Chair's statement', PRC Government, 17 July 2026, [online](#).
- 111 'Venezuela y China refuerzan cooperación en materia de inteligencia artificial' [Venezuela and China strengthen cooperation in artificial intelligence], *Diario Primicia / Prensa Mincyt*, 2025, [online](#).
- 112 Berwick, 'Special report: How ZTE helps Venezuela create China-style social control'.
- 113 'Instalarán 5.334 salas de autogobierno, una en cada Comuna o Circuito Comunal' [5,334 self-governance chambers will be installed—one in each commune or communal circuit], Ministerio del Poder Popular para las Comunas y los Movimientos Sociales [Ministry of People's Power for Communes and Social Movements], 27 January 2025, [online](#).
- 114 David Brunnstrom, 'Who's really running Venezuela?', *Reuters*, 13 January 2026, [online](#); Erin Banco, Jonathan Landay, Matt Spetalnick, 'US intelligence raises doubts about Venezuela leader's cooperation', *Reuters*, 28 January 2026, [online](#); Marianna Parraga, 'Sweeping oil reform in Venezuela approved, operators expected to gain autonomy', *Reuters*, 29 January 2026, [online](#).
- 115 Gabriela Jiménez-Ramírez, 'Desafíos de una comunicación para la vida en la era digital' [Challenges of communication for life in the digital age], in Nerlín Caruci (ed.), *La guerra cognitiva en la agonía digital 4.0: Sentidos y horizontes de la comunicación comunal en el tránsito hacia una humanidad nueva* [Cognitive warfare in the digital 4.0 death throes: meanings and horizons of communal communication in the transition towards a new humanity] (13–28), Fondo Editorial Mincyt, 2025, [online](#).
- 116 Pedro Penso, 'La confrontación en zona gris [Grey-zone confrontation]', and Róger Garcés, 'Naturaleza, dimensiones y modos de la guerra cognitiva [Nature, dimensions, and modes of cognitive warfare]', in Nerlín Caruci (ed.), *La guerra cognitiva en la agonía digital 4.0: Sentidos y horizontes de la comunicación comunal en el tránsito hacia una humanidad nueva* (79–92 and 95–107, especially 82, 99–100 and 102–106), Fondo Editorial Mincyt, 2025.

- 117 Carolina Escarrá Gil, 'Comunicación y pedagogía de una reforma constitucional para la nueva época' [Communication and pedagogy regarding a constitutional reform for the new era], in Nerlín Carucí (ed.), *La guerra cognitiva en la agonía digital 4.0: Sentidos y horizontes de la comunicación comunal en el tránsito hacia una humanidad nueva* (179–207, especially 204–205), Fondo Editorial Mincyt, 2025; Ley Orgánica del Plan de la Patria de las 7 Grandes Transformaciones 2025–2031 [Organic Law of the Homeland Plan of the Seven Great Transformations 2025–2031], Gaceta Oficial de la República Bolivariana de Venezuela, no. 6,907 Extraordinario, 24 May 2025, 198–199, [online](#).
- 118 Penso, 'La confrontación en zona gris'; Garcés, 'Naturaleza, dimensiones y modos de la guerra cognitiva'.
- 119 Gabriela Jiménez Ramírez, 'Guerra cognitiva: la conquista del silencio interior', *La Inventadera*, 17 January 2026, [online](#).
- 120 Deivis Benítez, 'Venezuela y China sellan alianza tecnológica para el impulso de la inteligencia artificial' [Venezuela and China seal a technological alliance to promote artificial intelligence], *Correo del Orinoco*, 5 July 2025, [online](#).
- 121 Marelvis González, 'Alianza tecnológica entre Venezuela y China impulsa IA' [Technology alliance between Venezuela and China boosts AI], *Radio Miraflores*, 4 July 2025, [online](#); '中-委博览会期间签署"美好未来"的协议+《视频》' [Agreement on a 'bright future' signed during the China–Venezuela Expo + video], Venezuelan Youth Federation, 6 July 2025, [online](#).
- 122 'Delcy Rodríguez crea Viceministerio de IA e inaugura centro tecnológico petrolero' [Delcy Rodríguez creates AI Vice-Ministry and inaugurates oil technology centre], *Correo del Caroní*, 30 May 2026, [online](#); 'CAR1: Caracas – Ciron Data Center', *Ciron*, no date, [online](#).
