TECH POLICY BRIEF

Watch the Watchers: Surveillance technologies for political control in Venezuela

Andrés Azpúrua · Iria Puyosa

VE SIN FILTRO

DFRLab

VE SIN FILTRO

CONEXIÓN SEGURA Y LIBRE

About VE sin Filtro / Conexión Segura y Libre

VE sin Filtro is a program dedicated to monitoring and documenting threats to the exercise of human rights in the digital environment in Venezuela, created by the digital human rights organization Conexión Segura y Libre (Free and Secure Online). Since 2014 it has helped identify and circumvent media censorship and has pioneered the joint use of automated network measurements, volunteer-contributed tests, and network traffic analysis to document Internet censorship. VE sin Filtro has used open-source investigations to examine restrictions on human rights online to attribute state-sponsored digital attacks in Venezuela. With technical evidence and data analysis, it exposes and documents the extent of Internet blocking and censorship, indiscriminate government surveillance and cyber-attacks against civil society. Conexión Segura y Libre offers emergency assistance to civil society organizations, journalists and independent media under attack or recently blocked; helping to resolve the incident and mitigating the impact of censorship; and provides support and training to activists, journalists and organizations, and develops recommendations and best practices to counter threats to their rights and safety.

Atlantic Council
TECHNOLOGY PROGRAMS

DFRLab

About the Digital Forensic Research Lab

The Digital Forensic Research Lab (DFRLab) at the Atlantic Council is a first of its kind organization with technical and policy expertise on disinformation, connective technologies, democracy, and the future of digital rights. Incubated at the Atlantic Council in 2016, the DFRLab is a field-builder, studying, defining, and informing approaches to the global information ecosystem and the technology that underpins it.

Authors

Andrés Azpúrua, executive director, Conexión Segura

Iria Puyosa, resident senior fellow at the Atlantic Council's Democracy + Tech Initiative

Contributors

Daniela Alvarado Mejías, investigative journalist

Carlos Guerra, technical advisor on information security

Marco Antonio Ruiz, communications coordinator, Conexión Segura

Valentina Aguana, technical project coordinator, Conexión Segura

Version 1.0 - Public Release

Cover: An image of the late Venezuelan President Hugo Chávez is seen on monitor screens at the headquarters of the "Integrated Monitoring and Support System" (SIMA) in Caracas, December 11, 2013. REUTERS/Carlos Garcia Rawlins

© 2026 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

March 2026

Table of contents

Executive summary

This report provides a detailed analysis of the surveillance technologies used in Venezuela for social and political control under Nicolás Maduro's regime and continuing under Acting President Delcy Rodríguez following Maduro's removal by US forces on January 3, 2026. Despite the change in leadership, Venezuela's extensive surveillance infrastructure—including video monitoring systems, telecommunications interception, cyberpatrolling, state-sponsored digital applications, device searches and seizures, drone surveillance, and cyberattacks—remains fully operational. This report documents how this surveillance apparatus, which costs over $1 billion, enables comprehensive authoritarian control mechanisms that facilitate systematic political repression over a population of around twenty-seven million individuals.

Key findings

- **Video surveillance infrastructure:** Venezuela's CCTV infrastructure has been systematically weaponized for political control rather than public safety. Chinese vendors—particularly CEIEC, Hikvision, and Dahua—dominate the supply chain despite international sanctions. Advanced facial recognition and license plate detection capabilities enhanced by artificial intelligence operate without privacy protections, judicial oversight, or mechanisms for citizen consent. The VEN911 emergency response system integrates extensive camera networks, enabling rapid identification and targeting of dissidents, protesters, and political opponents. The co-opting of opposition-controlled municipal systems demonstrates how ostensibly independent security infrastructure is compromised for surveillance.
- **Drone surveillance and movement monitoring:** Venezuelan security forces deploy sophisticated drone capabilities combining advanced technical systems with psychological warfare tactics. Commercial drones, ranging from compact consumer DJI models to advanced Autel models with extended surveillance capabilities, operate without legal frameworks governing their deployment or oversight. The deliberate visibility of drone operations—particularly nighttime flights over protest zones and residences of opposition figures—serves dual purposes: gathering intelligence on movement patterns while creating pervasive chilling effects on political assembly. GPS tracking devices discovered in vehicles of political prisoners' families, equipped with listening capabilities, reveal covert surveillance layers providing continuous location data and environmental audio.
- **State-sponsored digital applications:** The Patria ("Homeland") System represents the platformization of citizen control, transforming social welfare delivery into an instrument for systematic data extraction and political manipulation. The Patria database enables comprehensive identification and large-scale data collection, with the platform's domain registered to PSUV (Venezuela's ruling party) rather than to any state agency, demonstrating operational fusion between the state apparatus and the party structure. Access to welfare benefits is conditioned on mandatory registration and the continuous provision of personal information. The system's technical design allows mapping users' relationships with other people and institutions, enabling administrators to create detailed connection networks even for non-users. Meanwhile, VenApp is explicitly being used to facilitate the systematic snitching of anti-government activities.
- **Cyberpatrolling and social media surveillance:** Systematic cyberpatrolling across social media platforms and messaging applications, coordinated by the political and military intelligence agencies SEBIN and DGCIM, has evolved into a comprehensive machine of digital persecution that criminalizes online expression. Operation Knock Knock in 2024 exemplified the integration of multiple surveillance streams—VenApp reporting features, Telegram doxxing groups, Instagram terror campaigns, and door-to-door arrests—into coordinated persecution mechanisms. Criminal prosecutions arising from cyberpatrolling rely on decontextualized digital content without technical forensic analysis, proper chain-of-custody procedures, or evidence of concrete harm.

- **Telecommunications interception at scale:** Telecommunications interception is the most intrusive component of Venezuela's surveillance apparatus, with documented evidence of systematic practices that far exceed any legitimate law enforcement justification. Spain's Telefónica's 2021 transparency report—the last released before government pressure ended such disclosures—revealed 1,523,363 affected mobile telephone lines and 205,800 interception orders, demonstrating industrial-scale surveillance that is impossible to justify by targeted criminal investigations.[1] CANTV's state-owned infrastructure provides direct access to telecommunications data and internet traffic surveillance capabilities. The regulatory framework's structural flaws enable abuse: the Criminal Processing Code's mandate that telecommunications institutions maintain 24/7 availability to process interception requests, combined with the judicial system's subordination to executive power and the absence of independent oversight, creates conditions for unlimited surveillance without meaningful constraints.
- **State-sponsored cyberattacks and infiltration:** State-sponsored cyberattacks are systematic, employing sophisticated techniques combining technical capabilities with coordination across multiple government entities. Large-scale phishing campaigns targeting Volunteers for Venezuela, Healthcare Heroes, and grassroots electoral organizing units sabotaged opposition initiatives. Some mass-phishing campaigns used sophisticated network manipulation by CANTV to direct users to malicious government-controlled servers. Furthermore, opposition organizational platforms were exploited, and telecommunications interception capabilities used in targeted account takeovers. The coordination among state entities with technical and regulatory mandates and anonymous disinformation networks reveals state-sponsored malicious Internet manipulation. Venezuela's persistent efforts to acquire commercial spyware from multiple companies, combined with Citizen Lab's identification of FinFisher command-and-control infrastructure in Caracas, point to the deployment of spyware.
- **Warrantless device searches and seizures:** Warrantless inspection of mobile phones has become a pervasive practice, combining control, intimidation, punishment, and extortion in open contradiction to national and international human rights standards. Case documentation reveals forced cooperation accompanied by coercion and threats of detention or criminal prosecution. Economic extortion compounds political weaponization, with reports documenting demands for thousands of dollars in cash or Zelle transfers as conditions for not detaining individuals. High-profile individuals may undergo equipment inspections at airports, during which forensic analysis may be performed. Emerging patterns include online searches for travelers' names on Google and social media to find information about the political opinions of ordinary citizens.

Takeaways

Venezuela's surveillance infrastructure operates as a wide-reaching authoritarian control system transcending individual technologies and institutional actors. The convergence of video surveillance with telecommunications interception, cyberpatrolling with device searches, and state-sponsored applications with cyberattacks creates severely constrain civic space. The coexistence of various surveillance systems creates effects that are multiplicative rather than merely additive. An individual attending a protest faces multiple simultaneous risks, including being identified by facial recognition cameras, interception of communications while coordinating attendance, device searches at checkpoints, and potential cyberattacks that could compromise digital accounts. This layered vulnerability transforms constitutionally protected political participation into high-risk activities requiring operational security measures. Human rights violations extend far beyond immediate abuses to cause profound societal damage, including the normalization of self-policing and the erosion of civic space.

Critically, the surveillance infrastructure remains operational and intact despite Maduro's removal on January 3, 2026, demonstrating that technological capabilities and institutional frameworks for authoritarian control transcend individual leadership and require deliberate dismantling rather than mere regime leadership change. Understanding these systems in their full complexity—including technical capabilities, supply chains, institutional operators, legal frameworks, and human rights impacts—proves essential for supporting Venezuelan civil society under conditions of severe repression. There is a need for informing international policy responses addressing both current abuses and future accountability mechanisms, and ultimately contributing to dismantling the surveillance state apparatus itself, which is a necessary condition for genuine democratic transition.

Recommendations

The report provides targeted recommendations for four key stakeholder groups, focusing on the immediate operational needs of those most vulnerable to Venezuela's surveillance apparatus.

- **For civil society organizations:** Implement and provide tailored digital security and anti-surveillance training and resources to vulnerable populations; create emergency response networks for immediate assistance when activists face detention or device seizures; pursue accountability from surveillance technology vendors; and establish monitoring and sharing mechanisms to facilitate the documentation of surveillance technology and its human rights impacts.
- **For Venezuelan democracy activists:** Adopt digital security and surveillance mitigation protocols according to their roles and activities; use end-to-end encrypted communication platforms and implement hardware-based two-factor authentication to protect against interception of telecommunications; implement device sanitization protocols for high-risk scenarios such as checkpoints, airports, protests, and detention.
- **For democratic governments:** Demand dismantling of political surveillance infrastructure and accountability for documented abuses by conditioning sanctions relief and economic cooperation on concrete surveillance reforms and prosecution of officials responsible for systematic human rights violations; support Venezuelan civil society's digital security capacity through dedicated funding streams, technical assistance programs, and infrastructure support; and lead multilateral initiatives establishing norms against surveillance technology exports to authoritarian regimes through coordinated export control frameworks and supply chain transparency requirements.
- **For international multilateral organizations:** Develop accountability frameworks for surveillance technology vendors enabling human rights violations by investigating supply chains, documenting technological contributions to documented abuses, and pursuing legal mechanisms under international human rights law; provide technical assistance to Venezuelan civil society organizations by facilitating access to digital security tools and ongoing capacity building; coordinate international advocacy campaigns targeting surveillance technology companies through multilateral forums and public pressure; and integrate surveillance concerns into broader human rights monitoring by ensuring traditional human rights documentation mechanisms systematically incorporate digital rights violations and technology-enabled repression into investigations and reports.

Introduction

Against the volatile backdrop of Venezuela at a crossroads, Conexión Segura y Libre and the Atlantic Council's Digital Forensic Research Lab (DFRLab) have produced this report, which examines the country's surveillance technologies and their use for political control. The removal of Nicolás Maduro from the Venezuelan presidency does not signal the dismantling of the authoritarian infrastructure built over the past two decades. The sophisticated surveillance apparatus—which includes video monitoring systems, telecommunications interception, social media tracking, state-sponsored digital applications, device searches and seizures, drone surveillance, and cyberattacks—remains operational under Delcy Rodriguez's interim administration. Understanding these technologies, their capabilities, and their impacts on human rights is more critical than ever as Venezuela navigates an uncertain transition that could either lead to democratic reforms or the consolidation of a surveillance state under a new figurehead.

This report provides a comprehensive analysis of the surveillance technologies deployed in Venezuela for social and political control. The analysis encompasses both mass surveillance capabilities affecting large segments of the population and targeted monitoring of specific individuals and groups, particularly those engaged in journalism, activism, and political opposition. The surveillance ecosystem examined includes the VEN911 emergency response system integrated with closed-circuit television (CCTV) networks, facial recognition capabilities, license plate recognition systems, telecommunications interception at scale, social media monitoring and cyberpatrolling, state-sponsored mobile applications such as Patria and VenApp, systematic searches and seizures of electronic devices at checkpoints and detention facilities, drone surveillance operations, and sophisticated cyberattacks including phishing campaigns and likely malware deployment.

The report documents the technical capabilities of these systems, identifies the technology vendors and supply chains that enable them, maps their geographical deployment across Venezuelan territory, analyzes the institutional actors authorized to access and use surveillance data, and assesses the human rights impacts on the population. Particular attention is paid to the experiences of women in politics, journalism, and civil society organizations, who face disproportionate risks from state surveillance and repression. The analysis focuses on the period from October 2023 to January 2026, immediately after Maduro's removal, while including background information on the twenty-year history of state surveillance in Venezuela.

Objectives

This project pursues three primary objectives.

First, document and analyze surveillance practices in Venezuela, providing an outlook into specific mechanisms, technical capabilities, and the full scope of deployed technologies. This documentation addresses a critical knowledge gap: the absence of precise information prevents vulnerable populations, including journalists, activists, and women in public life, from implementing effective digital security measures to mitigate risks and protect themselves. By exposing surveillance practices and supply chains, the project enables civil society and potentially international bodies to hold technology vendors accountable for human rights abuses.

Second, to inform mitigation efforts and protection measures for those most at risk. The research findings translate into evidence-based insights to guide concrete actions to protect against surveillance and repression. By providing tailored information and guidance, the project will empower direct beneficiaries to better understand specific threats and develop more effective digital security and protection strategies. Enhanced understanding of regime surveillance practices significantly benefits those operating in high-risk environments by enabling them to better navigate and counter threats.

Third, to build resilience among vulnerable populations by increasing awareness and enabling citizen agency to evade, challenge, and resist rights-violating surveillance practices. The project fosters digital resilience not only among direct beneficiaries but also among the wider population, contributing to long-term outcomes that strengthen democratic institutions and the capacity of civil society to operate effectively despite surveillance pressures. The project's long-term vision comprises lessons applicable to the divergent paths of both democratization and authoritarian regime survival.

Methodology

The research employed multiple methodologies to ensure comprehensive and verifiable findings. Technical analysis of government-owned regime applications, particularly the Patria app, assessed data-gathering permissions and data storage methods to understand privacy vulnerabilities and state surveillance capabilities. Open-source intelligence (OSINT) research techniques systematically collected and verified publicly available information from government announcements, procurement records, social media posts by security forces, and journalistic investigations.

Conexión Segura y Libre developed a crowdsourcing campaign—limited by security constraints—to document the deployment of CCTV cameras throughout Venezuela, mapping the extent and nature of the country's surveillance infrastructure. Through document analysis, Conexión Segura y Libre and DFRLab examined legal frameworks, legislative records, procurement contracts, leaked internal documents, and official reports to understand the regulatory environment that facilitates surveillance. Additionally, the research team identified discrepancies between stated policies and actual practices.

In-depth interviews with technology experts, security sources, and individuals who had experienced surveillance and detention provided first-hand accounts of operational patterns and the impacts of surveillance. The interviews followed rigorous security protocols to protect sources operating under high-risk conditions. The research team also reviewed existing documentation from Venezuelan civil society organizations, international human rights bodies, and independent investigative journalism to contextualize findings within broader patterns of authoritarian control.

Report structure

The report proceeds through seven substantive sections examining distinct components of Venezuela's surveillance infrastructure.

The first section analyzes video surveillance systems, including the political context and regulatory framework governing CCTV deployments, detailed case studies of surveillance networks in three urban areas, facial recognition and license plate recognition capabilities, access and usage patterns by security forces, and human rights risks and impacts. The second section examines drone surveillance as well as GPS trackers, including the regulatory framework, suppliers, and key model capabilities, drone operations by security forces, recent deployments targeting the civilian population, and human rights impacts.

The third section analyzes state-sponsored and state-run digital applications, providing technical analysis and documentation of political uses for both the Patria app and VenApp. The fourth section investigates social media and internet surveillance, addressing limitations on freedom of expression within the legal context, state institutions' cyberpatrolling operations, harassment and doxxing targeting dissidents, persecution campaigns exemplified by Operation Knock Knock, and the intersection of information operations, surveillance, and repression.

The fifth section assesses private telecommunications interception, covering the technical basis for interception, the regulatory framework authorizing surveillance, evidence of telecommunications interception at scale, including institutional processes and agencies conducting interception. The sixth section examines cyberattacks, infiltration, and malware, covering phishing campaigns targeting journalists and pro-democracy activists, with analyses of targets, procedures, and noteworthy cases, including attacks on Volunteers for Venezuela, Healthcare Heroes, and grassroots electoral organizing units known as Comanditos. It also documents the intersection between information operations and phishing attacks. The seventh section documents the search and seizure of electronic devices, examining the political and legal context that enables these practices, patterns of searches at street checkpoints and airports, and during short-term detentions, and forensic extraction capabilities employed by security forces.

Throughout this analysis, the report maintains focus on the core reality that while political leadership in Venezuela may have changed dramatically with Maduro's removal, the surveillance infrastructure enabling authoritarian control remains intact and operational. Understanding these systems, their capabilities, and their human rights impacts is essential for supporting Venezuelan civil society, informing international policy responses, and ultimately contributing to the conditions necessary for a genuine democratic transition.

The evidence presented in this report serves multiple audiences: activists and journalists seeking to protect themselves; policymakers evaluating responses to Venezuela's political crisis; technology companies assessing their complicity in human rights abuses; and the international community working to support democratic aspirations in Venezuela.

Background: Venezuela at a new dawn for democracy

On January 3, 2026, United States Special Forces conducted a military operation at Venezuela's Fuerte Tiuna Army base, capturing Nicolás Maduro and bringing him to the US to face charges. This operation ended Maduro's thirteen-year authoritarian rule and significantly disrupted Venezuelan politics. It also raised questions about the country's future direction.

Within hours of the operation, Venezuelan Vice President Delcy Rodríguez stepped in as acting president, initiating a politically unstable period marked by competing influences from Washington DC, internal factions of Chavismo, and demands from Venezuelan civil society for a democratic transition.

The Trump administration's approach to post-Maduro Venezuela prioritized US economic and strategic interests over democracy promotion.[2] Following Maduro's capture, President Donald Trump explicitly dismissed support for either María Corina Machado, the 2025 Nobel Peace Prize laureate who led the democratic opposition, or Edmundo González Urrutia, widely recognized as the legitimate winner of the July 2024 presidential election. Instead, Trump emphasized US interests in Venezuelan oil and strategic minerals while maintaining relationships with Venezuela's existing power structure. US Secretary of State Marco Rubio outlined a three-stage timeline for post-Maduro Venezuela, including stabilization, economic recovery, and eventual democratic transition.[3] The timeline is expected to be measured in months or even years.

Delcy Rodríguez faces a challenging situation, trying to balance the demands of Washington, maintain control over a divided Chavista coalition, and manage Venezuela's complex relationships with authoritarian allies.[4] The Trump administration's demand for Venezuela to sever ties with China, Russia, Iran, and Cuba has created immediate operational challenges. Notably, the surveillance systems detailed in this report are foundational to the regime's stability. Chinese firms play a crucial role in the infrastructure that supports Venezuela's surveillance state. As of February 12, 2026, this surveillance infrastructure remains fully operational under Rodríguez, allowing the regime to maintain the social control mechanisms that characterized the Maduro era. Expelling Chinese technology firms would significantly disrupt Venezuela's surveillance systems, which are essential for the regime's internal control.

In May 2025, Russia signed a strategic partnership treaty with Venezuela, committing both nations to extensive cooperation in hydrocarbons and military technology.[5] Until the end of 2025, Russia was Venezuela's primary supplier of naphtha and diluents—critical additives necessary for processing Venezuela's heavy crude oil. However, energy deals signed on January 7, 2026, which allowed the US to become Venezuela's diluent supplier, directly conflicted with Russia's commitments.[6] Consequently, Venezuelan officials reluctantly abandoned their two-decade-long partnership with Russia.[7]

Iran provides Venezuela with significant international cooperation related to US security interests, particularly in drone technology production at El Libertador Air Base, where Iranian personnel have set up manufacturing operations.[8] On December 30, 2025, the US Treasury imposed sanctions on Empresa Aeronáutica Nacional SA for its joint ventures with Iranian companies involved in producing drone capabilities that pose a direct threat to US interests.[9] During a US Senate hearing, Secretary of State Marco Rubio stated that Iranian drones in Venezuela represent a "red line" that Rodríguez needs to address.[10]

Cuban intelligence advisors have been embedded within Venezuelan security services, offering counterintelligence expertise, interrogation training, and assistance with repression coordination. Nearly two thousand Cuban personnel reportedly left Venezuela by the end of January.[11] However, the number of Cuban security personnel still in Venezuela remains unknown, making it difficult to estimate the impact on the regime's espionage capabilities.