- 123 'Government AI Readiness Index 2025', *Oxford Insights*, 2025, [online](#); Henry Chirinos, 'Rationing: nightmare of a Venezuela desperate to recover its power grid', *EFE*, 9 May 2026, [online](#); Alison J Stafford Powell, Janet K Kim, Lise S Test, Rob O'Brien, 'BIS revises license review policy for advanced computing commodities (AI semiconductors) to China and Macau when exported from the United States', *Sanctions News*, 28 January 2026, [online](#).
- 124 Chirinos, 'Rationing: nightmare of a Venezuela desperate to recover its power grid'; A Gustavo Hernández, 'Delcy's fragile reopening meets the old power crisis', *Caracas Chronicles*, 15 May 2026, [online](#); James O'Donnell, Casey Crownhart, 'We did the math on AI's energy footprint. Here's the story you haven't heard', *MIT Technology Review*, 20 May 2025, [online](#).
- 125 '智慧养殖解决方案' [Smart farming solutions], *Xfyun.cn*, no date, [online](#).
- 126 'Huawei Cloud: the first choice of multicloud provider for LATAM Enterprises to stay ahead in time', *Huawei Cloud*, 19 March 2026, [online](#).
- 127 'Regions and locations of data centers', *Huawei Cloud*, no date, [online](#); 'Global products and services', *Huawei Cloud*, no date, [online](#).
- 128 'iFLYTEK All-in-One server', iFLYTEK, no date, [online](#).
- 129 'All-in-One server', *Xfyun.cn*, no date, [online](#); iFLYTEK, 'In today's fast-moving AI era, every company is asking how to use large models faster, safer, and more private. The iFLYTEK All-in-One AI solution provides the answer', *Facebook*, 16 October 2026, [online](#); iFLYTEK, 'iFLYTEK showcases all-in-one AI solutions at MWC26, bringing private, customizable AI to industry', *Global Newswire*, 5 March 2026, [online](#).
- 130 Alex Colville, 'China's global AI firewall', *China Media Project*, 12 June 2025, [online](#).
- 131 Kevin Schaul, 'See the hidden rules behind AI. Then use them to rewrite this article', *Washington Post*, 11 May 2026, [online](#).
- 132 Alex Colville, Yang Mengli, Jordyn Haime, David Bandurski, *Guided intelligence: China's AI Strategy and the global information space*, Psychological Defence Agency, 2026, [online](#).
- 133 'iFLYTEK', *Sina*, 2026, [online](#); lvdong@guancha.cn, '坚持用华为算力训练·讯飞有困难也有优势' [Insisting on using Huawei's computing power for training presents both challenges and advantages for iFlytek], *Guancha*, 1 May 2026, [online](#).
- 134 lvdong@guancha.cn, '坚持用华为算力训练·讯飞有困难也有优势' [Insisting on using Huawei's computing power for training presents both challenges and advantages for iFlytek].
- 135 Clavel Rangel, Sam Jones, "'Tonnes of rubble': 58,000 buildings estimated destroyed in Venezuela earthquakes", *The Guardian*, 1 July 2026, [online](#).
- 136 'Ministro Márquez asume la conducción de la Sala Nacional de Autogobierno Popular' [Minister Márquez assumes leadership of the National Chamber of Popular Self-Government], Ministerio del Poder Popular para la Energía Eléctrica [Ministry of People's Power for Electric Energy], 27 January 2025, [online](#); 'Instalarán 5.334 salas de autogobierno, una en cada Comuna o Circuito Comunal' [5,334 self-governance chambers will be installed—one in each commune or communal circuit], Ministerio del Poder Popular para las Comunas, Movimientos Sociales y Agricultura Urbana [Ministry of People's Power for Communes, Social Movements and Urban Agriculture], 27 January 2025, [online](#); 'Venezuela instalará Sala de Autogobierno Popular con IA' [Venezuela to set up a Popular Self-Government Centre with AI], *Ciudad CCS*, 28 January 2025, [online](#).
- 137 'Instalarán 5.334 salas de autogobierno, una en cada Comuna o Circuito Comunal' [5,334 self-governance chambers will be installed—one in each commune or communal circuit], Ministerio del Poder Popular para las Comunas, Movimientos Sociales y Agricultura Urbana [Ministry of People's Power for Communes, Social Movements, and Urban Agriculture]; '1 x 10 del buen gobierno' [1x10 of good governance], Oficina de Prensa Presidencial [Presidential Press Office], May 2022, [online](#); 'Sistema 1x10 del Buen Gobierno' [1x10 Good Governance System], [online](#); 'Registra la información de la comunidad donde resides' [Record the information about the community where you reside], *Sistema Patria*, 8 June 2023, [online](#).
- 138 '1 x 10 del Buen Gobierno', Oficina de Prensa Presidencial, May 2022, [online](#).
- 139 '36 mil proyectos postulados por las comunidades están inscritos ante el CNE' [36,000 projects nominated by communities are registered with the CNE], Prensa Presidencial [Presidential Press Office], 27 January 2025, [online](#); 'Presidente Maduro lanza revolucionario método del 1x10 para gobernar con el Poder Popular' [President Maduro launches revolutionary 1x10 method to govern with people's power], Ministerio del Poder Popular para las Comunas, Movimientos Sociales y Agricultura Urbana [Ministry of People's Power for Communes, Social Movements and Urban Agriculture], 20 May 2022, [online](#).
- 140 'Gobierno Bolivariano crea Guía de Instalación y Funcionamiento de la Sala Nacional del Sistema de Gobierno Popular' [Bolivarian Government creates installation and operating guide for the National Room of the Popular Government System], Prensa Presidencial [Presidential Press Office], 20 February 2025, [online](#); 'Sala del Sistema del Gobierno Popular: Guía de Instalación y Funcionamiento Salas de Autogobierno' [Room of the Popular Government System: installation and operating guide for self-government rooms], *Gobierno Comunal / Plan Patria*, 2025, [online](#); Ley Orgánica del Plan de la Patria de las 7 Grandes Transformaciones 2025–2031 [Organic Law of the Homeland Plan of the Seven Great Transformations 2025–2031], *Gaceta Oficial de la República Bolivariana de Venezuela*, no. 6,907 Extraordinario, 24 May 2025.
- 141 'Gobierno Bolivariano activa la Sala Nacional del Sistema de Gobierno Popular' [Bolivarian Government activates the National Room of the Popular Government System], Ministerio del Poder Popular para las Comunas, Movimientos Sociales y Agricultura Urbana [Ministry of People's Power for Communes, Social Movements and Urban Agriculture], 7 February 2025, [online](#).
- 142 'Gobierno Bolivariano crea Guía de Instalación y Funcionamiento de la Sala Nacional del Sistema de Gobierno Popular' [Bolivarian Government creates installation and operating guide for the National Room of the Popular Government System], Prensa Presidencial [Presidential Press Office], 20 February 2025, [online](#).
- 143 'Salas de Autogobierno Comunal deben estar consolidadas en 30 días' [Communal self-government rooms must be consolidated within 30 days], Prensa Presidencial [Presidential Press Office], 27 April 2025, [online](#); 'Salas de Autogobierno y Justicia Comunal de Guayaquiro recibieron dotación' [Self-government and communal justice rooms in Guayaquiro received equipment], Ministerio del Poder Popular para las Comunas, Movimientos Sociales y Agricultura Urbana [Ministry of People's Power for Communes, Social Movements and Urban Agriculture], 22 April 2025, [online](#).
- 144 'Vicepresidenta Delcy Rodríguez: Más del 94% de los Circuitos Comunales cuentan con Salas de Autogobierno Popular' [Vice President Delcy Rodríguez: more than 94% of communal circuits have popular self-government rooms], Sistema de Gobierno Popular y Comunal [Popular and Communal System of Government], 27 June 2025, [online](#); '100% de instalación de Salas de Autogobierno y entrega de equipos telefónicos en La Guaira' [100% installation of self-government rooms and delivery of telephone equipment in La Guaira], Ministerio del Poder Popular para las Comunas, Movimientos Sociales y Agricultura Urbana [Ministry of People's Power for Communes, Social Movements and Urban Agriculture], 28 June 2025, [online](#).