Both Cuban G2 and Iranian intelligence forces were linked to Venezuela's security apparatus via the Strategic Center for Security and Protection of the Homeland (CESPPA).[12] The CESPPA had been created in October 2013 as Venezuela's central intelligence coordination body, with legal authority to centralize information from all state security services (SEBIN, DGCIM, the DIM, and police forces) and to classify any information it deemed sensitive to national security. On February 9, 2026, acting President Delcy Rodríguez formally suppressed and dissolved CESPPA through Decree 5.248, published in Gaceta Oficial Extraordinaria No. 6.985, as part of a broader dismantling of Chavista-era institutional structures. This move reflects, at least in part, the accelerating withdrawal of Cuban and Iranian influence from Venezuela following Maduro's capture and under direct U.S. pressure. The elimination of CESPPA is the most significant institutional reform of Venezuela's intelligence architecture in over a decade.[13]

Initial steps toward political liberalization in Venezuela have focused primarily on the release of political prisoners, with estimates ranging from one to two thousand prisoners at the beginning of 2026. As of March 2, 2026, the Venezuelan human rights organization Justicia, Encuentro y Perdón ("Justice, Reunion, and Forgiveness") reported that 603 political prisoners had been released, leaving at least 759 still in detention, according to its own records of documented political prisioners.[14] The ongoing detention of political prisoners includes not only politicians, journalists, and human rights defenders, but also ordinary citizens arrested for participating in peaceful protests or electoral organizing activities. Among the detainees are teenagers, elderly individuals over seventy years old (who, according to Venezuelan law, should be granted house arrest even if convicted), those with life-threatening illnesses, and people with disabilities. Notably, one prisoner died in custody in January 2026.[15]

Beyond the release of prisoners, other indicators of political liberalization remain minimal. The Venezuelan censorship apparatus continues to operate at full capacity, blocking 135 websites, including sixty-one news outlets, as well as social media platforms like X and messaging apps such as Signal. Circumvention tools including VPNs (e.g. NordVPN, Psiphon, Mullvad, TorGuard, Tor Project, Proton) and public DNS servers like Google Public DNS and Cloudflare are also blocked.[16]

The legal framework enabling the criminalization of dissent—including the Law Against Hatred and the Organic Law Against the Imperialist Blockade—remains fully operational. Despite the threat of arrest, on February 12, 2026, college students organized well-attended peaceful demonstrations across the country to remember those who were killed in previous protests against the regime and to demand the release of political prisoners. These were the largest demonstrations recorded in the country since the August 2024 crackdown, during which at least twenty-five individuals were killed, dozens experienced brief forced disappearances, and around 2,400 were arbitrarily detained.[17]

At the time of editing this report, María Corina Machado and Edmundo González Urrutia are still unable to safely return to Venezuela. The continued exile of Venezuela's democratically elected leaders significantly hampers any democratic transition since their physical absence prevents them from organizing political activities or exercising the mandate granted by Venezuelan voters.

In the post-Maduro period, a fundamental tension has emerged: while the removal of Maduro eliminated the regime's figurehead, the authoritarian infrastructure that has sustained two decades of political repression remains in place and operational. Understanding this infrastructure—especially the extensive surveillance apparatus outlined in this report—is crucial for assessing the potential for a democratic transition versus the continuation of authoritarian rule under new leadership.

Video surveillance systems

The extensive video surveillance system deployed across Venezuela serves as a tool of domestic control. The surveillance apparatus operates within a legal vacuum that provides virtually no protection for citizens' privacy rights or due process guarantees. While the incorporation of CCTV systems into public security policies dates to 2007, significant expansion began in 2013, when then-Minister of Interior, Justice, and Peace Miguel Rodríguez Torres announced a $1.2 billion investment to install 30,000 cameras across sixteen cities through an agreement with China Electronics Import and Export Corporation (CEIEC).[18] This initiative created the Integrated Monitoring and Assistance System (SIMA), alongside the VEN911 emergency response system. In 2019, the Gran Misión Cuadrantes de Paz ("Great Mission Peace Quadrants") reorganized security policies around small territorial sectors with fixed patrols, while maintaining centralized monitoring through VEN911.[19]

The regime dramatically accelerated the deployment of CCTV throughout 2025 under the direction of the current interior minister, Diosdado Cabello. In June 2025, VEN911 Commander Neptalí Rodríguez reported 3,920 operational cameras monitored through twenty-six command-and-control centers, including the National Command-and-Control Center, nineteen state offices and six municipal facilities.[20] By December 2025, Cabello announced that the figure had surged to approximately seven thousand cameras, representing a 78.6 percent increase in just six months.[21] This expansion coincided with Cabello's November 2025 exhortation to "cover the majority of the territory with cameras" and his directive that mayors pressure private businesses to reorient their security cameras toward public streets, effectively conscripting commercial surveillance infrastructure into state monitoring networks. The minister explicitly acknowledged on April 3, 2025 that "the 911 is distributed throughout Venezuela, and we are linked with the cameras that shopping centers have, that residential complexes have," revealing integration between ostensibly private security systems and the national intelligence apparatus.[22]

The 2025 deployment wave extended surveillance beyond traditional public spaces into hospitals, residential neighborhoods, and opposition strongholds. On June 22 of that year, then-Minister of Health Magaly Gutiérrez announced the installation of cameras in major hospitals to monitor patients and medical staff, framing surveillance as necessary to prevent "sabotage" by unspecified opposition elements.[23] Caracas Mayor Carmen Meléndez declared plans on August 15, 2025 to install "smart cameras" at every traffic light and street corner in the capital, explicitly threatening to photograph and prosecute citizens for minor infractions like littering. "If we see someone from the command post throwing trash into the streets, we're going to take their picture, we're going to track them down, and then we're going to apply the Ordinance on Citizen Coexistence, Civility, and Community Justice," Meléndez said in an August 2025 radio interview.[24]

Most significantly, Cabello acknowledged on July 16, 2025 that security cameras played a "key role in identifying protesters" during the post-electoral demonstrations that took place from July 29 to August 3, 2024, publicly confirming what civil society organizations had previously documented: that CCTV footage systematically enables the identification, tracking, and arrest of government critics. This aggressive expansion occurred precisely as political repression intensified following the fraudulent July 2024 elections, suggesting surveillance infrastructure deployment directly serves regime consolidation rather than citizen security. The Rodriguez administration inherits this expanded technical capacity.

VEN911 likely serves a much broader purpose than just public safety emergency response, given its observed deployment footprint and the technical architecture of its infrastructure, provided by Chinese telecommunications manufacturer ZTE. And with at least eleven operational command centers organized in a clear national-regional-state hierarchy, the system has the physical infrastructure to enable ongoing, citywide population monitoring, particularly in Caracas and other major cities.

Among VEN911's component systems, the core feature of ZTE's Smart City Solution is its integration with big data and AI analysis platforms. It aligns with capabilities that Venezuelan officials have acknowledged: retroactive identification of protesters from recorded footage, license plate tracking at city access points, and real-time feeds to command centers.[25] Additionally, ZTE Government Cloud Solution provides a crucial enabling layer: a unified, cross-departmental data platform.[26] This means that surveillance data collected through VEN911 cameras can be cross-referenced with the Patria registry, SEBIN databases, and telecommunications intercept records held by other regime agencies. The combination of these ZTE-developed systems indicates that VEN911 may have the capacity for continuous movement tracking of individuals of interest and the retrospective identification of participants in public gatherings. These capabilities surpass those of a conventional emergency dispatch system and form the operational backbone of the regime's political surveillance apparatus.

The absence of judicial oversight mechanisms, data retention policies, or access controls means these systems can be weaponized against dissidents, protesters, and civil society organizations with impunity. This section examines three notable deployments, analyzes the supply chain behind the infrastructure, and assesses the human rights implications under the ruling regime, now headed by Delcy Rodriguez.

CCTV deployments

Three deployments illustrate the diverse operational models, political dynamics, and human rights implications characterizing Venezuela's CCTV infrastructure. Greater Caracas exemplifies the regime's most sophisticated surveillance architecture, in which the national VEN911 system integrate with municipal networks to create comprehensive monitoring capabilities across the capital region. Trujillo state demonstrates how national government resources fund the expansion of surveillance in interior regions, under conditions that prioritize regime security objectives over citizen safety, with camera placements concentrated around government facilities and the ruling PSUV party offices. Los Teques, Municipio Guaicaipuro in Miranda state, represents the regime's showcase deployment combining advanced Hikvision artificial intelligence capabilities, including facial recognition and license plate detection, with explicit political messaging from Minister Cabello praising its capacity to "detect everything" and "identify those who seek to act with impunity."[27] Together, these cases expose how surveillance infrastructure ostensibly deployed for crime prevention becomes weaponized for authoritarian control.

Greater Caracas metropolitan area: Co-opting municipal public safety systems

The capital region hosts Venezuela's most extensive CCTV infrastructure, integrating VEN911 systems with municipal networks across five boroughs. Intelligence officials report that VEN911 headquarters at Plaza Venezuela maintains command centers with direct feeds from strategically positioned cameras monitoring major thoroughfares, including the city's major avenues and highways. The system includes both fixed installations and mobile command units equipped with deployable camera arrays on extendable poles.

The municipality of Libertador, administered directly by the national government since it is within the country's capital, serves as the testing ground for centralized surveillance architectures. According to Neptalí Rodríguez, by June 2025 there were 774 security cameras in the municipality. Since October 2024, camera installation projects in the area have been managed by Fundación Caracas Inteligente ("Smart Caracas Foundation"), which is affiliated with the Caracas Mayor's Office.[28] Among the projects they have implemented are installing Wi-Fi networks in public spaces, as well as panic buttons and security cameras linked to VEN911 and the Peace Quadrants. On its social media platforms, Fundación Caracas Inteligente has reported the installation of cameras in main public squares such as Plaza de la Victoria and Plaza Venezuela, and at bus terminals such as the La Bandera Terminal and the Route 421 rapid transit terminal in central Caracas.[29] They also installed fifteen "smart" bus stops across the city equipped with panic buttons and

cameras linked to the VEN911 and the Peace Quadrants systems.[30] Both the cameras and the panic buttons installed by Fundación Caracas Inteligente were manufactured by the Chinese company Hangzhou Hikvision Digital Technology Co., which is currently sanctioned by the United States and the European Union for developing "key person" detection software used to surveil ethnic minorities in China.[31]

Hikvision cameras located in the Plaza Venezuela sector of the Libertador municipality. (Source: Caracasinteligente on Instagram[32])

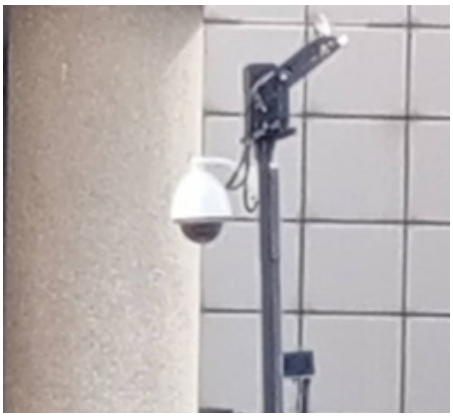
Opposition-controlled municipalities in Miranda state face complex pressures regarding surveillance infrastructure. The municipalities of Chacao, Baruta, and El Hatillo have developed parallel systems seemingly for legitimate public safety that nominally operate independently but face persistent pressure to integrate with the national security apparatus. These municipalities exemplify a broader pattern in which ostensibly independent security infrastructure is co-opted for political repression. These local systems also pose risks to opposition activists, protesters, and government critics because the central government can request and obtain access to their camera systems.

Chacao municipality exemplifies this dual dynamic: its Center for Integrated Security and Communication (CISC) employs Hikvision equipment and HikCentral Professional V3.0 software to manage extensive camera coverage throughout the commercially important borough. In March 2024, Chacao installed ten emergency buttons that allow direct video communication with CISC operators. The municipality publicized these installations as public safety improvements, yet their integration into centralized national databases remains opaque. Female residents and activists report heightened surveillance in areas where women traditionally organize community initiatives and protests.

The mayor of Chacao, Gustavo Duque, has highlighted his municipality's surveillance system as "the most modern in the country," featuring facial recognition and license plate detection technology.[33] On his social media accounts, the mayor has demonstrated that the cameras can clearly focus on details from more than one hundred meters away. There are at least 310 active cameras in this small municipality of five square miles, with a moderately high population density of approximately 12,000 people per square mile.[34]

These cameras are managed from CISC, which works in conjunction with the Chacao Municipal Police. CISC has a protocol for the immediate detection of "anomalous events" such as demonstrations, which allows for the activation of specific monitoring controls and the coordination of deployments in real time. There are indications of operational coordination between CISC and the VEN911 system, but no evidence of technical integration. CISC has temporarily deactivated cameras at specific locations when procedures such as raids or operations by agencies like the Directorate General of Military Counterintelligence (DGCIM) are to be carried out, to prevent these events from being recorded in its systems.[35]

In July 2022, when activists in Chacao created graffiti opposition slogans near Avenida Libertador, a main intermunicipal avenue, security forces detained them within hours. Civil society organizations documented evidence suggesting CCTV footage facilitated rapid identification and arrest. The detained activists—primarily young men and women associated with the opposition party Voluntad Popular—faced charges of "incitement to hatred" and "conspiracy." Women activists reported particularly invasive interrogations about their relationships with male organizers, reflecting gendered assumptions about women's participation in political dissent.



Camera located in the La Castellana sector of the Chacao munincipality, Caracas. (Source: VEsinFiltro)

Throughout the municipality of Chacao, dome-shaped PTZ (pan-tilt-zoom) cameras with 360-degree vision are visible. The entire system operates exclusively on an IP network and includes a DVR (digital video recorder) that distributes the camera feed to tablets used by authorized personnel. The municipality mayor, along with other officials and political figures, can view the camera feeds in real time on their tablets.[36]

Fixed and PTZ Hikvision cameras in the Altamira sector (left), and the Los Palos Grandes sector (right), Chacao municipality. (Source: VEsinFiltro)[122]

Both Baruta and El Hatillo municipalities also maintain independent security networks using Hikvision equipment, yet operate in environments where national security forces can requisition camera feeds without judicial authorization.

In Baruta, there has been a VEN911 command-and-control coordination center since 2016, although the exact number of security cameras it manages is unknown. Similarly, the Baruta Mayor's Office independently operates its own video surveillance system, with both fixed and PTZ cameras distributed throughout the municipality. However, municipal authorities have not disclosed information about the number of cameras they operate, their locations, or the characteristics of their control room.

Monitoring room at the VEN911 Baruta headquarters. (Source: Ven911baruta on Instagram[37])

Cameras belonging to the VEN 911 system in Chuao, Baruta Municipality. (Source: VEsinFiltro)

Since 2021, the municipality of El Hatillo has been installing security cameras in locations such as the historic town center and the Los Naranjos sector. By August 2023, this low-population-density municipality had thirty devices, including PTZ and mini-bullet cameras. These cameras feature artificial intelligence and a zoom capability similar to that of the systems used in Chacao. The cameras deployed in this municipality are managed by the Integrated Control Center (CCI), which, in turn, forwards incident reports to the El Hatillo Municipal Police Operations Center. As in Chacao, the mayor's office has not publicly acknowledged any linkages to VEN911 or the Peace Quadrants. To address public safety matters, El Hatillo also utilizes the police radio systems and a network of more than one hundred neighborhood WhatsApp groups. These WhatsApp groups serve as direct communication channels where residents can request personalized information about their area, file complaints, and report incidents to the CCI.

Multiple models of security cameras in El Hatillo, Caracas. (Source: PoliHatillo on Instagram[38])

The SIMA began operating in the Sucre Municipality in 2013 as part of a pilot project to reduce crime in the Petare neighborhood. On December 20, 2025, Interior Minister Cabello reported that the municipality had more than six hundred operational security cameras, some of which were located along a section of the Gran Mariscal de Ayacucho highway, which connects Caracas to the town of Guarenas.[39]

Many of these cameras were installed by the state-owned company Cantv, using a fiber optic network and integrated into the VEN911 system and the Peace Quadrants. In this municipality, Conexión Segura researchers have observed older bullet-type cameras, as well as dome and mini-bullet cameras manufactured by Dahua Technology, in underserved neighborhoods such as Petare and La Dolorita.

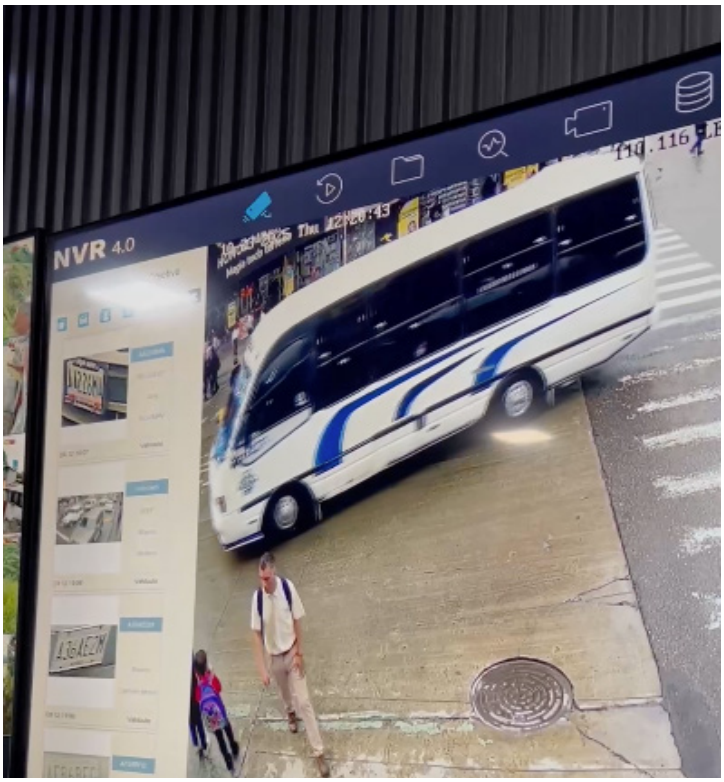
Cameras installed in the Sucre municipality. (Source: Cantv_ve on Instagram)

Despite the January 2026 political upheaval, surveillance camera placements near protest sites and politically sensitive locations are still underway. On January 21, security forces installed new cameras directly overlooking the encampments of relatives of political prisoners, who were holding vigil camps outside the Zona 7 detention facility, located in Sucre Municipality, governed by the PSUV ruling party. The cameras were placed to record vigil participants and individuals who approached to provide material support (e.g., food, medicine, blankets) to detainees' families. The gendered impact of such surveillance proves particularly acute: women constitute the majority of family members maintaining these vigils and face heightened risks of identification, harassment, and detention.

SOS Guaicaipuro: advanced artificial intelligence capabilities

Los Teques represents the regime's showcase deployment, combining extensive camera coverage with advanced artificial intelligence capabilities and explicit political messaging. In 2022, Mayor Farith Fraija initiated the installation of security cameras in strategic locations throughout Los Teques to create a real-time monitoring system coordinated with the Peace Quadrants. The project began with twenty cameras connected to a VEN911 situation room branded SOS Guaicaipuro.[40] By December 23, 2025, Fraija announced that the municipality had reached four hundred installed cameras covering main city access points, busy avenues, public squares, residential areas, and low-income neighborhoods.[41]

The political significance of the Guaicaipuro deployment became explicit on November 13, 2025 when Cabello visited Los Teques and effusively praised the surveillance infrastructure: "Guaicaipuro has an extraordinary camera system, because everything can be detected, especially in the capital, any place and event, which allows identifying those who seek to act with impunity, being key for security forces."[42] Cabello's language—emphasizing detection capabilities—transparently frames surveillance as political control rather than crime prevention. His specific reference to cameras being "key for security forces" rather than citizen safety implicitly acknowledging intelligence applications.



NVR 4.0 system used by SOS Guaicaipuro, showing its vehicle license plate recognition technology. (Source: Farith Fraija, Mayor of Guaicaipuro on TikTok[44])

The municipality openly displays on social media the technical sophistication of its Hikvision-supplied infrastructure. All cameras are from the sanctioned Chinese vendor Hikvision, including PTZ, turret, bullet, and mini-bullet models, providing comprehensive coverage. In an October 23, 2025, video, Fraija showcased the SOS Guaicaipuro Operations Room, revealing monitors displaying Hikvision's NVR 4.0 firmware interface.[43] This advanced system employs artificial intelligence for facial recognition, automatic license plate detection, heat mapping, and people counting. Fraija explicitly highlighted these AI capabilities in promotional materials, demonstrating the regime's confidence that advanced surveillance technology serves its interests. The operations room also features a Hikvision DS-1100KI(C) network keyboard with a four-axis joystick, enabling operators to remotely control PTZ cameras for real-time tracking of individuals or vehicles.

The Guaicaipuro deployment illustrates several concerning dynamics. First, rapid expansion from twenty to four hundred cameras in three years demonstrates the regime's capacity to scale surveillance infrastructure despite economic constraints, suggesting that surveillance receives budget priority over social services. Second, the explicit integration of real-time facial recognition and license plate detection capabilities—technologies that democratic societies regulate heavily—operates without any privacy protections, judicial oversight, or mechanisms for citizen consent. Third, Cabello's public celebration of the system's capacity confirms that regime officials viewed comprehensive surveillance as desirable and saw no political cost to openly threatening dissidents. Fourth, Mayor Fraija's enthusiastic promotion of AI-powered monitoring suggests that local officials recognized that the conspicuous expansion of surveillance enhanced their standing.

Trujillo State: integration of report sources

On April 26, 2025, Governor Gerardo Márquez and Health Minister Magaly Gutiérrez inaugurated new headquarters for the state command center, which includes a monitoring and video surveillance room for the municipality of Valera with 72 cameras. These cameras are manufactured by the Chinese company Dahua Technologies.[45] The Trujillo command interoperates with the 1x10 Good Governance system, which receives community reports submitted via Line 58, a VENapp feature that allows users to submit complaints and reports to government authorities.[46] It integrates with government situational rooms located in each commune, which are responsible for following up on reports submitted on the 1x10 platform. This command center coordinates with both the video surveillance system VEN911 and the VENApp application. This entails a linkage among government agencies, looping the surveillance system with a messaging platform VENApp, which has been used to dox individuals whom the regime labels as "terrorists."[47]

Cameras acquired in 2024 by the Government of Trujillo. (Source: gobtrujillo on Instagram)[48]

During the religious ceremonies for the canonization of José Gregorio Hernández in October 2025, the Trujillo state government reinaugurated the Trujillo Police headquarters in Isnotú, where the new Saint was born. Governor Gerardo Márquez reported that 18 PTZ cameras were installed as part of a video surveillance system at the entrances and exits and in the town center. It is worth noting that human rights activists took advantage of the religious celebration to call for the liberation of political prisoners. On October 18, 2025, journalist and former opposition councilman Yorbin García was identified and detained by officers of the Bolivarian National Intelligence Service (SEBIN) near the Isnotú Shrine. Conexión Segura was unable to confirm a direct link between this detention and the cameras installed in the town, as a large contingent of security forces, such as the SEBIN and the Directorate General of Military Counterintelligence (DGCIM), were present and constantly patrolling the area during the ceremony.

Technology supply

Chinese companies dominate Venezuela's surveillance technology supply chain, reflecting broader geopolitical alignments. Understanding vendor relationships proves essential for assessing technical capabilities and potential vulnerabilities in the surveillance apparatus that the Rodriguez administration inherits.

Between 2009 and 2013, approximately $80 million from the Cuba-Venezuela Bilateral Agreement was allocated to the development of the 171 Security and Emergency Response Center (Cesae 171), the direct predecessor of VEN911, through the National Development Fund (Fonden). Cuba participated in projects such as the National Citizen Security System (SINASEC) and the installation of 171 emergency response centers in the states of Aragua, Barinas, Falcón, Portuguesa, and Trujillo.[49] There is no clear evidence that any of these projects was actually fully implemented.

After 2013, China became the main provider of surveillance technology in Venezuela. Most of the Chinese companies identified as providers of surveillance technologies for Venezuela have been sanctioned by the United States, including ZTE Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, and Autel Robotics.[50]

Chinese Providers

China Electronics Import and Export Corporation (CEIEC) emerged as the primary architect of Venezuela's centralized surveillance infrastructure through its $1.2 billion contract announced in 2013. The company restructured the entire VEN911 system, comprising video surveillance, emergency dispatch, and data analytics.[51] Mobile command units with deployable multi-camera arrays mounted on telescoping poles are a signature CEIEC piece of equipment visible in state media coverage of security operations.

In 2020, the US Department of Treasury sanctioned CEIEC for "supporting the illegitimate Maduro regime's efforts to undermine democracy in Venezuela, including efforts to restrict internet service and conduct digital surveillance and cyber operations against political opponents."[52] CEIEC has been involved in Venezuelan prison security through the Technological Prison Security System (Sitesep).[53] The company's continued operations indicate mechanisms for sanctions evasion and regime prioritization of surveillance capabilities despite international isolation.

Mobile command unit with CEIEC multi-camera system on a deployable mast. (Source: VEsinFiltro)

Hikvision has captured significant market share beyond national government contracts, supplying equipment to both government and opposition-controlled municipal security networks. Hikvision faces US Entity List restrictions over its involvement in Xinjiang surveillance infrastructure.[54] The company provides cameras, network video recorders (NVRs), DVRs, and management software to municipalities in Miranda state, including Baruta, Chacao, El Hatillo, and Zamora—all with mayors affiliated with the Fuerza Vecinal party, which is not formally part of the Chavista regime's coalition. Chacao's CISC notably employs HikCentral Professional V3.0, an advanced security management platform that integrates multiple camera feeds, access control systems, and analytics tools. Hikvision also supplies emergency buttons deployed in the Chacao municipality that allow users to contact the CISC directly via video call in an emergency. The model used in Chacao corresponds to the Hikvision DS-PEA2-21 panic alarm station.[55] Since December 2024, Foundación Caracas Inteligente has also begun installing this same intercom model in several squares and strategic locations in the Libertador municipality.[56]

Zhejiang Dahua Technology Co., Ltd. has become a major hardware supplier for public surveillance installations in Venezuela. Their IPC-HFW2541T-ZAS bullet camera has been deployed across various municipalities, including Caracas, Miranda, and Trujillo. This model is a mid-range commercial camera featuring motorized varifocal optics, infrared night vision, and onboard video analytics. The technical specifications of the camera support functions such as perimeter intrusion detection and object classification, with capabilities for facial and license plate recognition integrated into the VEN911 command data streams.

Alarm stations in Chacao (left) and Libertador (right). (Sources: luisgonzalofer on Instagram; Caracasinteligente on Instagram)

Despite being placed on the US Entity List in October 2019 due to its involvement in the surveillance and repression of Uyghur populations in Xinjiang, Dahua has maintained access to Venezuelan market.[57] Additionally, Dahua and the Venezuelan administration have been exploring further integration of artificial intelligence into their systems.

High-level agreements between China and Venezuela, as well as testimony from workers in the field, have also revealed the involvement of other Chinese companies, such as Huawei Technologies Co. Ltd, ZTE Corporation, and China CAMC Engineering Co. Ltd in projects linked to the VEN911 system, although the extent of their involvement is unclear.

Belarusian providers

Between 2021 and 2023, the Venezuelan Ministry of People's Power for Interior Relations, Justice and Peace (MPPRIJP) held discussions with the Belarusian company Synesis for the acquisition of software to improve its integration of video surveillance systems and advanced facial recognition.[58] Synesis is sanctioned by the United States for providing software used by Belarusian authorities to facilitate the identification and arrest of protesters.[59]

The Kipod software offered to Venezuela features:

- Facial recognition system, including notifications and searches for specific individuals and their movement patterns
- License plate recognition
- Detection of a person with a firearm/bladed weapon
- Detection of abandoned objects
- Smoke detection (a demo for government officials used an image of protests in Caracas as an example)
- Crowd detection
- Perimeter security control and object detection in the area
- Traffic rule compliance monitoring

A roadmap memorandum was signed between the MPPRIJP and 24x7 Panoptes, the Synesis subsidiary that operates the surveillance system in Belarus, during an intergovernmental meeting in Caracas in 2021.[60] In 2023, during an official visit for an intergovernmental meeting in Minsk, Admiral Juan Carlos Oti, Director General of the Command, Control, and Telecommunications Centers (VEN 911), witnessed a demonstration of the software at the Operational Situation Headquarters of the Minsk City Police Department. It is unknown whether the planned demonstration in Venezuela took place or if the software was acquired.

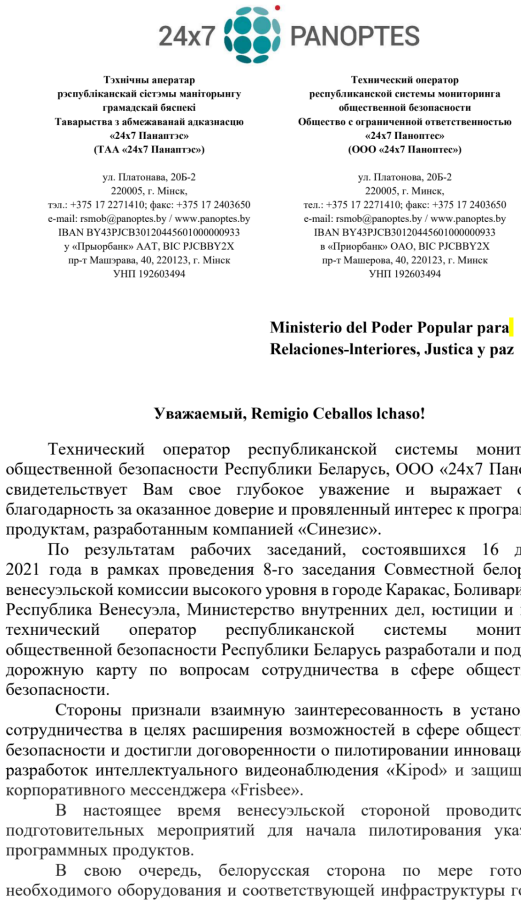
Admiral Juan Carlos Oti, Director General of the Command, Control and Telecommunications Centers (VEN 911), at the Main Directorate of Internal Affairs of the Minsk City Executive Committee, in 2023. (Source: Ministry of Internal Affairs of the Minsk City Executive Committee[61])

The access and usage of CCTV systems by security forces

The VEN911 system appears to operate as a hub where camera feeds can be accessed by national security entities, including the Bolivarian National Intelligence Service (SEBIN), the Directorate General of Military Counterintelligence (DGCIM), and the Ministry for Interior Relations, Justice, and Peace. Security forces could access video for investigations targeting political opponents, monitoring protests, identifying activists, and facilitating arrest operations.

Venezuelan surveillance architecture lacks fundamental safeguards that democratic systems employ to prevent abuse. No legal framework governs how footage can be used, who can access it, or for what purposes. The absence of judicial oversight, data retention policies, access controls, and civilian oversight bodies creates an environment where security forces can exploit CCTV systems for political persecution without accountability.

During a broadcast of his TV show Con el mazo dando ("With the mallet hitting") on July 16, 2025, Cabello acknowledged that security cameras on the streets played a key role in identifying protesters during the demonstrations that took place between July 29 and August 3, 2024, in protest of the stolen presidential election. He said, "Do you know what the poor innocent children of Atocha from the opposition were doing? They were provoking the police, pushing them, and then recording themselves when the police got angry and reacted; what happened before wasn't shown. Now there are cameras everywhere, so behave yourselves, they're watching you, they're looking at you."[62]



24x7 PANOPTES

Тэхнічны аператар
рэспубліканскай сістэмы маніторынгу
грамадскай бяспекі
Таварыства з абмежаванай адказнасцю
«24x7 Панаптэс»
(ТАА «24x7 Панаптэс»)

ул. Платонава, 20Б-2
220005, г. Мінск,
тэл.: +375 17 2271410; факс: +375 17 2403650
e-mail: rsmob@panoptes.by / www.panoptes.by
IBAN BY43PJCB30120445601000000933
у «Прыорбанк» ААТ, BIC PJCBBY2X
пр-т Машэрава, 40, 220123, г. Мінск
УНП 192603494

Технический оператор
республиканской системы мониторинга
общественной безопасности
Общество с ограниченной ответственностью
«24x7 Панаптес»
(ООО «24x7 Панаптес»)

ул. Платонова, 20Б-2
220005, г. Минск,
тел.: +375 17 2271410; факс: +375 17 2403650
e-mail: rsmob@panoptes.by / www.panoptes.by
IBAN BY43PJCB30120445601000000933
в «Приорбанк» ОАО, BIC PJCBBY2X
пр-т Машерова, 40, 220123, г. Минск
УНП 192603494

Ministerio del Poder Popular para Relaciones-Interiores, Justica y paz

Уважаемый, Remigio Ceballos Ichaso!

Технический оператор республиканской системы мониторинга общественной безопасности Республики Беларусь, ООО «24x7 Панаптес», свидетельствует Вам свое глубокое уважение и выражает особую благодарность за оказанное доверие и провяленный интерес к программным продуктам, разработанным компанией «Синезис».

По результатам рабочих заседаний, состоявшихся 16 декабря 2021 года в рамках проведения 8-го заседания Совместной белорусско-венесуэльской комиссии высокого уровня в городе Каракас, Боливарианская Республика Венесуэла, Министерство внутренних дел, юстиции и мира и технический оператор республиканской системы мониторинга общественной безопасности Республики Беларусь разработали и подписали дорожную карту по вопросам сотрудничества в сфере общественной безопасности.

Стороны признали взаимную заинтересованность в установлении сотрудничества в целях расширения возможностей в сфере общественной безопасности и достигли договоренности о пилотировании инновационных разработок интеллектуального видеонаблюдения «Kipod» и защищенного корпоративного мессенджера «Frisbee».

В настоящее время венесуэльской стороной проводится ряд подготовительных мероприятий для начала пилотирования указанных программных продуктов.

В свою очередь, белорусская сторона по мере готовности необходимого оборудования и соответствующей инфраструктуры готова в

Letter from Director A. P. Knysh of the Belarusian company 24x7 Panoptes addressed to Remigio Ceballos, Minister of People's Power for Interior Relations and Justice, provided by BELPOL.

On August 7, 2025, Cabello held a press conference to announce that the Bolivarian National Intelligence Service (SEBIN) had thwarted an alleged attempt to attack a recently inaugurated monument in the Plaza Venezuela area, adjacent to the SEBIN administrative building. He showed images taken by security cameras at the site showing a man leaving a bag there, in which explosives were later allegedly found.[63] The man recorded by the cameras, identified as José Daniel García Ortega, was later featured in a video released by Cabello in which he confessed to the act and linked the Venezuelan opposition to an alleged plan to carry out various attacks in the country. A total of thirteen people were arrested and accused of participating in the plan; opposition leader María Corina Machado and former Colombian presidents Álvaro Uribe, Iván Duque, Andrés Pastrana, and Juan Manuel Santos were named as the alleged masterminds.

Security cameras have also been used to directly intimidate protesters participating in peaceful demonstrations. On January 21, 2026, relatives of political prisoners held at the Bolivarian National Police (PNB) command known as Zone 7 denounced the installation of security cameras to monitor the camp where they had been holding a weeks-long vigil to demand the release of prisoners promised by the government. In videos shared on social media, officers can be seen placing a tripod with a camera on the roof of a riot-control vehicle. This camera was connected to the control panel of another camera already mounted on a nearby pole.[64] The device installed by the police was pointed directly at the tents where the protesters were sleeping and at the area designated as a restroom. The officers argued that the installation was legal because it was located in a security zone near the police headquarters.

Mobile cameras used to monitor protesters in Zone 7 in January 2026. (Source: cristiancrespoj on X[65])

Public information regarding data retention policies remains nonexistent. Security officials interviewed claimed to retain footage for periods ranging from ninety days to six months, though actual practices likely vary widely. VEN911 command centers may retain footage for longer periods, particularly recordings of high-value targets flagged for intelligence purposes. The technical capability for retroactive searches—querying archived footage to track an individual's movements days or weeks after the recording—may pose serious risks to activists and dissidents. Once security forces identify a person of interest, they can potentially reconstruct that individual's historical movements, identify associates, map networks, and establish patterns. Combined with data from telecommunications intercepts, social media monitoring, and device inspections at security checkpoints, CCTV footage could enable comprehensive surveillance targeting.

Human rights risks and impacts of video surveillance

Security forces can use CCTV footage to identify protest participants for subsequent detention, harassment, and prosecution. The knowledge that security forces monitor public spaces through extensive CCTV networks has a profound chilling effect on political participation and free expression. This is confirmed by grassroots activists in Caracas. Many people reduced their presence in public spaces, limited in-person meetings, or stopped organizing open activities starting in 2024. Activists opted for small gatherings, frequent changes of location, minimal use of mobile phones, and self-censorship on social media and in community groups. Individuals who responded to a survey on the topic noted the strain of constantly being observed. Informal polls conducted by the researchers indicate that Venezuelans do not perceive CCTV

systems as tools for public safety, but rather as social control devices used to identify, track, and deter citizens critical of the regime. In everyday discourse, the CCTV systems are referred to as “the control systems,” “the party’s cameras,” “the applications for marking people,” or simply “the surveillance.”

Facial recognition risks

While comprehensive facial recognition implementation remains uncertain, the threat creates severe psychological impacts on dissidents and activists. It must be assumed that law enforcement agencies can use recordings extracted from these CCTV systems to identify individuals. Advanced facial recognition capabilities would enable real-time identification of individuals at protests, public events, or even routine activities like commuting. Combined with the extensive databases security forces maintain, facial recognition would allow tracking virtually any person of interest in public spaces.

Similar to the policies governing access to and retention of recordings, the facial recognition capabilities of the various surveillance systems have not been made public. Depending on the combination of these policies and technical capabilities, it could be possible to retroactively search recordings for the actions and routes taken by a person of interest, weeks or months after they were recorded. Another risk, although less likely in the Venezuelan context, is that operators of these systems could identify any person in the video in real time by cross-referencing their face against state-held databases.

License plate risks

The proliferation of CCTV deployments with integrated license plate recognition capabilities, coupled with license plate readers installed on strategic routes such as vehicular access points to Caracas and regional roads, could facilitate vehicle tracking on a massive scale, especially if they are integrated and record the movements of all vehicles and not just a list of wanted license plates. This kind of continuous, virtually unavoidable tracking, without sufficient safeguards and effective judicial oversight, would seriously threaten freedom of movement and the right to privacy, posing risks to dissidents.

Surveillance using drones and other methods to monitor movement in public spaces

Following the contested July 2024 presidential election and subsequent political crisis, Venezuelan security forces expanded aerial and ground-based surveillance targeting opposition mobilization and civil society activities. The deployment of industrial-grade drones equipped with high-resolution cameras, thermal imaging, and powerful zoom capabilities enhanced the monitoring of protests, political gatherings, and individual dissidents. Complementing this aerial surveillance infrastructure, security forces have installed GPS tracking devices with listening capabilities on vehicles belonging to family members of political prisoners and opposition figures. These location-tracking technologies operate covertly, requiring physical access to target vehicles, to provide comprehensive data on movement patterns and frequently visited locations, enabling real-time tracking.

This section first examines drone surveillance operations targeting protests and opposition gatherings, then analyzes intimidation tactics employing visible drone presence, documents GPS tracking device deployment, and concludes with an analysis of human rights impacts across both surveillance modalities.

Monitoring protests through drone surveillance

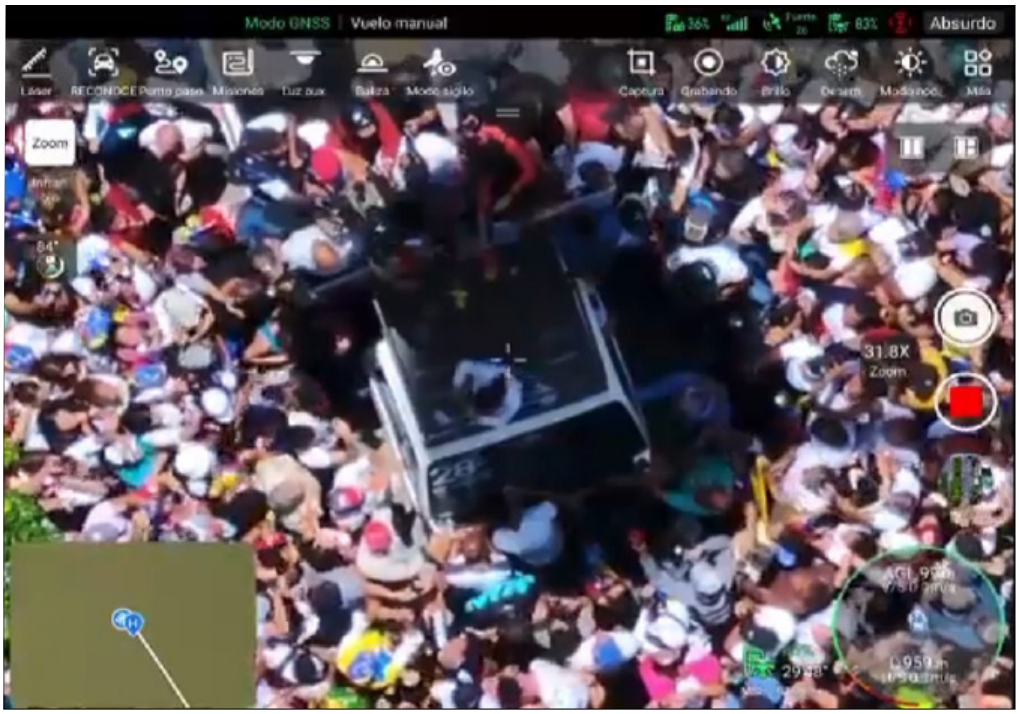
The earliest drone deployments in Venezuela originated from contracts associated with the VEN911 system. Drones provided to the Ministry of Interior, Justice, and Peace under these contracts saw limited operational deployment and currently appear non-operational, with some units still visible in offices and pilot training facilities.[66]

The post-electoral crisis of 2024 triggered expansion in drone surveillance operations. Security forces deployed drones to monitor streets, surveil protests, and track individuals while simultaneously employing these capabilities for intimidation purposes.[67] The protocols for the operation of drones by state security forces remain undisclosed.

The most sophisticated drones identified are Autel EVO Max 4T units.[68] This model is a specialized enterprise surveillance quadcopter featuring a flight time of up to 42 minutes and a transmission range of 20 kilometers. Its standout feature is a versatile 4-in-1 camera system that includes a 48MP zoom camera with 10× optical and 160× hybrid zoom, capable of identifying vehicles from 2 kilometers away. Additionally, it has a 50MP wide-angle camera, a 640×512 thermal imager, and a laser rangefinder with a range of 1,200 meters. The EVO Max 4T is equipped with advanced autonomous capabilities, including GPS-denied navigation via SLAM, A-Mesh multi-unit networking, AI subject tracking, and resistance to electromagnetic interference. Autel specifically markets this platform for use in public safety surveillance, search-and-rescue operations, and infrastructure monitoring.

The EVA Max 4T has been formally procured and deployed in at least two active conflict zones: Ukraine (by both Russian and Ukrainian forces) and Gaza by Israeli forces.[69] These battlefield deployments have resulted in the U.S. adding Autel to the Pentagon's Section 1260H list of Chinese military companies in January 2025.[70]

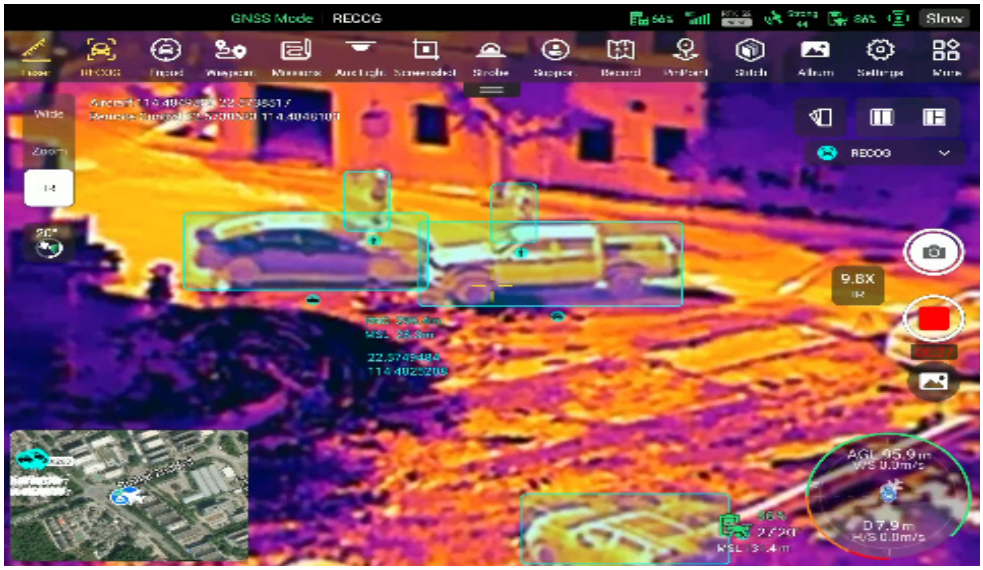
After the 2024 presidential election, opposition leader María Corina Machado became a primary target of surveillance. On August 3, 2024, during an opposition rally in a commercial neighborhood in Caracas, a drone captured high-resolution footage showing Machado's face in an extreme close-up as she removed a



31.8x zoom of María Corina Machado at a rally captured by a drone, video published by Delcy Rodríguez on X. (Source:@delcyrodriguezv on X)

hood covering her face while boarding the truck platform that served as the event stage. Despite arriving on a motorcycle to avoid identification by authorities, the drone's 31.8x optical zoom enabled identification from a significant distance. Then-Vice President Delcy Rodríguez disseminated this footage via social media, demonstrating both the surveillance capability and the regime's willingness to publicize its monitoring of opposition leadership. [71] [72]

VEsinFiltro has documented at least twenty distinct cases of drone deployment, mainly for capturing aerial recordings of opposition rallies in Caracas and other cities. These recordings were shared on social media



Autel Alpha operator's user interface with IR camera enabled, as seen in a promotional video by the manufacturer. (Source: Autel Robotics)

by high-ranking regime officials and official state media.[73] The footage showed that these drones could focus sharply on specific individuals' faces from a distance, suggesting that authorities might use this technology to identify and target rally participants.