- 145 'Maduro en inauguración de sala de autogobierno comunal' [Maduro at inauguration of communal self-government room], *YouTube*, 20 October

- 2025, [online](#); 'Gobierno anuncia nuevo Sistema de Consulta al entregar más de 20 mil obras comunitarias' [Government announces new consultation system while delivering more than 20,000 community works], *Globovisión*, 20 October 2025, [online](#).
- 146 'El 1x10 del Buen Gobierno ha solucionado el 88,07% de los reportes recibidos a través de la VenApp' [The 1x10 Good Government system has resolved 88.07% of reports received through VenApp], *Mazo4F*, 4 December 2025, [online](#).
- 147 'Maduro en la Sala de autogobierno comunal Simón Rodríguez' [Maduro in the Simón Rodríguez communal self-government room], presidential broadcast, *YouTube*, 18 September 2025, [online](#); 'Ministro Prado: Las salas de Autogobierno deben confluír todas las instancias de las comunas' [Minister Prado: all commune bodies should come together in the self-government rooms], *Venezolana de Televisión*, 8 December 2025, [online](#); 'Crean guía para instalar salas de autogobierno comunal en Venezuela' [Guide created for installing communal self-government rooms in Venezuela], *Extra News Mundo*, 26 March 2025, [online](#).
- 148 'Venezuela: country focus', European Union Agency for Asylum, November 2023, [online](#); Iria Puyosa, Andrés Azpúrua, *Venezuela: a playbook for digital repression*, Atlantic Council / DFRLab, July 2024, [online](#); 'patria.org.ve', *WHOIS*, accessed 12 June 2026, [online](#).
- 149 *Manual de Usuario para la Aplicación Comunas-SEGEN* [User manual for the Comunas-SEGEN application], Sistema de Gobierno Popular y Comunal [Popular and Communal Government System], 2026, [online](#); 'Venezuela avanza en la construcción de un sistema de información sobre riesgos comunitarios' [Venezuela advances in building a community-risk information system], *Ciudad Valencia*, 12 March 2026, [online](#).
- 150 *The digital communal State: operational infrastructure and technical rollout of the Salas de Autogobierno Popular in Venezuela*, commissioned technical assessment, 2026, on file with the author; Department of the Treasury, 'Treasury sanctions CEIEC for supporting the illegitimate Maduro regime's efforts to undermine democracy in Venezuela'; 'Service? Don't rely on Venezuela's state telecoms firm CANTV', *Reuters*, 22 November 2018, [online](#).
- 151 VE sin Filtro and DFRLab, 'Watch the watchers: surveillance technologies for political control in Venezuela', 26 March 2026, [online](#); 'Diosdado Cabello afirma que ahora "hay cámaras por todos lados": "Pórtense bien, los están viendo"' [Diosdado Cabello says there are now 'cameras everywhere': "Behave yourselves, they are watching you"], *Contrapunto*, 17 July 2025, [online](#); 'Venezuela fortalece seguridad ciudadana con más de siete mil cámaras del VEN 911' [Venezuela strengthens citizen security with more than 7,000 VEN911 cameras], *Venezolana de Televisión*, 5 December 2025, [online](#).
- 152 '1 x 10 del Buen Gobierno' [1x10 Good Government], Oficina de Prensa Presidencial [Presidential Press Office], May 2022, [online](#); 'Gobierno Bolivariano activa la Sala Nacional del Sistema de Gobierno Popular' [Bolivarian Government activates the National Room of the Popular Government System], Ministerio del Poder Popular para las Comunas, Movimientos Sociales y Agricultura Urbana [Ministry of People's Power for Communes, Social Movements and Urban Agriculture], 7 February 2025, [online](#); *Manual de Usuario para la Aplicación Comunas-SEGEN* [User manual for the Comunas-SEGEN application], Sistema de Gobierno Popular y Comunal [Popular and Communal Government System], 2026, [online](#); European Union Agency for Asylum, 'Venezuela: country focus'; 'Salas de Autogobierno se encuentran desplegadas en 5.336 comunas y circuitos comunales' [Self-government rooms are deployed in 5,336 communes and communal circuits], *Radio Nacional de Venezuela*, 10 March 2026, [online](#).