Additional advanced models identified in operational use include the Autel Alpha—a heavy industrial surveillance quadcopter weighing 6.34 kg in standard configuration, previously unreported in Venezuelan security force inventories.[74] The Bolivarian National Guard operates Autel Dragonfish units, vertical takeoff and landing (VTOL) fixed-wing drones designed for extended operations. The National Guard maintains responsibilities for public order control, making these long-endurance surveillance platforms particularly concerning for monitoring political activities.

Venezuela implements a high-low acquisition strategy for drone procurement. High-end surveillance operations employ commercial Autel-branded drones with advanced surveillance and security specifications. Lower-tier reconnaissance and surveillance operations use multiple models of compact DJI quadcopters, including DJI Mini-series units apparently operated directly by tactical units of police forces. This analysis excludes drones operated by the Bolivarian Military Aviation or other exclusively military platforms.

Model	Operating Security Forces	Type
DJI mini 2	GNB	Compact Consumer Quadcopter (Foldable)
DJU mini 3	CPNB	Compact Consumer Quadcopter (Foldable)
DJI mini 4 Pro	CPNB	Compact Consumer Quadcopter (Foldable)
DJI Mavic Air 2	GNB, CPNB	Commercial Consumer Quadcopter (Foldable)
Autel EVO Max 4T	SEBIN	Industrial, Surveillance Quadcopter (Foldable, Weather-Resistant)
Autel Alpha	SEBIN	Heavy Industrial, Surveillance Quadcopter (Foldable, Weather-Resistant)
Autel Swordfish	GNB	Industrial, Surveillance and Defense VTOL fixed-wing drone
DJI AVATA	GNB	Consumer First Person View Quadcopter

Table with a selection of drone models identified in use by Venezuelan security forces. (Source: VE sin Filtro.)

Intimidation and harassment through visible drone presence

Between July 30 and August 3, 2024, drones observed flying over various areas of downtown Caracas at night were documented on social media. In these posts, the drones, equipped with multiple lights, appeared to be searching for hotspots of protest and likely served as an intimidation tactic.

Footage of the surveillance drones was shared on social media by residents observing them from apartment windows in downtown Caracas. Analysts indicate that the security agencies operating these drones intended to instill fear and create a chilling effect among potential protesters. This judgement is based on the number of drones patrolling the same sector simultaneously, rather than deploying more sparsely to cover larger areas. Furthermore, some of the identified models are technically capable of flying without lights, yet the drones were consistently observed patrolling with their lights on. That choice served no operational necessity and appears designed to maximize public awareness of their presence, suggesting intimidatory intent.[75]

In addition to monitoring protests, these drones could also be used to spy on political dissidents. On January 7, 2025, Machado reported that drones were flying over the house of her mother, Corina Parisca, in Caracas.[76] A similar incident was reported on November 23, 2024, at the Argentine Embassy in Caracas, where five opposition members were seeking asylum. One of them, Pedro Urruchurtu, denounced the use of drones to monitor them on his social media account during a siege by security forces.[77]

On January 6, 2026, just days after Nicolás Maduro was seized by the US Armed Forces, drone flights were observed monitoring the vicinity of the Presidential Miraflores Palace and possibly other strategic locations at night. In that incident, unidentified pro-regime armed individuals reacted in confusion, reportedly firing at the state surveillance drones, thinking it was a second attack by US forces.[78]

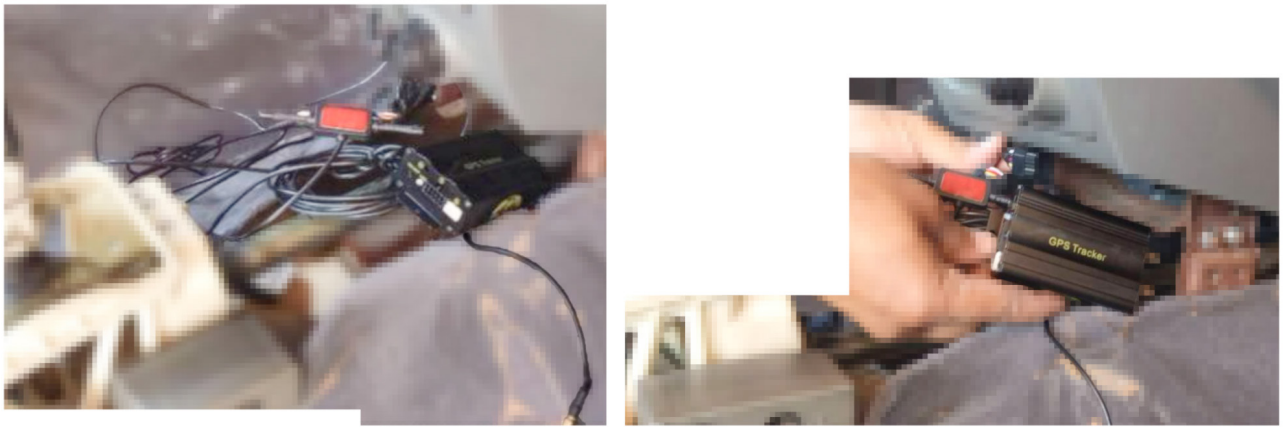
GPS trackers and listening devices

GPS tracking technology enables covert surveillance of target movements over extended time periods. Installation requires physical access to the target vehicle at a moment when the owner would not notice the intrusion. Once deployed, tracking devices generate near-continuous location data streams that operators can exploit to reconstruct previous routes, identify frequently visited locations, establish patterns of movement, and enable real-time tracking to facilitate additional operations. Devices documented in Venezuelan surveillance operations include integrated microphones enabling eavesdropping on conversations. GPS tracking proves necessarily more operationally risky if operators wish to avoid detection—requiring physical access to vehicles—but provides additional surveillance layers that increase immediacy, granularity, resilience against anti-surveillance practices, and independent operation capability.

Instances of GPS tracking have included the targeting vehicles owned by family members of political prisoners with military backgrounds. The focus on families with military connections may reflect security force concerns about the activities of the families of the detained, or may represent part of a wider pattern tracking groups advocating for the release of political prisoners. It is also possible that these individuals might have been targeted because their cases are perceived as particularly threatening to regime security. Civil society organizations assess that relatives of certain civilian political prisoners or other civic actors may have been similarly targeted without ever discovering the devices.

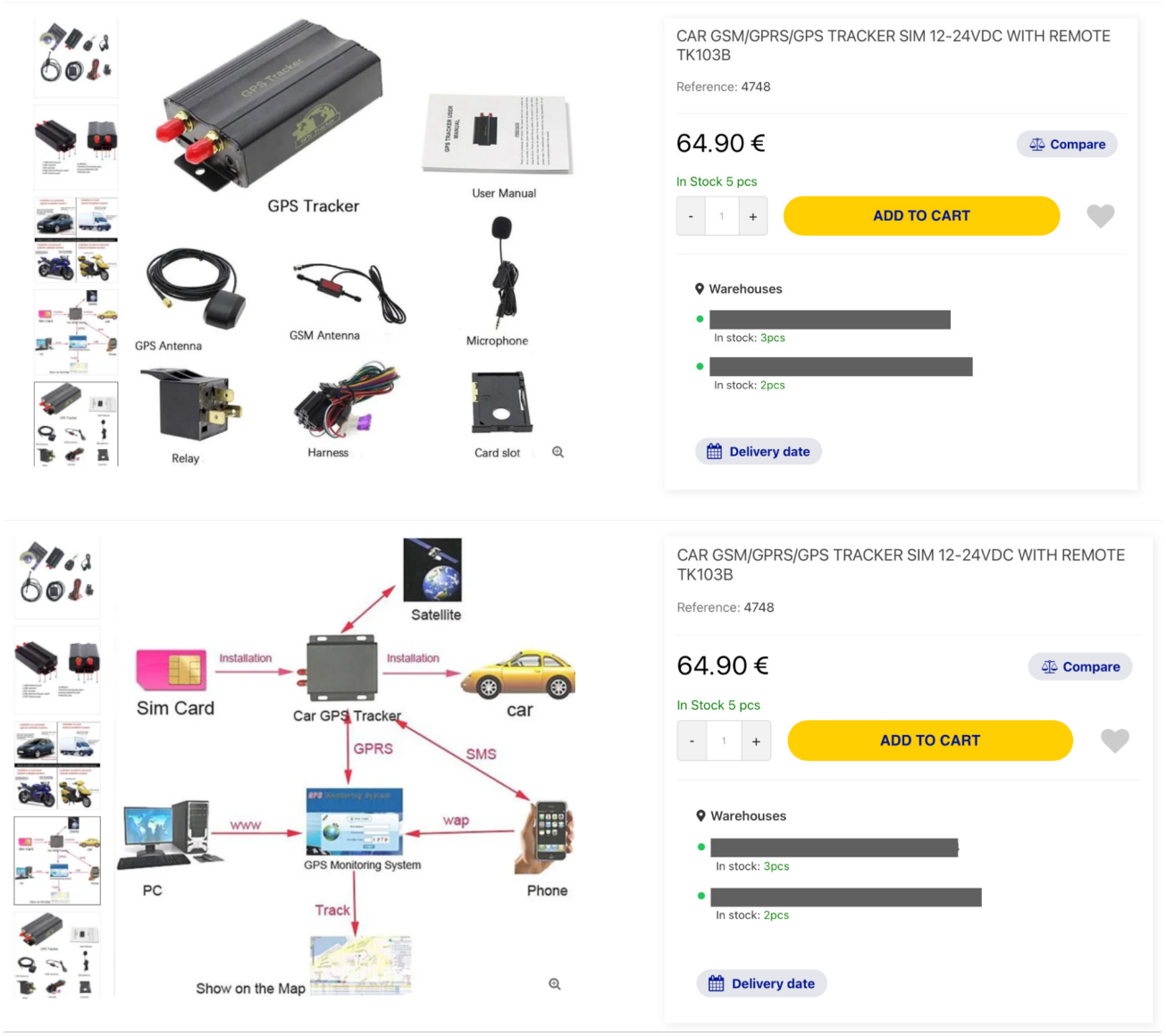
Internal trackers

In a previously unreported case from 2023, VEsinFiltro documented a GPS tracker hidden inside the cabin of a vehicle used by family members of a political prisoner.[79] The device matches TK-103 GPS tracker models available from multiple Chinese manufacturers. This older-generation design requires a SIM card for GSM/GPRS cellular communications, supporting SMS messages, voice calls, and low-bandwidth cellular data.



Images of the device inside the victim's vehicle while in the process of being uninstalled.
Sections of the image are pixelated or obfuscated to protect the victims´ privacy. (Source: VEsinFiltro)

The unit was hidden behind plastic dashboard covers and connected to the vehicle's electrical system for power. A technician servicing the vehicle discovered the device when investigating electrical problems that developed one week after a family member visited the detention center where their relative was held. During that detention center visit, the car remained out of sight for at least one hour—the apparent installation window. The mechanical problems that led to the discovery suggest the installation may have been conducted hastily or by personnel without technical expertise, thereby inadvertently damaging vehicle systems. Trackers concealed inside vehicle cabins are especially difficult to both install and identify. Models observed operate on vehicle electrical systems, enabling nearly indefinite operation without requiring battery replacement.



Product listing of a similar TK103 GPS tracker showing key components and its operation. (Source: ABCLED[80])

The integrated microphone enables eavesdropping on vehicle conversations by dialing the tracker's phone number when monitor mode is enabled. Operators send commands to TK103 units via SMS and calls to the SIM card phone number. Users can monitor vehicle location through a manufacturer-provided website or directly from the unit via SMS messages containing GPS coordinates and map links, either on demand or automatically at set intervals when the vehicle moves. Online portals or mobile applications enable operators to review historical routes and movements, configure geofencing alerts, and access additional monitoring features.

External trackers

Externally mounted trackers provide similar functionality but prove substantially easier for security forces to install, as brief periods when vehicles are parked without supervision provide sufficient installation windows. While operating on internal batteries rather than vehicle power, these batteries can last several months depending on the model and usage patterns. When devices approach battery depletion, operators can hypothetically swap units to maintain continuous surveillance.

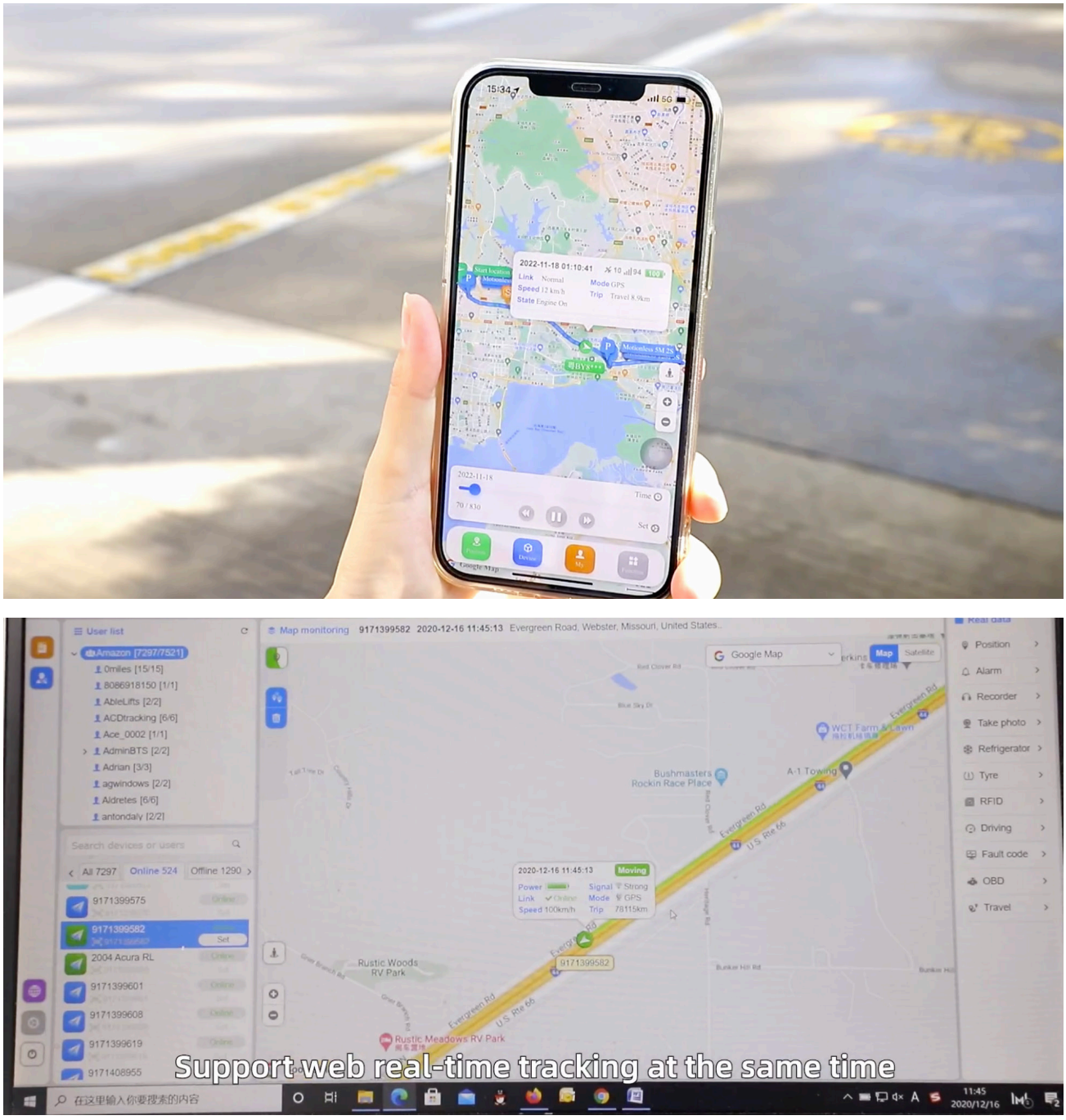
On September 15, 2025, Margareth Baduel, an activist for political prisoners, publicly denounced via social media the presence of a tracking device on a vehicle used by her family.[81] The device was identified as a GPS tracker. Margareth Baduel is the sister of political prisoner Josnars Baduel and daughter of General Raúl Isaías Baduel, a former Chávez minister who died while being a political prisoner in 2021.[82]

The tracker in Baduel's car was affixed magnetically to the rear underside of the vehicle as documented in several videos. After the tracker's discovery was circulated on social media, officials from the Criminal Investigation Division of the Bolivarian National Police quickly arrived at the site to retrieve the device without providing any explanation.[83]

The unit visually matches the SinoTrack 915L model or the slightly less capable 915 model. SinoTrack 915L and 915 models require operational SIM cards and accept SMS commands. SinoTrack provides mobile applications and web interfaces for monitoring and management that support large numbers of units, historical route playback, and other features designed for fleet management applications, which security forces have repurposed for political surveillance.

Left: Excerpt from a video published by the Committee for the Freedom of Political Prisoners (CLIPPVE) showing the GPS tracker installed under the vehicle. Right: Partial screenshot of the SinoTrack website. (Sources: @clippve on X; SinoTrack)

The device includes a microphone that can capture surrounding conversations, though its effectiveness for recording conversations inside vehicles is likely limited by the external mounting location under the chassis. The optimal microphone placement for vehicle interior surveillance would require internal installation, suggesting that this external tracker's audio capability may primarily serve as supplementary intelligence when targets exit vehicles. Battery life reaches 120 days in standby mode, where operators request location via SMS or calls. Alternative modes that enable automatic location updates at various intervals provide shorter battery life but more frequent position reporting. The multi-month battery life enables extended surveillance operations without requiring repeated physical access to target vehicles.



Frames from video demonstrating the function to replay historical movements recorded by a tracker, in addition to real time tracking on the Amazon listing for the ST-915L. (Source: Sinto Track, Amazon.com [84])

Human rights impacts of movement surveillance

Drone surveillance by security forces operating within the context of restricted fundamental freedoms generates severe human rights impacts. Beyond surveillance collection, security forces employ drones as psychological weapons to suppress opposition mobilization. The possibility of aerial surveillance produces chilling effects, and the pervasive sense of surveillance erodes community organization and small-scale protest initiatives, even absent direct enforcement actions. The intimidation function operates through multiple mechanisms. First, the visible presence of hovering drones signals to protest participants that authorities are monitoring and recording their activities. Second, government officials and state media deliberately amplify the surveillance message through the dissemination of drone footage showing opposition activities. Third, in the context of documented persecution of protest participants through arbitrary detention, prosecution, and imprisonment, individuals realize that aerial surveillance creates identification records that may be used against them.

The absence of meaningful rules and controls limiting surveillance deployment, data retention policies, access restrictions, independent oversight mechanisms, and victim remedies enables abuse. Although protests occur in public spaces, persistent aerial surveillance, analogous to CCTV systems, captures details that collectively affect privacy: who attended, who they associated with, how long they stayed, and their movement patterns. In persecution contexts, this information converts into material risks affecting personal safety and liberties. When attending political events, individuals are subject to aerial surveillance that may be circulated through pro-government channels or used as evidence to justify targeting, a coercive means of restricting the full exercise of political rights.

Venezuelan law requires judicial authorization for intrusive surveillance measures that involve manipulating vehicles or accessing private spaces. Specifically, listening devices that record environmental conversations require prosecutors to obtain judicial approval, which must clearly state the crime under investigation, the technical means employed, the deployment location, and a duration of no more than thirty days.[85] In practice, documented cases of GPS tracker deployment reveal no judicial oversight, and family members targeted by these devices have received no legal notice or explanation of their installation. The covert nature of GPS surveillance means that many targets may remain unaware of monitoring for extended periods, during which authorities accumulate comprehensive intelligence on opposition networks, activities, and operational patterns.

The systematic deployment of movement surveillance technologies—both aerial and ground-based—without judicial oversight, legal constraints, or transparency fundamentally undermines freedom of assembly and association guaranteed under international human rights law. The Inter-American Commission on Human Rights has recognized that pervasive surveillance, which creates a reasonable fear of identification and subsequent persecution, effectively prevents the exercise of the right to assemble, even when direct prohibitions are absent.13 Venezuela's movement-surveillance infrastructure achieves precisely this chilling effect, transforming constitutionally protected political participation into activity that requires sophisticated operational security measures and entails substantial personal risk.

State-sponsored and state-run digital apps

Over the past decade, a dual-use technological surveillance network has been consolidated in Venezuela. In official discourse, these digital tools are presented as instruments for optimizing public service delivery. However, the accumulated evidence indicates that this infrastructure has primarily been used for the systematic, large-scale collection of personal data and for social control.

The Venezuelan state has advanced a process of platformization of citizen control through the deployment of digital applications. The Patria System—presented as a social protection platform—and VenApp—promoted as a citizen service tool—constitute the two central pillars of the government apps ecosystem. Together, they enable the systematic extraction of information, the classification of the population, and the application of social control mechanisms. Their socio-technical architecture reveals how authoritarian regimes leverage digital platforms to transform social welfare delivery and public service access into instruments of political control.

The Patria System

The Chinese company ZTE played a central role in developing the database for the Carnet de la Patria ("Homeland Card"), incorporating advanced capabilities for identification and massive data gathering.[86] The Patria System and the Patria Card have become the primary channels for accessing subsidies and welfare assistance programs, while also serving as instruments of economic pressure and behavioral control. The dependence of millions of people on these benefits transforms the system into a tool that conditions daily subsistence on mandatory registration and the constant provision of personal information.

A particularly revealing element is that the platform's web domain (patria.org.ve) is registered in the name of the United Socialist Party of Venezuela (PSUV), instead of any state agency.[87] This fact demonstrates the operational fusion between the state apparatus and the party structure, blurring any functional separation between public policies and political control, and subordinating the data of millions of citizens to a logic of party loyalty and utility.

Access to welfare benefits is neither automatic nor transparent; it is conditioned on registration and the continuous provision of information within the system, without transparent criteria for allocation. To maintain eligibility and increase the chances of receiving welfare benefits, users must periodically update their data and respond to surveys about their socioeconomic situation and consumption habits. In practice, this design turns the need to access essential goods and welfare into a permanent incentive to update the information the citizen provides to the state.

The system's technical design reinforces the logic of authoritarian control. A significant portion of the information collected by the Patria System focuses on users' relationships with other people and institutions, enabling administrators to create detailed network maps of connections among citizens, even if those citizens do not use the platform. Some examples include the registration of household members and other direct relatives, registration of friends and acquaintances in the "Return to the Homeland" operation (for reporting migrant relatives returning to the country who may be unregistered), healthcare professionals who have provided services to the user, records of bank transfers made and received including personal data of the counterparts, identities of contact persons in local state organizations such and communal councils and CLAP food distribution chains, and registration of people to whom users lend their motor vehicles, among others.

It is noteworthy that the platform does not offer any control or authorization verification for the provision of third-party personal data, or any accessible data management or protection policies on the platform or in the Google Play Store.

Another notable aspect of the implementation of the Patria System platform is the technical limitation of user access from outside Venezuela. To start, the mobile application is not available on the Google Play Store for devices outside the country. Moreover, the system uses geofencing, a technique that prevents access to the relevant servers from outside the country. The system checks the country reported by the network to confirm that the application is being accessed from within Venezuela; if not, access will be denied.

This political control has one of its most visible expressions in the electoral realm through the so-called "red points," PSUV kiosks installed near polling stations on election days. Although formally presented as spaces to foster voter turnout and provide guidance on the process, in practice, they function as mechanisms to monitor whether Homeland Card users have cast their votes. At these red points, staff from the ruling party record voters' attendance by scanning the QR code on their Homeland Cards or manually entering their personal identification data into a party database. The ruling party uses that information to call welfare recipients to vote if they have not shown up at the polling stations in the early morning. After election day, those who voted may receive one-time bonuses, while those who abstained may be denied welfare benefits. In this way, the act of voting—which should be voluntary and free from pressure—is integrated into a system of rewards and punishments mediated by digital platforms. Although the red points do not allow verification of the vote's content, when this mechanism was established in 2018, a conspiracy theory spread claiming that the QR code somehow allowed checking the vote's content.[88] That is not technically feasible, but some people were persuaded of it, so they feel further compelled to vote for the ruling party.

The red points thus embody the convergence between technological surveillance and political control, reinforcing the perception of constant monitoring and facilitating indirect coercion that affects the effective exercise of political rights, especially among populations most dependent on state assistance.

VenApp

VenApp is a newer piece in the Venezuelan regime's digital ecosystem. Unlike the Patria System, whose central focus is individual monitoring and economic coercion, VENApp shifts the focus to collective surveillance and promotes what can be described as an institutionalization of neighborhood snitching, under the guise of a social super app, including a tool to report problems with government services

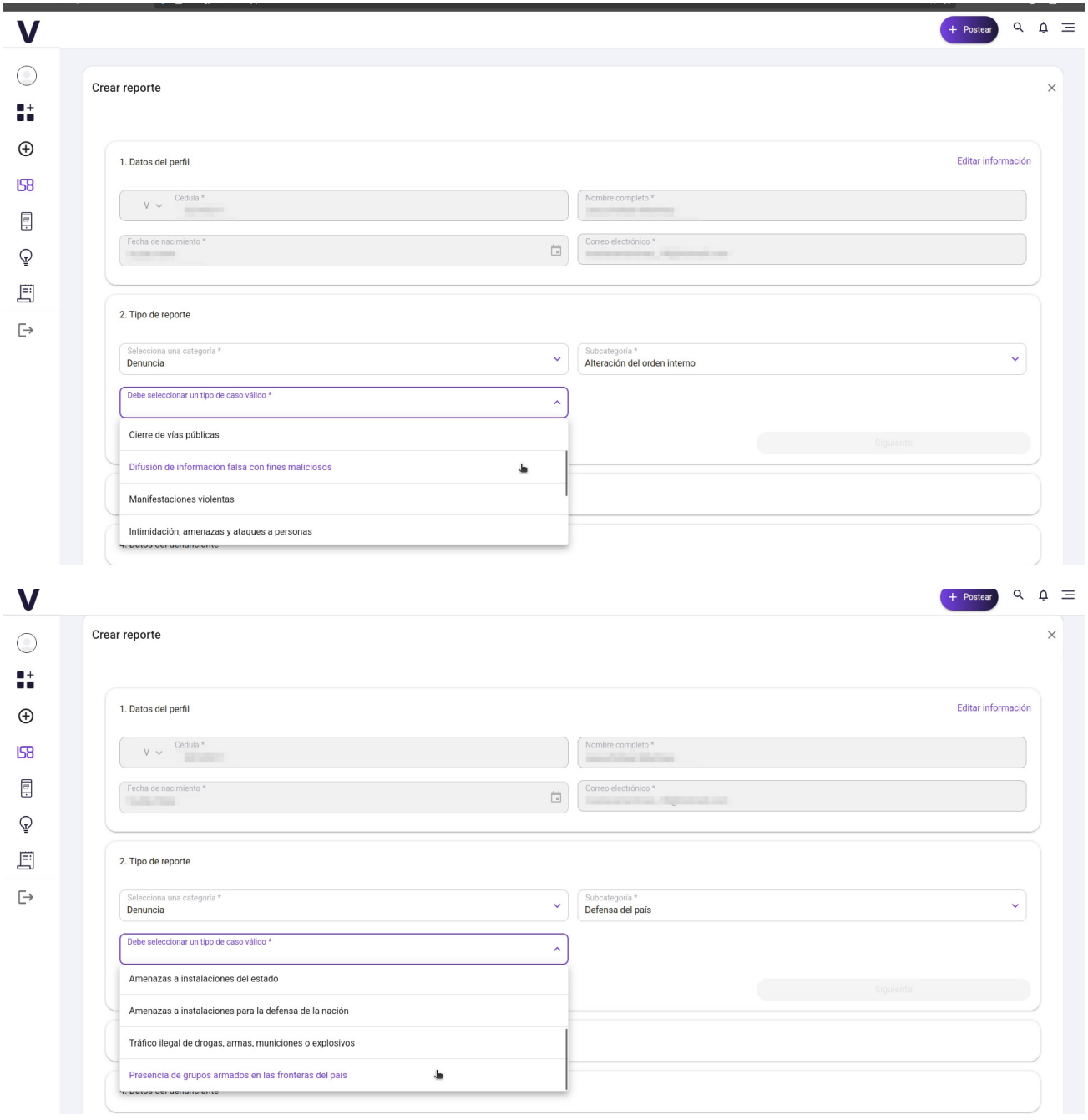
VenApp provides a technological platform for denouncements that Chavismo sought to institutionalize since at least 2008, when it attempted to pass the Law of Intelligence and Counterintelligence, which compelled citizens to collaborate with intelligence services by providing information about people critical of the government. That law was popularly nicknamed "Ley Sapo," as Venezuelans typically call snitches sapos ("toads"). Public outrage became so intense that the law was repealed two weeks after it was approved.[89]

Initially, a precursor version of VenApp was designed to monitor PSUV supporters' electoral mobilization during the 2021 gubernatorial elections. Later, in 2022, it was opened to the general public as a Venezuelan messaging app with public channels similar to Telegram and a photo-sharing feed similar to Instagram. The app gained traction in 2023 when it was relaunched as a platform for reporting failures in utilities and other public services, leveraging its geolocation-sharing capability.[90] Immediately after the July 2024 presidential election, a new feature was added to VenApp to allow citizens to report protests and individuals who participated in the opposition electoral organization.[91]

VenApp is based on a commercial platform developed by a Panama-based company that is adaptable to various use cases for different clients.[92] This is why the same app has had different features and use cases in a span of just five years. Technically, VenApp has a more standardized data structure than the Patria System and therefore does not directly request sensitive information such as political affiliation or personal identification data. However, the reporting functionality presents a significant problem. The app interface offers reporting categories that have historically been associated with political persecution, and the criteria

for labeling events under these categories can be applied arbitrarily. This is the case for categories such as “Presence of suspicious persons in the national territory,” “Drone sightings,” “Disruption of public order,” “Closure of public roads,” “Dissemination of false information for malicious purposes,” and “Intimidation, threats, and attacks against individuals.” Another feature that poses a direct risk is the app’s persistent prompting of users to share their geolocation.

Currently, the snitching feature channels these reports to the Bolivarian National Armed Forces (FANB), the Communal Militia Units, and the Popular Bases of Integral Defense.[93] These entities receive, process,



VenApp reporting interface. (Source: VenApp)

and eventually act on citizen complaints submitted through the application, within the framework of the so-called Territorial Defense System, which, according to official discourse, aims to strengthen the "defense of the people."[94] This formulation transformed what was originally marketed as an e-government channel into a mechanism that encouraged peer-to-peer surveillance, enabled geolocated reports of politically undesirable behavior, and normalized snitching as a civic duty.

In addition to the information explicitly captured by the reporting form, the VenApp platform includes trackers and embedded advertising in its code with identifiers associated with Google AdSense and Facebook, allowing not only for monetization by the website administrators of the traffic generated by citizens using the platform, but also for user profiling based on their browsing habits. This information can be used to personalize advertising and potentially to determine individual users' specific activities.

Originally, VenApp was available in app stores. However, it was removed from both the Google Play Store for Android devices and the App Store for iOS devices after August 2024, when the Venezuelan regime was openly promoting the app as a channel for doxxing demonstrators and opposition sympathizers. The app stores did not officially announce that that was the reason for the removal, but the timing was very telling. Since then, VenApp has focused on working as web application like other websites, with smaller efforts behind promoting installing the app manually.

Manually installing the app on Android devices outside the app store exposes users to additional risks. The procedure, known as sideloading, is considered unsafe for users because it involves installing software without the usual layers of verification, integrity checks, and updates provided by official app stores. With sideloading, users are more exposed to risks such as installing altered versions of the application with malicious code that facilitates unauthorized access to personal data, or an official version operating as a vector for monitoring or collecting sensitive information, without the available safeguards offered by the app store.

The logic underlying the design and use of VenApp does not arise in isolation, but rather aligns with the communication and organizational doctrine expressed in official documents such as the manual "Networks, Streets, Media, Walls, and Radio Bemba."[95] In this text, the digital space is conceived as a permanent front of political action, where surveillance, citizen monitoring, and reporting behaviors considered deviant or threatening are part of the "communication battle." This doctrine legitimizes the active participation of civil and community structures in observation and reporting tasks, normalizing the use of digital platforms as institutional channels for collecting information about citizens for political control.

Applications ecosystem

The Patria System and VenApp do not operate in isolation. Both platforms contribute to a broader data collection infrastructure for building comprehensive population profiles. This process unfolds without informed consent and through opaque interoperability mechanisms between different state institutions. Through the Patria System, the state collects a significant amount of sensitive information, including demographic and socioeconomic data, health records, bank and cryptocurrency transactions, records of state benefits, and affiliations with government-sponsored programs.[96] The Patria System interoperates with records from the National Institute of Transport and the Venezuelan Institute of Social Security, allowing for the automatic linking, verification, and updating of citizen data. The system's power lies not only in the volume of information it aggregates, but also in its integration capabilities, which enable the construction of individual or population-level profiles.

The Patria System's fundamental rights violation lies in conditioning access to essential goods and services on the provision of data for a population-wide surveillance system. In a context where hyperinflation and economic collapse have destroyed purchasing power and where approximately 80 percent of the population lives below the poverty line, state-controlled food distribution and subsidies give the ruling party

significant power over the population. By making access to these resources contingent on registration in a system that collects extensive personal data, monitors political behavior, and tracks social relationships, the state transforms basic needs into levers of political control. As primary caretakers in Venezuelan households, women bear disproportionate responsibility for accessing food through CLAP distribution programs, managing household finances, and maintaining family eligibility for social benefits.

The absence of comprehensive data protection legislation, combined with embedded tracking technologies and advertising identifiers in state applications, creates conditions for the systematic exploitation of citizens' data without meaningful consent or any recourse. Patria and VenApp both collect extensive information about users and their social networks, while simultaneously embedding commercial tracking technologies that profile users for advertising purposes. Citizens coerced into using these platforms have no practical ability to refuse tracking, no access to information about how their data is used or shared, and no legal mechanisms to demand accountability or rectification.

Other state-run digital applications linked to the Patria ecosystem include cryptocurrency and money transfers, point-of-sale payments, subsidized gas station payments, subscriptions to cash benefits, and subsidized food programs:

vePatria

Includes features for managing the most commonly used Patria System benefits and associated data collection requests. At the time of publication, this mobile app is only accessible within Venezuela and is not available in official app stores.

veQR

It Allows users to register their Patria Card, apply for discretionary cash handouts, and register to purchase subsidized food distributed by the CLAP program. It has also been used to facilitate participant registration for ruling party rallies.

veMonedero

Focuses on financial operations such as bank transfers and other transactions, including phone top-ups, and cryptocurrency transactions. This application allows you to send funds to family and friends and convert cryptocurrencies to the national currency.

vePDV

Focuses on information and transactions related to vehicle fuel. In addition to displaying available fuel quotas at subsidized prices, it includes a list and map of service stations near the user, along with their prices and fuel availability. It also enables payment for fuel refills through wallets registered in the Patria System.

vePOS

Focuses on point-of-sale functionality for businesses and service providers, allowing users to pay with funds they have in the Patria System Wallet.

Cyberpatrolling and social media surveillance

The persecution of critical expression in Venezuela relies on a progressively institutionalized digital monitoring apparatus that includes surveillance on open platforms. This practice intensified following the 2013 creation of the Strategic Center for Security and Protection of the Homeland (CESPPA), which promoted training for security forces including the Bolivarian National Guard in using social media as early warning systems against expressions deemed disruptive or contrary to the political order.[97]

The monitoring operates through systematic cyberpatrolling across social media platforms, including X, Instagram, TikTok, and Facebook, as well as private messaging spaces such as WhatsApp and Telegram. Publications, comments, hashtags, and interaction patterns are tracked by intelligence agencies—particularly the Bolivarian National Intelligence Service (SEBIN)—and used as evidence in criminal investigations. This monitoring extends beyond public figures or political leaders to ordinary citizens, journalists, activists, and community leaders, encompassing identification of critical accounts, monitoring of content histories, and surveillance of messages distributed in spaces perceived as private or semi-private, such as WhatsApp groups. The monitoring is complemented by the role of individuals who, willingly or under coercion, agree to serve as informants on the social media and WhatsApp activities of their neighbors and co-workers.

Following the July 2024 presidential elections, this type of monitoring appears to have intensified significantly, combining intimidation campaigns, arrests, and the strategic use of digital platforms as tools for surveillance and deterrence.[98] During this period, digital space became a direct extension of the state persecution apparatus, with VenApp and Telegram playing a role in the collection, systematization, and circulation of personal information about individuals identified as opposition supporters or electoral witnesses.[99]

This section examines the cyberpatrolling mechanisms and practices employed by Venezuelan security forces, the systematic doxxing and harassment campaigns targeting dissidents linked to Operation Knock Knock, patterns evident in arrests and prosecutions for expression on the Internet, and the resulting impacts on freedom of expression and assembly.

Cyberpatrolling and doxxing: the machinery of digital persecution

Venezuelan security forces conduct systematic cyberpatrolling across social media platforms and messaging applications to identify, track, and compile information on individuals expressing criticism of the government. This surveillance operates through multiple institutional channels, with SEBIN and the General Directorate of Military Counterintelligence (DGCIM) serving as the primary intelligence agencies, supported by regional and municipal police forces that conduct localized monitoring. Complementing these official operations, coordinated networks of accounts, trolls, and suspected bots simultaneously amplify pro-government narratives and harass dissenters.

These networks operate with apparent coordination across platforms, particularly on Telegram, where channels such as “Caza Guarimbas VE” (“Hunt Guarimbas VE”) systematically compiled and disseminate doxxing lists containing names, photographs, addresses, identification numbers, and other personal information of individuals identified as opposition supporters, protesters, or electoral observers. [100] [101] The compiled information facilitates subsequent arrests, harassment, and reprisals against identified individuals and their families. This practice intensified dramatically following the July 2024 elections, when Telegram channels became central repositories for personal data weaponized against perceived dissidents.

Operation Knock Knock ("Operación Tun Tun," named after the sound of knocking on doors) was relaunched on July 29, 2024, as a door-to-door arrest campaign following the disputed presidential election results. [102] The operation integrated multiple surveillance streams into a coordinated persecution mechanism, including reporting and doxing via VenApp and Telegram groups.

The operation functioned as both physical persecution and psychological warfare. Security forces posted over sixty-five audiovisual pieces associated with Operation Knock Knock, most of which featured identical typography and the slogan "Sin Lloradera" ("No Crying").[103] These materials exhibited two primary patterns: videos showing demonstrators at protests followed by footage of their capture and forced confessions, typically presented with mocking tones, sound effects, and animations of closing prison bars; and videos employing horror movie aesthetics—including music from films like Child's Play and Saw—accompanied by threatening messages and references to horror characters like Chucky and Jigsaw to maximize psychological impact.

Content originated primarily from Diosdado Cabello's television program Con el Mazo Dando and his associated social media accounts on Telegram and Instagram were subsequently reposted by other users and adopted by official security force accounts, including the Bolivarian National Police (PNB), DGCIM, and regional and municipal police forces. VEsinFiltro documented at least fifty-five arrest cases between July 2024 and January 2025 in which security forces used detained individuals for propaganda on social media, with twenty-seven explicitly linked to Operation Knock Knock through the use of its characteristic audiovisual elements or mentions in tags and descriptions.[104]

Many videos captured patrol cars arriving at citizens' homes, showing armed and hooded agents taking individuals to police headquarters. Close-up recordings forced detainees not only to confess to alleged crimes—typically "incitement to hatred," or "terrorism"—but also to apologize to the government and incriminate democratic political leaders. Documented cases include María Oropeza, coordinator for the political party Vente Venezuela in Portuguesa state, who livestreamed her arrest by DGCIM officers on August 7, 2024, as they broke into her home with crowbars without a court order.[105] The public exhibition of arrests, forced "confessions," and severe charges reinforces the intimidating logic and promotes self-censorship among the broader population.[106]

Prosecution patterns for internet expression

Since 2020, there has been a noticeable trend of criminal prosecutions against journalists and ordinary citizens as direct consequences of personal expressions shared in digital environments. These cases reveal consistent patterns of how the Venezuelan regime weaponizes digital surveillance against freedom of expression. Analysis of documented cases reveals several recurring patterns.

First, investigations originate from systematic digital surveillance rather than traditional investigative procedures, with cyberpatrolling serving both as the catalyst for criminal investigations and their primary evidentiary foundation. Prosecutors rely heavily on decontextualized digital content—publications, messages, images, and videos—reinterpreted through a criminal lens, without contextual analysis or evidence of concrete harm or a direct causal relationship to verifiable material facts. Evidentiary assessment rests principally on declarations from police officials who participated in cyberpatrolling and digital content review, and lack specialized technical reports, independent forensic analysis to conclusively establish authorship, or proper chain-of-custody procedures for digital evidence. The case of Juan Francisco Alvarado—a journalism student detained on March 20, 2025, and subsequently sentenced to fifteen years in prison for alleged incitement to hatred—exemplifies this use of cyberpatrolling as a tool for criminalizing online expression. According to judicial records, the criminal investigation centered on broad and prolonged monitoring of his digital activity across multiple platforms, without clear delineation of technical criteria, time period, or specific legal basis.[107]

Second, authorities apply vague and expansive criminal provisions—particularly "incitement to hatred" under the Law Against Hatred, for Peaceful Coexistence and Tolerance, along with charges of terrorism, treason, conspiracy, and attacks on honor and reputation—without clear criteria for proportionality, actual harm, or intentionality. This allows criminalization of opinions, citizen complaints, or political assessments that constitute legitimate public debate. Women face particular vulnerabilities in this system: Marggie Orozco, a sixty-five-year-old physician, received a thirty-year prison sentence for disseminating a WhatsApp audio criticizing government management and calling for electoral participation, following denunciation by community council members who had previously subjected her to harassment and threatened to exclude her from social benefits.[108] Similarly, Randal Glendysmar Telles Peña, a twenty-two-year-old woman, was sentenced to fifteen years for posting a critical TikTok video, with DGCIM officers locating and arresting her at her workplace.[109] Nakary Mena remains the sole woman journalist imprisoned in Venezuela for her professional work.[110]

Third, surveillance extends into semi-private communication spaces with community reporting mechanisms transforming neighbors into informants. Multiple documented cases involve arrests stemming from WhatsApp group messages or voice notes shared in community contexts, including Marcos José Palma Martínez, sentenced to fifteen years for distributing a critical audio in a community WhatsApp group.[111]

Fourth, military personnel face particular vulnerability: Jesús Gabriel Molina Sifontes, an active National Bolivarian Armed Force officer, received an eight-year sentence for disobedience and incitement to rebellion after publishing a WhatsApp status featuring Venezuela's seven-star flag[112]—an image reported by a superior officer to DGCIM despite absence of criminal elements.[113]

Fifth, arrests frequently occur without judicial orders, preceded by threats and accompanied by prolonged periods of incommunicado detention and denial of legal representation. Detention sites include SEBIN headquarters, DGCIM facilities, and National Bolivarian Guard commands, all with severely restricted visitation. Journalist Rory Branker, editor of digital media outlet La Patilla, was detained on February 20, 2025 after sharing an image related to US government rewards offered against senior Venezuelan officials.[114] Branker was released on February 4, 2026, after enduring arbitrary transfers and prolonged forced disappearance.