- 153 'Instalarán 5.334 salas de autogobierno, una en cada Comuna o Circuito Comunal' [5,334 self-government rooms will be installed, one in each commune or communal circuit], Ministerio del Poder Popular para las Comunas, Movimientos Sociales y Agricultura Urbana [Ministry of People's Power for Communes, Social Movements and Urban Agriculture], 27 January 2025, [online](#); 'Gobierno Bolivariano activa la Sala Nacional del Sistema de Gobierno Popular' [Bolivarian Government activates the National Room of the Popular Government System], Ministerio del Poder Popular para las Comunas, Movimientos Sociales y Agricultura Urbana [Ministry of People's Power for Communes, Social Movements and Urban Agriculture], 7 February 2025, [online](#); 'Sala del Sistema del Gobierno Popular: Guía de Instalación y Funcionamiento Salas de Autogobierno' [Room of the Popular Government System: installation and operating guide for self-government rooms], Gobierno Comunal / Plan Patria [Communal Government / Homeland Plan], 2025, [online](#).
- 154 Milagros Socorro, 'Una bóveda de cristal: la reingeniería del control civil en Venezuela' [A glass vault: the re-engineering of civil control in Venezuela], *La Gran Aldea*, 26 December 2025, [online](#).
- 155 'Gobierno Bolivariano activa la Sala Nacional del Sistema de Gobierno Popular' [Bolivarian Government activates the National Room of the Popular Government System], Ministerio del Poder Popular para las Comunas, Movimientos Sociales y Agricultura Urbana [Ministry of People's Power for Communes, Social Movements and Urban Agriculture], 7 February 2025, [online](#).
- 156 UN General Assembly, 'International Covenant on Civil and Political Rights', adopted 16 December 1966, entered into force 23 March 1976, United Nations, [online](#).
- 157 科大讯飞开放平台, '声纹识别' ['Voiceprint recognition'], no date, [online](#); 科大讯飞开放平台, '声纹识别 API 文档' ['Voiceprint recognition API documentation'], no date, [online](#).
- 158 'China: voice biometric collection threatens privacy', *HRW*, 22 October 2017, [online](#); Alexandra Harney, 'Risky partner: top US universities took funds from Chinese firm tied to Xinjiang security', *Reuters*, 13 June 2019, [online](#); Bureau of Industry and Security, 'Addition of certain entities to the Entity List', Department of Commerce, US Government, *Federal Register*, 84(196), 9 October 2019, [online](#).
- 159 'Punished for seeking change: killings, enforced disappearances and arbitrary detention following Venezuela's 2024 election', *HRW*, 30 April 2025, [online](#).
- 160 Gabriela Jiménez Ramírez, 'Guerra cognitiva: la conquista del silencio interior' [Cognitive warfare: the conquest of inner silence], Ministerio del Poder Popular para Ciencia y Tecnología [Ministry of the People's Power for Science and Technology], 16 January 2026, [online](#).
- 161 Zhong Nan, 'China sets up new bureau for overseas State assets', *China Daily*, 8 April 2026, [online](#).

Acronyms and abbreviations

AI	artificial intelligence
CANTV	<i>Compañía Anónima Nacional Teléfonos de Venezuela</i> (National Telephone Company of Venezuela)
CCP	Chinese Communist Party
CCTV	closed-circuit television
CLAP	Local Committees for Supply and Production
CONATEL	<i>Comisión Nacional de Telecomunicaciones</i>
CPU	central processing unit
DGCIM	<i>Dirección General de Contrainteligencia Militar</i> (General Directorate of Military Counterintelligence)
FAES	Fuerzas de Acciones Especiales de la Policía Nacional Bolivariana (Special Action Forces of the Bolivarian National Police)
GPU	graphics processing unit
LLM	large language model
MoU	memorandum of understanding
PSUV	<i>Partido Socialista Unido de Venezuela</i> (United Socialist Party of Venezuela)
SEBIN	<i>Servicio Bolivariano de Inteligencia Nacional</i> (Bolivarian National Intelligence Service)
SIMA	<i>Sistema Integrado de Monitoreo y Asistencia</i> (Integrated Monitoring and Assistance System)
UN	United Nations



25
YEARS
2001–2026