Sixth, procedural violations pervade prosecutions: the absence of independent technical expertise, the lack of forensic protocols to validate the authenticity of digital evidence, the denial of adequate defense, the application of military jurisdiction to civilians, and the imposition of disproportionate sentences that are disconnected from the alleged offense severity. The October 2024 report by the United Nations Independent International Fact-Finding Mission on Venezuela documented the case of Whilfer Piña Azuaje, a political activist detained after allegedly posting a threat against then-President Maduro in a WhatsApp status. Authorities announced the seizure and "extraction" of his mobile phone, with charges including conspiracy, criminal association, and attempted assassination—based solely on a social media message.[115]

Finally, public dissemination of arrests through propaganda videos serves as an example and a deterrent. Security forces broadcast detention footage, forced confessions, and severe criminal charges to reinforce that the state observes, identifies, and punishes dissent in even its most quotidian forms.

Impacts on freedom of expression and association

The convergence of digital surveillance, selective prosecution, and arbitrary detention has generated profound impacts on freedom of expression in Venezuela. These effects constitute not isolated episodes of censorship but rather a communicational environment marked by fear, self-restraint, and a progressive reduction of civic space.

One of the most widespread consequences is the normalization of self-censorship. The real possibility that a publication, audio, or message—even disseminated in closed or community spaces—may result in criminal proceedings, detention, or reprisals has led broad sectors of the citizenry to moderate their language, avoid sensitive topics, or completely abstain from opining on matters of public interest. This preventive silencing occurs in a context of legal uncertainty, where no clear criteria exist for what type of expression may be considered criminal. Discretionary application of broad criminal provisions reinforces perceptions of permanent risk and transforms digital expression into a potentially dangerous activity.

For journalists and activists, the described mechanisms have led to forced displacement, both internal and transnational. Fear of arbitrary detention, prolonged imprisonment under severe conditions, and family persecution have compelled hundreds to abandon their communities, jobs, and social networks. This forced displacement not only affects individuals but also weakens civil society's organizational capacity.

Community reporting mechanisms and induced denunciations generate additional chilling effects on social cohesion and collective action. The possibility of denunciation by a neighbor, community council member, or acquaintance transforms social interaction into a terrain of suspicion, weakening community cohesion and collective action.

Detentions, convictions, and criminal proceedings for digital expressions additionally serve exemplary and disciplinary functions. Public dissemination of arrests, severe charges, or recorded "confessions" reinforces the idea that the state observes, identifies, and punishes dissent even in its most everyday forms. This effect requires no massive persecution to prove effective: visible cases with disproportionate sanctions produce a generalized inhibitory impact.

Private telecommunications interception

Private telecommunications interception represents one of the most intrusive components of Venezuela's surveillance apparatus, directly violating the private communications of millions of citizens through systematic and widespread practices that far exceed any legitimate law enforcement justification. Venezuela's constitutional and legal framework nominally protects communication privacy through multiple overlapping provisions. Article 60 of the Constitution of the Bolivarian Republic of Venezuela (CRBV) guarantees every person the right to protection of their private life and ensures the right to access information regarding oneself gathered by the state, while mandating data collection respects privacy.[116] [117] The Organic Law on Telecommunications (2000) establishes that telecommunications interception requests can only be undertaken after prosecutors obtain court approval in pursuit of a criminal investigation.[118] The 1991 Law on Protection of Communication Privacy stipulates that private communications can only be intercepted by judicial order under limited circumstances, including crimes against state security, public patrimony, narcotics, kidnapping, and extortion. However, the vast disparity between legal protections and documented practice reveals systematic disregard for statutory limitations and international human rights standards.

Unlike other surveillance methods, such as CCTV cameras or drone monitoring, telecommunications interception typically leaves no evidence that affected individuals can detect or document. Understanding the scale and nature of these practices requires distinguishing between content interception (the actual substance of the communication, including call audio, message text, and internet traffic) and metadata collection (information about communications, including phone numbers, timestamps, duration, and location data), as the privacy violations and surveillance capabilities differ substantially between these categories.

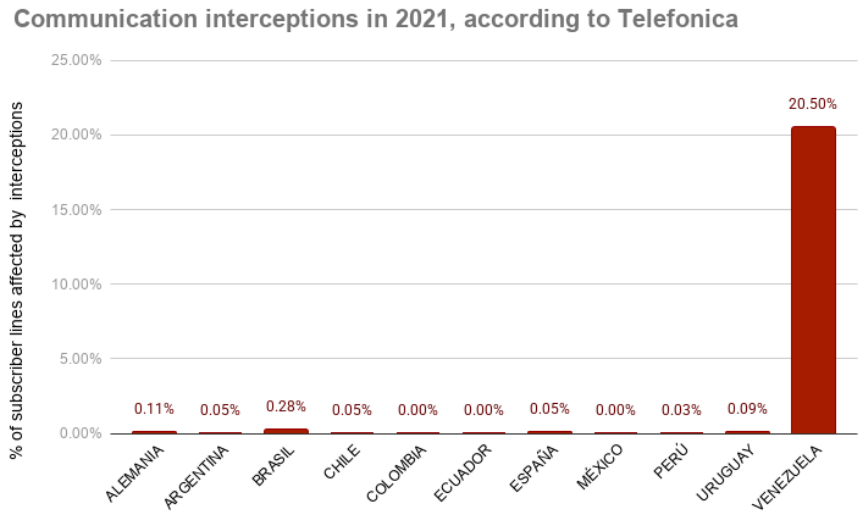
The following sections analyze telecommunications interception at a massive scale, the migration of vulnerable populations to encrypted messaging applications that reduce traditional interception effectiveness, internet traffic surveillance capabilities deployed by state-owned telecommunications provider CANTV, location tracking through both provider cooperation and unauthorized IMSI catcher devices, and the human rights impacts of this pervasive surveillance on Venezuelan civil society.

Private telecommunications interception at scale

Since 2011, private phone calls of journalists and politicians have been routinely recorded and subsequently broadcast on state media, often edited or manipulated for incrimination purposes, demonstrating systematic disregard for legal protections.[119] Venezuelans have been reporting "tapped calls" and intercepted SMS messages since as early as 2007, but these remained largely anecdotal accounts difficult to verify systematically. A critical breakthrough occurred in 2021, when Telefónica, the Spanish parent company of Movistar Venezuela, published quantitative data in its transparency report. The report revealed that during 2021, Movistar facilitated the interception of communication content from more than 1.5 million subscriber lines—approximately 21 percent of Movistar Venezuela's total subscriber base.[120] Telefónica's data disclosure encompassed calls, messages, cellular location, and internet traffic without disaggregating specific interception types.

This interception rate is alarmingly disproportionate and difficult to reconcile with strictly exceptional, individualized, and proportionate use in serious criminal investigations. In other Telefónica markets across Latin America and Europe, the percentage of intercepted lines did not reach one percent of subscribers. Venezuela's interception rate thus exceeded that of comparable markets by more than twentyfold, indicating systemic abuse rather than targeted law enforcement activity. The scale demonstrates substantial governmental investment in processing massive volumes of data gathered by this surveillance apparatus.

Share of Telefonica and its subsidiaries subscriber lines affected by telecommunications interception in 2021 by market, based on data published by Telefonica. (Source: VEsinFiltro[121])



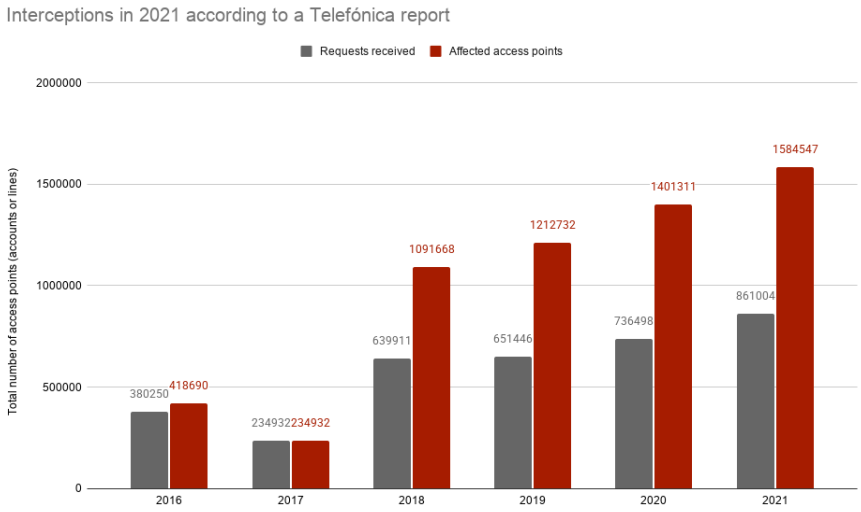
The progression of interceptions over time reveals escalating governmental surveillance ambitions. The number of subscriber lines affected by interceptions increased sevenfold between 2016 and 2021, rising from 234,932 lines to 1,584,547.[123] This significant expansion occurred during a period of intensifying political repression following the 2015 opposition electoral victories and accelerated through the 2017 constitutional crisis and popular unrest, suggesting a correlation between surveillance expansion and authoritarian consolidation.[124]

Data on governmental interception orders disappeared from subsequent Telefónica transparency reports following the 2021 publication, preventing continued public monitoring of this abuse. However, the 2021 report provided a critical window into practices that are almost certainly continuing at other Venezuelan telecommunications operators that have never published comparable transparency data.

Movistar also delivered metadata from 13 percent of its subscriber lines during 2021, providing authorities with information about communication patterns, contact networks, subscriber information and location history, even when actual communication content was not intercepted.[125] [126] This metadata surveillance can enable sophisticated analysis of social networks, identification of organizational structures, and tracking of individual movements—capabilities particularly valuable for political surveillance targeting civil society organizations, opposition movements, and independent journalists. The cumulative impact of both content and metadata interception affected approximately one-third of Movistar's subscriber base, creating pervasive surveillance that fundamentally altered how Venezuelans communicate.

The intercepted data became accessible to an extraordinarily broad and poorly defined list of "competent authorities" that contradicted both Venezuelan legal protections and international human rights standards. Movistar Venezuela's transparency report specified that interception requests did not require judicial orders but could be submitted by the Public Ministry (General Prosecutor's office), CICPC (Venezuela's main criminal investigations agency), Servicio Bolivariano de Inteligencia Nacional (SEBIN), police forces qualified to conduct criminal investigation, components of the Bolivarian National Armed Forces, police intelligence authorities, the National Bolivarian Police, any other auxiliary criminal investigation or other special penal investigation entities, and inexplicably, the National University of Security (UNES).[126]

Number of interception requests and the number of subscriber lines affected by telecommunications interception by year, based on data published by Telefonica. (Source: VEsinFiltro)



This expansive authorization structure created conditions for indiscriminate interception and abuse by authorities operating outside Venezuelan legislation and international standards. The inclusion of university security training institutions among entities authorized to request telecommunications interception particularly highlights the absence of any meaningful oversight or proportionality assessment. In a context of documented political persecution, this uncontrolled access to private communications enables systematic human rights violations.[127]

State-owned telecommunications providers likely facilitate surveillance at rates comparable to or higher than Movistar's. CANTV, which operates as both the preeminent residential internet service provider and a major mobile carrier (Movilnet), is not subject to independent oversight and is under direct governmental control. Phone records remain accessible to prosecutors without judicial authorization.

Migration to messaging applications

The migration of Venezuelan communications from traditional cellular calls and SMS to encrypted messaging applications represents a significant defensive adaptation by populations vulnerable to surveillance. While cellular phone calls remain a common communication method, audio and video calls via WhatsApp and Signal have increasingly replaced traditional telephony, particularly among activists, journalists, opposition members, and civil society organizations aware of interception risks. This migration substantially limits the intelligence value that telecommunications interception can yield beyond geolocation data and other metadata, as end-to-end encrypted messaging platforms prevent access to content even when telecommunications providers cooperate with surveillance requests.

WhatsApp's encrypted messaging has become the most extensively used digital platform in Venezuela, with nearly fifteen million users—more than half the country's population—connecting daily.[128] The platform serves as a primary communications infrastructure for ordinary citizens' everyday business, and increasingly for political news consumption. The shift of public debate from open social media platforms to semi-private WhatsApp groups arose in response to both economic factors (reduced data consumption) and political considerations (a lower risk of immediate retaliation). Public debates have migrated to WhatsApp groups where political leaders, journalists, human rights defenders, social activists, and academics interact with reduced exposure risk, as the platform's encrypted and private chats theoretically protect conversations from direct governmental surveillance.

However, telecommunications interception can still compromise encrypted messaging platforms by exploiting SMS-based authentication systems, as the report covers in the following section on communications infiltration. Many messaging platforms use SMS verification codes to verify phone number ownership and secure accounts, creating a vulnerability when telecommunications providers facilitate SMS content interception. The persistence of SMS-based authentication vulnerabilities undermines the security otherwise provided by encrypted messaging apps and other online platforms. Organizations operating under maximum surveillance conditions increasingly recognize this weakness, using two-factor authentication PINs in messaging apps, and in other platforms app-based codes or physical FIDO keys for two-factor authentication rather than SMS codes. Yet the technical sophistication required for these protective measures, combined with limited digital literacy resources and unreliable internet connectivity, creates asymmetric vulnerabilities, leaving the most at-risk populations without the capacity to implement effective defenses.

Internet traffic surveillance

Beyond intercepting traditional telecommunications, Venezuelan authorities possess capabilities to conduct internet traffic surveillance, manipulation, and censorship. CANTV, the state-owned telecommunications provider operating as Venezuela's preeminent residential Internet service provider, has deployed advanced networking equipment capable of analyzing traffic, implementing Internet censorship, manipulating and altering traffic, and monitoring unencrypted Internet communications. The full extent of this traffic surveillance capability remains unclear, but documented incidents indicate it has been deployed against politically sensitive targets.

The technical capabilities of the state-owned CANTV provider, combined with the complete lack of independent oversight, create an environment in which comprehensive Internet surveillance can occur without public documentation or accountability. CANTV's manipulation of network traffic to support phishing attacks—described in the cyberattacks section of this report—is enabled by advanced network equipment also used to analyze Internet traffic. This equipment is designed to facilitate sophisticated Internet censorship, alter traffic, or surveil unencrypted Internet communications. It remains unclear whether this type of network traffic surveillance is currently in use and to what extent.

Private Internet service providers face intense pressure to cooperate with surveillance requests, given the regulatory authority of CONATEL (the National Telecommunications Commission) over licensing, spectrum allocation, and operational permissions. While the Telefónica transparency report included Internet traffic in its interception statistics without providing a clear breakdown by request type, the lack of granular data makes determining whether Venezuelan authorities systematically requested or received Internet traffic content from private providers impossible to ascertain definitively.

Location tracking and IMSI catchers

Location tracking through telecommunications infrastructure represents a distinct but related surveillance capability that Venezuelan authorities may deploy strategically. The Criminal Processing Code's mandate that telecommunications and financial institutions maintain 24/7 availability to "process and provide the location registry of citizens" creates a permanent, real-time tracking infrastructure accessible to a broad range of authorized entities.[129] The telecommunications interception data that can be requested by Venezuelan authorities include cellular location information generated whenever mobile phones connect to cell towers. Such data can enable detailed movement records revealing information about individuals' associations, activities, visits to sensitive locations, and relationships inferred through repeated co-location patterns.

Beyond this authorized telecommunications provider cooperation, technical evidence indicates deployment of unauthorized cellular surveillance devices known as IMSI catchers, Stingrays (after a prominent manufacturer), or cell-site simulators. These devices impersonate legitimate cell towers, causing nearby mobile phones to connect to them, thereby directly revealing which phones are present in a geographic area. This technology enables locating specific individuals within limited areas and potentially intercepting call content and text messages occurring in proximity to the false antenna, all without cooperation or knowledge from the telecommunications provider.22 Unlike historical location data that reconstructs past movements, real-time location access enables dynamic surveillance. Security forces can utilize this capability to track targets' locations, determine who was present at specific events, or identify individuals meeting with particular persons of interest.

The Fake Antenna Detection Project (FADe) documented technical evidence of cellular antennas exhibiting inconsistencies, suggesting they were false, in Caracas and along the Venezuela-Colombia border during an investigation conducted in 2019.[130] While observed technical evidence cannot always definitively identify the operator or intention behind each anomalous antenna, the false antennas appeared concentrated at strategically significant security locations, including Fuerte Tiuna (Venezuela's primary Army base where Maduro was captured), the central square Plaza Venezuela, vehicular access points to Caracas, and airports.[131] These locations strongly suggest deployment by security institutions to obtain direct, real-time location and communications data, possibly by specialized units within the security forces stationed at these sites.

Unlike telecommunications interception facilitated by provider cooperation, IMSI catcher operators maintain continuous, real-time, direct access without relying on external entities, waiting for response processing, or facing even the remote possibility that a request might not be processed. This autonomous capability provides tactical advantages for time-sensitive operations, including arrests, surveillance of high-value targets, or monitoring of sensitive locations. The concentration of anomalous antennas at military installations, transportation hubs, and protest-prone areas suggests operational deployment aligned with regime protection priorities rather than general law enforcement purposes.

Cyberattacks, infiltration, and malware

Venezuela's legal framework provides nominal protections against cybercrimes and unauthorized access to communications, but systematic violations by state actors render these safeguards meaningless in practice. The 2001 Special Law Against Informatic Crimes established criminal penalties for unauthorized access, interception of communications, and improper disclosure of personal data, with imprisonment ranging from three to five years for violations.[132] The 1991 Law on Protection of Communication Privacy reinforced inviolability principles, requiring judicial authorization for any interception and limiting lawful surveillance to specific crimes, including threats to state security, narcotics trafficking, and kidnapping.[133] However, these protections exist only on paper. Venezuela lacks comprehensive data protection legislation that aligns with international standards, and the 2021 Transparency Law—rather than guaranteeing accountability—further entrenched government secrecy and impunity.[134] The judiciary's subordination to executive power eliminates meaningful oversight of surveillance activities, while security forces regularly compel citizens to delete content or extract data from devices without legal authorization.

This regulatory vacuum enables systematic deployment of sophisticated cyberattacks against dissidents, journalists, and civil society organizations. Beyond mass telecommunications interception conducted with telecommunications provider cooperation, Venezuelan state actors employ stealthy techniques to access private communications and track targets, including phishing campaigns to compromise online accounts, unauthorized infiltration of organizational platforms containing sensitive information, and account takeovers of messaging applications. These operations frequently coordinate with disinformation campaigns and internet censorship infrastructure, amplifying their impact through simultaneous attacks on multiple fronts. The scale and sophistication of documented incidents demonstrate a deliberate state policy rather than isolated criminal activity.[135]

This section examines three categories of cyberattacks and digital intrusion techniques employed against Venezuelan civil society. The first subsection documents state-sponsored phishing operations, including mass-scale campaigns targeting opposition volunteer initiatives —Voluntarios por Venezuela, Héroes de la Salud, and electoral organizing units called comanditos—as well as targeted attacks against journalists and high-value individual targets. These campaigns combine technical sophistication with coordination across multiple government entities, demonstrating systematic rather than opportunistic targeting. The subsequent section analyzes unauthorized access to sensitive platforms and messaging accounts, including documented cases of account takeover exploiting telecommunications interception capabilities. The third section addresses spyware deployment, examining Venezuela's persistent efforts to acquire commercial surveillance tools and the limited but concerning evidence of their active use against human rights defenders.

Phishing targeting journalists and pro-democracy activists

Phishing represents the most common and best-documented category of state-sponsored cyberattacks in Venezuela.[136] Attacks clearly attributable to government actors have used fake websites that mimic opposition initiatives to identify activists, volunteers, and dissidents at scale, leaving technical traces that enable definitive attribution to state infrastructure. In many documented cases, exposed individuals face public identification as punishment, intimidation of others who might participate in similar initiatives, and deliberate erosion of trust in opposition organizations—objectives achieved through coordinated disinformation campaigns amplifying the stolen data.

Volunteers for Venezuela

In February 2019, during the constitutional crisis following Juan Guaidó's oath as interim president, the opposition announced a volunteer initiative to channel humanitarian aid into Venezuela. VE sin Filtro detected a large-scale phishing campaign targeting individuals attempting to register at voluntariosxvenezuela.com. The operation's primary objective was to capture personal information from citizens who believed they were registering with the legitimate portal. The attack required coordination among internet censorship apparatus, disinformation networks, and multiple state entities.[137]

The attack involved a combination of typosquatting, internet censorship, and a coordinated social media campaign. It exploited users' confusion about how to access the legitimate site, directing them to a malicious URL. This fraudulent website was almost identical to the original, using the domain voluntariosvenezuela.com instead of the legitimate voluntariosxvenezuela.com.

The sophisticated technique employed by CANTV—Venezuela's state-owned primary residential Internet service provider—was DNS response injection. Through traffic manipulation, CANTV intercepted DNS queries from user devices seeking the legitimate site's IP address and forged responses that directed them to malicious infrastructure.[138] This exceeded the capabilities of simple DNS spoofing, affecting any DNS request for voluntariosxvenezuela.com, including those from users employing public DNS resolvers (Google, Cloudflare, and Quad9), private resolvers, or direct IP addresses. The manipulation occurred via middlebox equipment within CANTV infrastructure inspecting all outbound traffic from the ISP.

Direct attribution to CANTV was possible through documentation of sophisticated DNS injection techniques that require control of telecommunications infrastructure. The investigation also documented CONATEL (National Telecommunications Commission) involvement through evidence in WHOIS registry records for multiple domains used during the phishing operation and through the institution's response to the incident.[139] The investigation documented that other phishing sites were operated by the same actors and had previously been used to steal credentials for Gmail, Twitter (now X), Facebook, and Hotmail, among other services. These phishing domains were registered using a pseudonym associated with telephone numbers belonging to official CONATEL lines.

When the attack was exposed on social media, registrant information was modified on the public WHOIS records at NIC.ve. The coordination among the censorship apparatus at critical moments when the phishing operation was suspended and reactivated using different domains, combined with coordination with state-aligned disinformation portals and networks, further evidenced state orchestration.

The public exposure of thousands of phishing victims occurred in a context where political affiliation disclosure carries material risks of discrimination and reprisals, including the historical precedent of the Tascón List used for systematic political discrimination during the Chavez administration from 2004 to 2012.[140] Beyond undermining confidence in opposition leadership, the campaign deliberately generated fear and sought to discredit journalists and digital researchers, including this report's co-author, Andrés Azpúrua.[141]

The attack combined ISP-level network interference with mass data capture in an environment with a documented history of political discrimination and reprisals. It simultaneously restricted civic space and violated the rights to privacy, freedom of association, and political participation, while creating powerful chilling effects.

Healthcare Heroes

On March 26, 2020, CANTV deceived users by injecting malicious DNS responses that targeted the websites heroesdesaludve.info and saludvzla.com. This manipulation directed individuals seeking to visit these sites to counterfeit replicas designed to capture their personal information.[142] Many users may have arrived at these malicious sites after clicking on links shared through various channels.

The legitimate initiative, launched by Guaidó's interim administration, aimed to provide financial assistance to healthcare workers who were facing challenging conditions due to the pandemic, as well as addressing the issue of persistently low public-sector wages. According to VE sin Filtro, tens of thousands of people likely submitted their information to the cloned website, considering the extensive reach and mobilization of the campaign, along with CANTV's significant share of Venezuelan internet traffic.

Grassroots electoral organizing units (Comanditos)

During the 2024 presidential election campaign, a phishing operation targeted opposition sympathizers and volunteers seeking to register comanditos—local groups for electoral mobilization. The operation distributed a fake registration form promoted by fraudulent social media accounts and messaging channels using the malicious shortened link bit.ly/Comandito instead of the legitimate bit.ly/Comanditos.[143]

The operation employed typosquatting, using nearly identical links to induce mistaken behavior, and delivered registration forms that obscured URL differentiation. Resource cloning deployed the form via the legitimate Google Forms platform, exploiting widespread trust in the platform and the difficulty of identifying its origin through URL inspection alone. Network and group amplification relied on X, Instagram, TikTok, and Telegram accounts that promoted the malicious link, posed as opposition supporters, and engaged in other disinformation activities.

The malicious link redirected to a replica of the original form hosted on Google Forms. The fraudulent form requested personal information and forced the collection of users' email addresses, adding an extra yes/no question: "Would you support street activities?" This suggests interest in profiling victims willing to participate in protests.

Cazadores de Fake News identified a network of at least forty-five fake accounts on X, controlled by pro-government actors and active since 2023, that participated in this phishing attack by promoting the malicious link to deceive followers of the opposition campaign and expose them by registering through the fake form.[144]

The phishing exposed identities of volunteers and sympathizers while enabling political profiling. The additional question on "street activities" indicates the mapping of protest disposition for potential reprisal. Beyond privacy violations, the operation attacked Venezuelans' rights of association and sabotaged electoral organizing.

Journalists and other high-value targets

Over the years, there have been several phishing cases targeting journalists and civil society organizations seeking to obtain access credentials for email accounts, social media, and WhatsApp. These attacks originate from various malicious actors, including those associated with the regime. Regime-associated actors have used phishing and other techniques to access email accounts, then disclose their contents via official media outlets or social media accounts to publish pro-regime messages or discredit opposition figures.

Over a single weekend in September 2024, Espacio Público documented two targeted phishing attacks. On September 14 of that year, journalist Andrés Rojas Jiménez received phishing messages seeking his Instagram credentials, according to an Espacio Público report.[145] The same publication reported that actress and writer Prakriti Maduro was targeted by a phishing attack on September 12, resulting in the loss of access to her X account. This attack occurred after she shared testimonies about arbitrary detentions that other users sent her via X direct messages in the context of post-electoral protests.[146]

Recent phishing attacks against journalists and other civic actors have increasingly failed due to greater awareness, the adoption of two-factor authentication, and rapid response mechanisms in collaboration with organizations that provide digital security support. Nevertheless, phishing attempts against certain high-profile figures remain persistent.

Unauthorized access to accounts and other cyberattacks

Obtaining unauthorized access to the email accounts of civil society members is a recurring practice, also targeting politicians, journalists, and activists. As indicated above, targeted phishing has frequently been used to gain unauthorized access to accounts and to take over social media profiles, but other hacking attacks have also been documented by VEsinFiltro.

Unauthorized access to email and social media accounts

In other instances, harassment campaigns by online government-aligned social media figures and user networks preceded attempts to gain access to accounts, presumably by the same pro-government actors. In one such case from December 2025, an Internet user from the central state of Aragua had their posts on X commenting on US-Venezuela tensions trigger a harassment campaign by government propagandists, quickly leading to veiled threats and doxing. Harassment that started on X quickly reached other social media platforms, WhatsApp, and phone calls. Actors connected to harassers attempted to gain access to the victim's X and Gmail accounts.[147]

A notable example of a targeted attack involved journalist Nelson Bocaranda in 2016. In this incident, attackers gained control of his Twitter (now X) account and accessed sensitive direct messages while Bocaranda was disclosing information from anonymous government sources. To execute the attack, state-linked actors obtained a new SIM card for Bocaranda's Movistar phone line. This allowed them to receive verification codes via SMS they used to gain access and change the account's password. The attackers' acquisition of a new SIM card caused Bocaranda's line to stop working on his phone; he subsequently had to request a new SIM card to regain access to his number.[148]

Messaging app account takeover

Cases of theft of WhatsApp accounts belonging to activists and human rights organizations have been documented. Although inconclusive, the evidence suggests that telecommunications interception may have been used to access them. This occurs in a local context where WhatsApp account theft is common in phishing operations with criminal objectives, typically to scam the family and friends of the account theft victim. It is possible that government operations have been disguised to simulate criminal account-theft schemes to camouflage state action.

In a 2021 case documented by Conexión Segura y Libre, a nongovernmental organization lost control of its WhatsApp account for several hours, which it had used to communicate with victims of human rights violations. Individuals operating the phone asserted they received no request for registration codes and did not fall victim to phishing. The incident occurred during a critical moment in the International Criminal Court prosecutor's pre-trial investigation of Venezuela. This incident was likely perpetrated by state actors who requested SMS message content from the mobile operator to register a WhatsApp account on a device under their control.

In a case from May 2023, human rights activist Lourdes Ruiz, while suffering systematic harassment from police forces, experienced unauthorized access to her Instagram account and the takeover of her Signal account by unknown actors, as well as repeated attempts to access one of her email accounts over a period of several days. Ruiz had been receiving intimidating calls from security forces and believed her phone line

was being monitored because of her work documenting human rights violations in detention centers. Ruiz indicated that she had stopped using Signal at the time and did not have the app installed. She also maintained that she did not receive any message with a code to register a Signal account. Ruiz asserted that the Signal account with her phone number was stolen and used to send intimate images of her, obtained from Instagram or one of her email accounts, to at least one person known to her in the human rights community. It is unknown whether the images were sent to other contacts.[149]

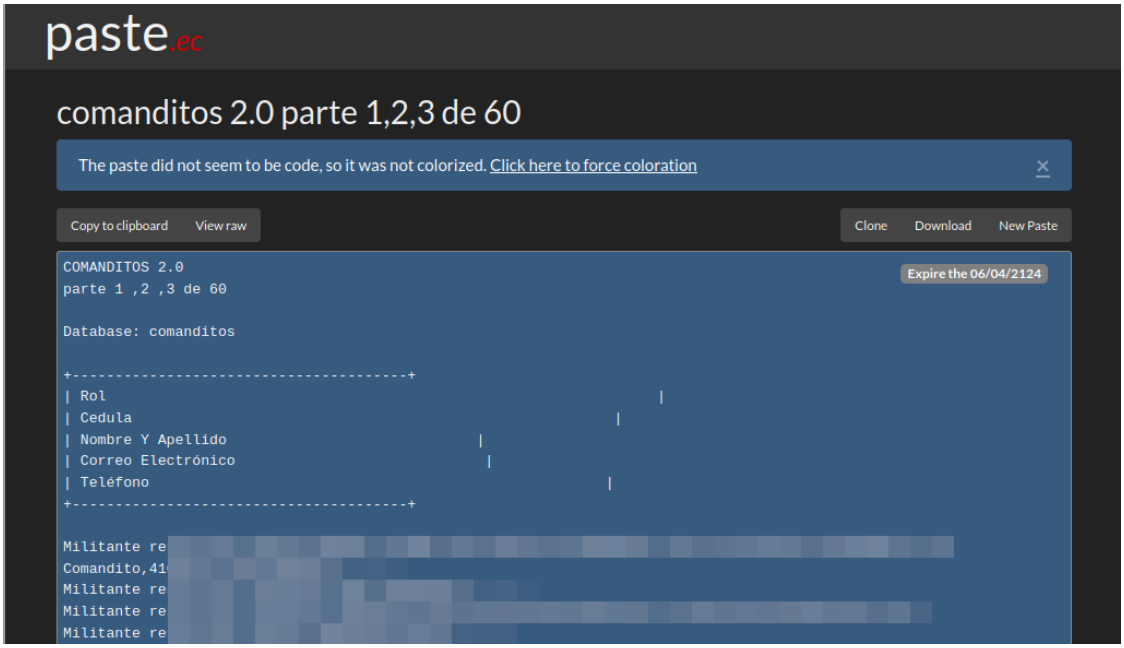
Unauthorized access after detentions

In some cases, individuals jailed or subjected to short-term detention have had their accounts compromised shortly after release, sometimes after repeated attempts. These attacks were likely facilitated by credentials or devices obtained during interrogations.

In two cases from December 2025, individuals who had been jailed lost control of their online accounts either during detention or shortly afterwards. In one case, the targeted individual lost access to their Facebook account and experienced multiple unsuccessful login attempts by other actors. These situations are difficult to resolve because of detention conditions, devices permanently seized by authorities, and phone numbers configured for account recovery that were either abandoned in Venezuela before a rapid departure or suspended by the phone line provider for lack of use.

Hacking of databases

Both victims and perpetrators of cyberattacks against strategic databases frequently prefer not to publicize incidents. A significant case with strong indicators of state-associated actor participation was the unauthorized access and partial disclosure of contents from the Primero Justicia party's internal member platform during the 2024 presidential campaign.

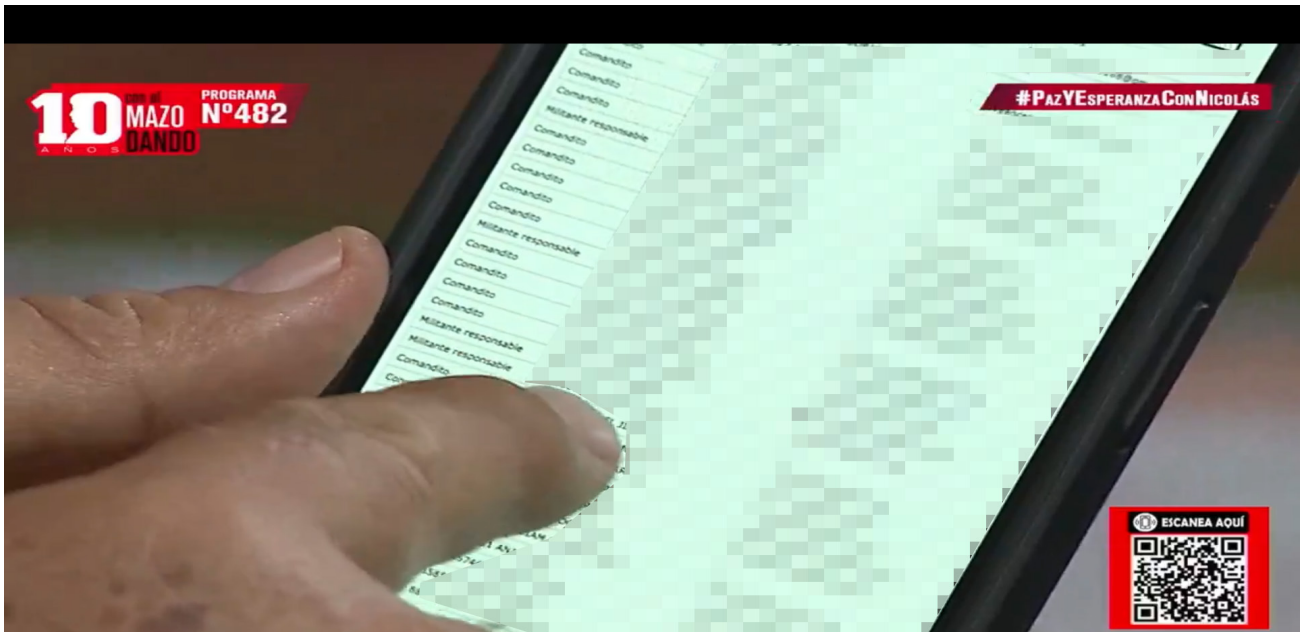


Screenshot of one of the documents shared by the account X @LaListaMachado showing the internal registry of political party members, June 27, 2024. Image edited for privacy protection. (Source: @LaListaMachado Certainty about how actors gained initial unauthorized access to the National Registry of Militants of the political party Primero Justicia and to its SORE database remains absent, and definitive attribution is not possible. VE sin Filtro confirmed that credentials exposed on social media did successfully authenticate to Primero Justicia's internal party platform and provided access to information collected from comanditos.com, matching data disclosed by Diosdado Cabello on television.

On June 26, 2024, Diosdado Cabello, current Minister of Interior Relations, Justice, and Peace, claimed on his program Con El Mazo Dando that the website comanditos.com had suffered a hack and database leak, displaying on camera a list with citizens' personal data, including names, national identity numbers, and email addresses.[150] Cabello also stated, "The confidentiality of your data has been given up by María Corina (Machado) and her combo," repeating a common disinformation narrative the government deploys during phishing campaigns.[151] The website comanditos.com was created and administered by the opposition party Primero Justicia as part of efforts to register volunteers during the presidential campaign, operating in parallel with registration coordinated by the opposition campaign command and the Vente Venezuela party, led by María Corina Machado. Both comanditos efforts functioned independently within the democratic coalition.

The anonymous X account @LaListaMachado claimed to possess the leaked data. As in other instances, parallel narratives mixed hacking and leaking as data sources.[152] [153] In subsequent days, the account published extensive excerpts from databases obtained from the Primero Justicia Party's Electoral Organization and Registration System (SORE), including comanditos members, party membership lists, and login credentials for some users with their passwords.

Certainty about how actors gained initial unauthorized access to the National Registry of Militants of the political party Primero Justicia and to its SORE database remains absent, and definitive attribution is not possible. VE sin Filtro confirmed that credentials exposed on social media did successfully authenticate to Primero Justicia's internal party platform and provided access to information collected from comanditos.com, matching data disclosed by Diosdado Cabello on television.[153]



Con El Mazo Dando broadcast #482, June 26, 2024. Image edited to protect the privacy of the people appearing on the leaked list.

This incident not only represents a privacy violation for citizens whose data was leaked, but also manifests broader concerns about political rights, freedom of association and digital rights in the Venezuelan political context. Additionally, information manipulation related to leaks is used to fabricate criminal charges or defame the victims publicly by governmental figures, including Diosdado Cabello, showing a pattern of persecution and delegitimization of opposition parties.

Elusive signs of spyware deployment

The use of spyware on mobile devices and computers belonging to state intelligence targets has grown dramatically worldwide, including in Latin America. Spyware typically accesses microphones, cameras, device content including messages, and real-time location, bypassing privacy protection measures such as encrypted communications because it runs directly on devices where these messages are sent or received. Full identification of any commercial spyware family's use by Venezuelan authorities has not been possible. However, individual cases, repeated and documented interest in acquiring spyware, and multiple investments in other digital surveillance systems all point to its use by Venezuelan state.

For years, Venezuela has sought to acquire sophisticated spyware from various companies. However, researchers have not been able to verify whether purchases were ultimately executed. Indeed, the commercialization of spyware is surrounded by secrecy, obfuscation, and intermediaries. It is reasonable to assume that companies commercializing these tools are especially interested in hiding contracts when dealing with countries sanctioned for widespread human rights violations or sales that could negatively impact them in high-value markets, including the United States and the European Union.

Between 2014 and 2015, Citizen Lab found evidence of infrastructure in Venezuela used to host command-and-control servers for FinFisher spyware, even though Venezuela was not mentioned as a client in a leak experienced by the company.[154] The command-and-control server for FinFisher spyware identified in Venezuela by Citizen Lab in its 2015 report was apparently located in Caracas. The finding was made possible by discovering a proxy server with software from the same company configured to anonymize and obfuscate the location of the server that controls spyware instances. This set of servers was operational between December 2014 and October 2015. Its existence indicates that FinFisher was used by Venezuelan authorities, or at a minimum, that a field demonstration was conducted.

In 2015, a leak from the now-defunct company Hacking Team exposed multiple conversations between the company and the Chávez government, and subsequently Nicolás Maduro's government.[155] In leaked emails, VenTech—a company with offices in Caracas and Madrid—asserted that "our client already has an approved budget for an interception system" regarding the Remote Control System (RCS) spyware.[156] In a previous email in the same thread, the company representative mentioned the possibility of placing the product in SEBIN and "DIM," a referenceto DGCIM. The leak does not clarify whether a follow-up took place, and an Armando.info investigation could neither confirm nor rule out the sale of this system to Venezuela.[157]

Documents obtained by journalists from intelligenceonline.com show that the firm 9th Vision, registered in South Africa, attempted to sell spyware to Venezuela's Ministry of Popular Power for Defense between 2021 and 2022.[158] This firm offers zero-click intrusions, in which a device can be infected without any action by the victim. It was reported that another firm that commercialized spyware was contacted by Venezuelan government authorities in 2021, but details have not been confirmed.

In a previously unreported 2022 case, Conexion Segura y Libre had brief access to a human rights activist's mobile phone exhibiting spyware infection symptoms. Simultaneously, she and other members of the same nongovernmental organization were victims of unauthorized email account access and other forms of persecution that were documented, including intimidating calls from SEBIN officials. In this incident, the victim reported that the phone displayed the operating system's screenshot capture animation without user interaction, and that the screenshots were not found in the photo gallery afterward. This behavior, along with other unexplained issues, points to spyware that was not properly optimized to operate undetected on that Android model.

Search and seizure of electronic devices

The warrantless inspection of mobile phones by Venezuelan state officials has become an increasingly pervasive and dangerous practice that exposes individuals' private lives and can lead to arbitrary detention, extortion, and reprisals. Through these inspections, authorities access personal information, private communications, and political opinions without judicial authorization or legal explanation, creating an environment of fear and defenselessness. This practice operates within a broader political context where Venezuela's authoritarian government has systematically dismantled judicial independence and the rule of law, transforming state security forces into instruments of political control rather than public service.

Venezuela lacks effective legal safeguards protecting citizens from arbitrary searches of electronic devices. The country's constitution nominally protects privacy and personal correspondence, but these guarantees have been systematically violated in practice, particularly following the contested 2024 presidential election and subsequent political repression.[159] The absence of clear legal procedures governing device inspections, combined with near-total impunity for security force abuses, has created conditions where millions of Venezuelans navigate constant surveillance risks.

The declaration of state of emergency on January 3, 2026 increased these risks by ordering security forces to find and capture anyone who "promoted or supports" the US operation in Veenzuela.[160] This section examines documented patterns of device searches and seizures, the tactics employed by state actors, and the profound human rights impacts of these practices on Venezuelan society.

Systematic documentation of abuses

To better understand and systematically document these practices, Conexión Segura y Libre conducted a public consultation from January 7 to 23, 2026, collecting reports from affected individuals and those with direct knowledge of incidents. The consultation was disseminated through social media, digital channels, and contact networks as an accessible and secure mechanism for reporting these incidents in a high-risk environment, enabling reporting of abuses. The consultation systematized fifty-eight reports of mobile phone inspections conducted by Venezuelan state officials, with incidents occurring primarily between 2024 and January 2026.[161] The collected testimonies do not attempt to measure the phenomenon exhaustively but rather to make it visible, identify operational patterns, and provide insights into how arbitrary phone inspections have become tools of control, intimidation, and punishment, with direct impacts on fundamental rights.

The documented incidents were concentrated at informal checkpoints, military control points on highways, and random street detentions, particularly in the country's most populous states, including Zulia, Miranda, the Capital District, Táchira, Carabobo, and Bolívar. In most cases, individuals were simply transiting on the street or traveling between states, with no judicial order or clear legal basis for inspecting their mobile devices. This geographic distribution reflects both the deployment of security forces and strategic chokepoints where authorities exercise maximum control over civilian movement.

The primary security forces identified as conducting these searches are the Bolivarian National Guard (GNB) and Bolivarian National Police (PNB), followed by state or municipal police corps, officials from the Directorate General of Military Counterintelligence (DGCIM), and unidentified uniformed personnel—some hooded or dressed in civilian clothes. In most cases, officials either did not identify themselves (thirty-six cases) or did so only partially (sixteen cases), thereby aggravating the arbitrariness of these actions and eliminating any possibility of accountability.

The collected information shows that in thirty-four cases there was a direct request to inspect the phone, while in twenty-three cases the inspection was forced, accompanied by coercion, detention threats, criminal incrimination, or reprisals. Even when victims indicated they had "consented" to the inspection, most stated they did so out of fear, nullifying any notion of free, prior, and informed consent. This pattern reveals the fiction of "voluntary" cooperation under authoritarian surveillance conditions—when refusal risks detention, physical harm, or worse, consent becomes meaningless. Female activists, journalists, and civil society workers report particular vulnerability to sexual harassment, intimidation through threats against family members, and gender-specific forms of coercion during device searches.

The most frequent inspection practices included accessing photo and video galleries, WhatsApp, Telegram, and SMS chats, social media, and files stored in the cloud (Google Drive, iCloud, Dropbox). In twenty-nine cases, officials forced device unlocking, and in fourteen cases, they temporarily confiscated phones or inspected them out of the affected person's view. Testimonies repeatedly report the use of keyword searches—including "Maduro," "Diosdado," "María Corina," "guarimbero" (a pejorative term for demonstrators), "government," or references to the July 28 elections—suggesting specific interest in identifying political opinions, connections, or critical content.

Officials systematically hunt for evidence of dissent, support for opposition, or participation in anti-government activities. The keyword searches reflect regime priorities and reveal the explicitly political nature of these inspections; they function not as legitimate law enforcement but as dragnet surveillance operations designed to identify and intimidate political opponents.

A particularly grave element is the economic extortion associated with these inspections. Six reports detail demands for payments in US dollars—in cash or via Zelle—as a condition for not detaining the individual, not forwarding information to the central authorities in the capital city or not charging the citizens with serious crimes such as terrorism, incitement to hatred, or illicit financing. In these cases, amounts demanded reached thousands of dollars, beyond the means of the low-income individuals detained, directly affecting victims' integrity, economic security, and family stability.

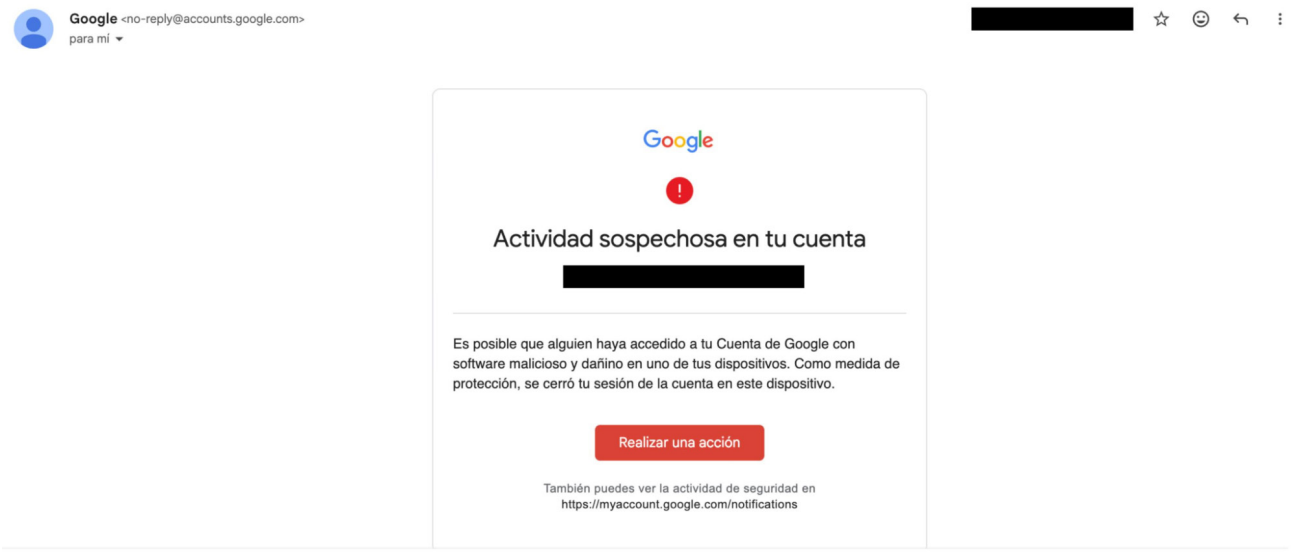
This systematic extortion transforms surveillance into a revenue stream for corrupt officials while compounding the political weaponization of device searches. Families must choose between financial ruin and the potential imprisonment of their relatives. The dollar-denominated demands reflect Venezuela's informal dollarized economy and officials' exploitation of desperate circumstances. For many Venezuelans, particularly women who often manage household economies and family resources, these extortion demands create impossible choices that reverberate through entire family networks.

Airport targeting of high-profile individuals

Individuals with recognizable profiles in human rights defense, activism, or journalism have been subjected to equipment inspections during interrogations lasting hours when entering or leaving Venezuela through airports.[162] These inspections are typically much more detailed than summary street inspections, encompassing multiple devices such as laptops, mobile phones, and tablets. Between 2023 and 2024, as Venezuela prepared for the July 2024 presidential election, at least seven activists for electoral rights from recognized NGOs experienced airport interrogations, and at least four were subjected to equipment inspections, some on multiple occasions.

In one case involving a human rights defender taken for interrogation at Maiquetía International Airport, which serves Caracas, officials coerced the individual into unlocking their devices and thoroughly inspected the contact list and chats. The defender's devices were taken and unlocked in another room for between four and five hours. At 9 a.m. the following day, they received a Google alert: "Suspicious activity in your account: Someone might have accessed your Google Account using harmful malware on one of your devices"—presumably trig-

gered by officials' manipulation of their equipment. The warning indicates that the authorities may have tried to open a Gmail session on a security personnel computer, or they may have installed malware on one of the temporarily seized devices. As a precaution, the human rights defender formatted their devices and secured their accounts afterwards.



Warning received by a human rights defender hours after the interrogation where their equipment was handled without their supervision. (Source: VE sin Filtro)

New emerging pattern: online search of individuals

Following January 3, 2026, Conexión Segura y Libre documented multiple cases in which individuals reported that upon arrival at Venezuelan airports, Migration Police officials requested passports and, before allowing access to immigration booths, conducted searches of their names on official devices, primarily through Google Search and search functionalities on social media platforms. These searches appear to serve objectives similar to mobile device inspections: identifying politically oriented posts, establishing individuals' possible connections, or detecting those who may have publicly expressed support for or celebration of the January 3 capture of Nicolás Maduro.

Direct online searching of information about travelers could constitute a surveillance strategy attempting to circumvent digital self-protection measures such as deleting content from personal devices, as well as the refusal of mobile phone inspections. Separate from the directly documented cases, the consultation identified fifteen reports specifically addressing searches by name on Google or social media. In five of these cases, individuals explicitly indicated they were searched on Instagram, and in one case both Google and Instagram searches were reported, indicating direct interest in contrasting identity and the person's public activity beyond information contained on the mobile device.

Violation of university campus territorial autonomy

On January 31, 2026, the University Council of the Central University of Venezuela publicly rejected the unannounced presence of police and military personnel in the University City of Caracas on January 27 during an official visit by Acting President Delcy Rodríguez.[163] According to the institutional statement, security force officials intimidated students through mobile phone inspections in actions characterized as disproportionate, intimidating, and violating university autonomy and fundamental rights.[164]

This statement confirms that mobile device inspections are not limited to checkpoints or street procedures but extend into university campuses, further eroding the boundaries between security, political control, and private life. Universities have historically served as spaces of relative autonomy and critical thought in Venezuela; their invasion by surveillance apparatus represents a significant escalation in authoritarian control.

Forensic extraction and other means of device data extraction

The DGCIM digital forensics laboratory is known to possess Cellebrite UFED Touch 2 devices to extract forensic images from mobile phones and computers during detentions and criminal investigations.[165] No public information is available on which other security agencies have these forensic analysis tools.

Authorities have access to far more comprehensive equipment inspections. These extraction tools can breach the security of some mobile phones, depending on their software and configuration, and extract data even without knowing the phone's password. Conexion Segura y Libre has seen evidence of other forms of data extraction from mobile phones, including officials locating documents stored in the devices and sending them to their own devices using WhatsApp, extraction of computer hard drives, and other methods. This points to an opportunistic approach using whatever tools are available while disregarding the integrity, verifiability, and chain of custody of extracted artifacts.

Pervasive chilling effects on political speech in spaces with a reasonable expectation of privacy

The impact of these practices transcends the immediate incident. Testimonies reflect persistent fear, self-censorship, application deletion, social media abandonment, and changes in digital routines—adopted as protection mechanisms against possible future inspections. For journalists, activists, and citizens perceived as "suspicious," these actions constitute intimidatory surveillance restricting de facto exercise of fundamental rights. The psychological toll extends beyond individuals to their families and communities, creating cascading effects that multiply the repressive impact of each device search.

The systematic nature of device searches creates pervasive chilling effects on democratic participation and civil society organizing. Knowing that any interaction with security forces could result in phone inspection, Venezuelans self-censor their communications and refrain from sharing political opinions—even in private messages. This anticipatory conformity represents precisely the outcome authoritarian regimes seek: a population that polices itself out of fear, reducing the need for direct repression.

Collectively, the data confirms that arbitrary mobile phone inspection in Venezuela does not constitute an isolated incident but rather a systematic and repeated practice combining control, intimidation, punishment, and extortion, in open contradiction with national and international human rights standards—particularly those relating to privacy, freedom of expression, and due process. The practice violates multiple provisions of the International Covenant on Civil and Political Rights, the American Convention on Human Rights, and Venezuela's own constitutional protections, which are now rendered meaningless by authoritarian practices.

The expansion of these practices into university campuses, airports, and road checkpoints demonstrates escalating authoritarian control over Venezuelan society. As traditional spaces of relative autonomy disappear under surveillance pressure, Venezuelans face increasingly difficult choices between digital self-protection and normal social, economic, and political participation. The resulting society—one where millions constantly calculate surveillance risks and modify behavior accordingly—represents the practical realization of authoritarian aspirations: a population subjugated not primarily through overt violence but through pervasive fear of arbitrary state intrusion into the private spheres of life.

Conclusions

The coexistence—even if without technical integration—of different surveillance systems results in multiplicative rather than merely additive effects. For instance, an individual attending a protest faces multiple risks: they might be identified through facial recognition cameras, have their communications intercepted while coordinating attendance, face doxxing on social media, undergo device searches at checkpoints, and experience potential cyberattacks that compromise their digital accounts. This comprehensive vulnerability transforms constitutionally protected political participation into high-risk activities that require sophisticated operational security measures, fundamentally altering the nature of democratic engagement.

Venezuela's CCTV infrastructure has been systematically weaponized for political control rather than public safety. Chinese vendors—particularly CEIEC, Hikvision, and Dahua—dominate the supply chain despite international sanctions, with advanced facial recognition and license plate detection, enhanced by artificial intelligence, operating without privacy protections, judicial oversight, or mechanisms for citizen consent. The co-option of opposition-controlled municipal systems demonstrates how ostensibly independent security infrastructure becomes compromised for surveillance purposes, creating comprehensive monitoring networks that enable rapid identification and targeting of dissidents, protesters, and political opponents.

Drone surveillance has evolved into a sophisticated intimidation apparatus combining advanced technical capabilities with psychological warfare tactics. Venezuelan security forces deploy commercial drones, ranging from compact consumer DJI models to advanced public safety Autel models with extended surveillance capabilities, operating without legal frameworks governing deployment or oversight. The deliberate visibility of drone operations, particularly nighttime flights equipped with multiple lights over protest zones and residences of opposition figures, serves dual purposes: gathering intelligence on movement patterns and participants while creating pervasive chilling effects on political assembly.

GPS tracking devices discovered in vehicles of political prisoners' families, some equipped with listening capabilities, reveal covert surveillance layers requiring physical access but providing continuous location data and environmental audio. The systematic deployment of movement surveillance technologies without judicial authorization fundamentally undermines freedom of assembly and association, transforming constitutionally protected political participation into activities that require operational security measures and entail substantial risk.

The Patria System is a pillar of Venezuela's platformization of citizen control, transforming social welfare delivery and public service access into instruments for systematic data extraction and political manipulation. The Patria database enables comprehensive identification and large-scale data collection, with the platform's domain registered to PSUV rather than any state agency—demonstrating operational fusion between the state apparatus and the party structure. Access to welfare benefits, which conditions millions of citizens' daily subsistence on mandatory registration and the continuous provision of personal information, creates permanent incentives for self-surveillance. The system's technical design allows mapping users' relationships with other people and institutions, enabling administrators to create detailed connection networks even for non-users.

Systematic cyberpatrolling across social media platforms and messaging applications, coordinated by SEBIN, DGCIM, and regional police forces, has evolved into a comprehensive machinery of digital persecution that criminalizes online expression and generates profound chilling effects on freedom of expression and association. Telegram channels such as "Caza Guarimbas VE" systematically compile and disseminate doxing lists containing the names, photographs, addresses, and identification numbers of individuals identified as opposition supporters, which facilitate subsequent harassment, reprisals, and even arrests. Operation Knock Knock exemplified the integration of multiple surveillance streams—VenApp reporting features, Tele-

gram groups, and door-to-door arrest campaigns—into coordinated persecution mechanisms that generated pervasive self-censorship across Venezuelan society. Criminal prosecutions arising from cyberpatrolling rely on decontextualized digital content, without technical forensic analysis, proper chain-of-custody procedures, or evidence of concrete harm, and apply vague provisions such as 'incitement to hatred' to criminalize citizen complaints and political opinions that constitute legitimate public discourse. The convergence of digital surveillance, selective prosecution, and arbitrary detention has normalized self-censorship, forced the displacement of journalists and activists, and weakened civil society's organizational capacity.

Telecommunications interception at scale represents the most intrusive component of Venezuela's surveillance apparatus, with documented evidence of systematic and widespread practices that far exceed any legitimate law enforcement justification. Telefónica's 2021 transparency report—the last released before government pressure ended such disclosures—revealed 1,523,363 affected telephone lines and 205,800 interception orders, demonstrating industrial-scale surveillance that is impossible to justify by targeted criminal investigations. CANTV's state-owned infrastructure provides direct access to telecommunications data and to internet traffic surveillance capabilities, while private providers face intense pressure to cooperate due to CONATEL's regulatory authority over licensing and operations. The regulatory framework's structural flaws enable abuse: the Criminal Processing Code's mandate that telecommunications and financial institutions maintain 24/7 availability to process interception requests, combined with the judicial system's subordination to executive power and the absence of independent oversight, creates conditions for unlimited surveillance without meaningful constraints. The FADe Project's documentation of IMSI catchers concentrated at strategically significant locations, including nearby military installations and airports, indicates that security institutions are deploying them to obtain direct, real-time location and communications data without provider cooperation or even a remote possibility of a request being denied.

State-sponsored cyberattacks are systematic, not isolated incidents, employing sophisticated techniques that combine technical capabilities with coordination across multiple government entities. Large-scale phishing campaigns instrumentalized CANTV's ISP-level infrastructure for DNS response injection, directing users to malicious sites. The coordination among the censorship apparatus, disinformation networks, and state entities reveals deliberate orchestration, with public exposure of phishing victims occurring in contexts where disclosing political affiliation carries material risks, given the historical precedent of systematic political discrimination. Unauthorized access to organizational platforms and messaging account takeovers frequently exploit telecommunications interception capabilities, with documented cases showing that intercepted SMS verification codes enable WhatsApp account hijacking and the takeover of email and social media accounts. Venezuela's persistent efforts to acquire commercial spyware from multiple companies, combined with Citizen Lab's identification of FinFisher command-and-control infrastructure in Caracas and documented cases of infection symptoms, point to active deployment despite the secrecy and obfuscation surrounding the commercialization of spyware for sanctioned regimes.

Warrantless inspection of mobile phones has become a pervasive and dangerous practice that combines control, intimidation, punishment, and extortion, in open contradiction to national and international human rights standards. The systematization reveals forced cooperation, as inspections are accompanied by coercion and threats of detention or criminal prosecution. Keyword searches for "Maduro," "Diosdado," "María Corina," or references to the July 28 elections reveal an explicitly political nature designed to identify dissent rather than serve legitimate law enforcement purposes. Economic extortion compounds political weaponization, with reports documenting demands for thousands of dollars in cash or Zelle transfers as conditions for not detaining individuals or charging them with terrorism or incitement to hatred, transforming surveillance into revenue streams for law enforcement ranks. High-profile individuals at airports face equipment inspections that last hours, while emerging patterns include online searches for travelers' names on Google and social media to find information about the political opinions of ordinary citizens.

Collectively, these findings demonstrate that Venezuela's surveillance infrastructure operates as an integrated authoritarian control system that transcends individual technologies or institutional actors. The convergence of video surveillance with telecommunications interception, cyberpatrolling with device searches, and state-sponsored applications with cyberattacks creates multiplicative effects that severely constrain civic space and alter the risk calculus for political participation. The human rights impacts extend far beyond immediate violations to generate profound societal transformations: the normalization of self-censorship, erosion of community trust, forced displacement of journalists and activists, and the rendering of constitutionally protected political participation into high-risk activities that require sophisticated operational security.

Critically, the surveillance infrastructure remains operational and intact despite Maduro's removal on January 3, 2026, demonstrating that technological capabilities and institutional frameworks for authoritarian control transcend individual leadership and require deliberate dismantling rather than mere regime leadership change. Understanding these systems in their full complexity, including their technical capabilities, supply chains, institutional operators, legal frameworks, and human rights impacts, proves essential for supporting Venezuelan civil society under conditions of maximum repression, informing international policy responses that address both current abuses and future accountability mechanisms, and ultimately contributing to the conditions necessary for genuine democratic transition that includes dismantling the surveillance state apparatus itself.

Recommendations

The following recommendations address the urgent needs of those most vulnerable to surveillance and identify concrete actions that governments and international organizations can take to constrain Venezuela's surveillance infrastructure, protect human rights defenders, support Venezuelan civil society's operational security, and establish accountability mechanisms for technology vendors that enable systematic human rights violations. These recommendations derive directly from documented cases, deployed surveillance systems, identified technical vulnerabilities, supply chain dependencies, and the operational realities facing activists under conditions of harsh repression.

For civil society organizations

- Improve data sharing and monitoring mechanisms documenting surveillance technology deployment and human rights impacts in Venezuela by deploying technical experts, coordinating evidence collection, and producing regular public reports on surveillance infrastructure evolution under the Rodriguez interim administration to increase public awareness and enable protective measures by sharing information, increasing awareness of mitigations against surveillance, identifying high-risk checkpoint areas, and developing countermeasures with the support of experts.
- Adopt and make available tailored digital security training and resources to various population groups, including journalists, activists, and opposition members with special attention to female leaders, by developing context-specific protocols addressing telecommunications interception, device seizure risks, phishing threats, and social media surveillance as the threats occur in Venezuela.
- Establish emergency response networks to provide immediate assistance when activists face detention, device seizure, or targeted cyberattacks, coordinating legal support, secure communications, facilitating safe relocation when necessary, and generating international pressure through rapid documentation shared with diplomatic missions, international human rights bodies, and media networks.
- Advocate for technology platforms to implement enhanced security features and abuse reporting mechanisms by engaging directly with messaging applications, social media companies, and cloud service providers to address Venezuela-specific threats. Human rights defenders should advocate for platforms to implement robust abuse-reporting mechanisms for doxxing and coordinated harassment campaigns, and to provide expedited verification processes to restore accounts to users who have been hacked.
- Pursue accountability for surveillance technology vendors through documentation campaigns, legal actions, and advocacy targeting companies supplying repressive infrastructure by compiling evidence of specific human rights violations enabled by identified technologies and suppliers. Organizations should systematically document how specific surveillance technologies directly facilitate documented human rights violations. This evidence supports international pressure and advocacy, corporate accountability campaigns, and potential legal actions under international human rights frameworks.

For Venezuelan democracy activists

- Adopt digital security and surveillance mitigation protocols, including for emergency scenarios. Establish security support networks with digital security experts and digital rights organizations. Strengthen phishing awareness and protections.
- Use end-to-end encrypted communications platforms, and follow clear communication security protocols. Adopt protections for these platforms including using two-factor authentication and PINs in messaging apps.

- Enable and use phishing-resistant multi-factor authentication, specifically hardware security keys and TOTP (Time-based One-Time Password) authenticator apps, to protect against telecommunications interception capabilities. SMS-based verification codes should be entirely phased out, as they rely on telecommunications infrastructure susceptible to state interception.
- Ensure device security including keeping the device updated with the latest OS and security patches. Setting a cellphone PIN of at least six characters, or ideally a password. Avoiding pirated software and any other software from untrusted sources.
- Inspect undersides of vehicles if they have been under control of security forces, and also internally in cases involving high-profile targeted persons, specially if experiencing unexplained electrical issues.
- Women activists, journalists, and human rights defenders should consider their increased exposure to surveillance and adopt practices to increase the isolation and protection of both their professional and personal communications, accounts, and content and devices whenever possible.
- Implement device sanitization protocols for mobility and high-risk scenarios, including checkpoints, airports, protests, and detention, by protecting the device, maintaining minimal sensitive content on devices and obfuscating what can't be removed, setting up protocols or using secondary devices for sensitive activities, and enabling remote wiping capabilities.
- Maintain secure backups of critical evidence and organizational records to ensure continuity and data preservation following device seizure, confiscation, or destruction by regularly exporting key documentation to encrypted external storage held in secure locations.

For democratic governments

- Demand dismantling of political surveillance infrastructure and accountability for documented abuses by conditioning sanctions relief and economic cooperation on concrete surveillance reforms and prosecuting officials responsible for systematic human rights violations, and establishing independent oversight mechanisms.
- Support Venezuelan civil society's digital security capacity through dedicated funding streams, technical assistance programs, and infrastructure support by providing resources for secure communications, device replacement following seizures, security audits, and ongoing technical training coordinated through experienced digital rights organizations. Governments should establish dedicated funding mechanisms—separate from broader democracy promotion—specifically for addressing digital security needs: procurement of secure devices and communications infrastructure, technical assistance from experienced practitioners familiar with high-threat environments, support for ongoing security training programs, emergency funds for device replacement following confiscations, and resources for security audits of vulnerable organizations.
- Lead multilateral initiatives establishing norms against surveillance technology exports to authoritarian regimes by coordinating export control frameworks, supply chain transparency requirements, and due diligence standards for surveillance technology sales through hemispheric and multilateral forums, including the Organization of American States.

For international organizations

- Develop accountability frameworks for surveillance technology vendors enabling human rights violations by investigating supply chains, documenting specific technological contributions to documented abuses, and pursuing legal mechanisms under international human rights law, including potential presure recommendations and referrals to appropriate judicial bodies. This includes mapping complete supply chains, documenting technological specifications enabling specific abuse patterns (facial recognition, forensic extraction, telecommunications interception), establishing causal links between supplied technologies and documented human rights violations, and pursuing accountability through appropriate legal frameworks, including accountability actions and support for civil litigation against complicit vendors.
- Provide technical assistance to Venezuelan civil society organizations by facilitating access to digital security tools and ongoing capacity building through partnerships with established digital rights organizations and cybersecurity experts familiar with high-threat operating environments. This should include facilitating partnerships between Venezuelan civil society and international security experts, providing resources for secure infrastructure procurement, coordinating training programs that address the Venezuela-specific threat landscape, supporting security audits that identify organizational vulnerabilities, and maintaining ongoing advisory relationships as threats evolve.
- Coordinate international advocacy campaigns targeting surveillance technology companies through multilateral forums, shareholder actions, and public pressure by leveraging organizational platforms to spotlight vendor complicity in human rights violations and mobilize coordinated responses from member states, civil society, and private sector actors. This includes organizing multilateral statements condemning vendor complicity, coordinating member state actions restricting technology exports, supporting shareholder advocacy highlighting reputational risks, facilitating civil society documentation campaigns, and leveraging organizational platforms to generate sustained public attention.
- Integrate surveillance concerns into broader human rights monitoring and reporting by ensuring that traditional human rights documentation mechanisms systematically incorporate digital rights violations, surveillance infrastructure analysis, and technology-enabled repression into investigations, reports, and recommendations for Venezuela. Too often, surveillance violations receive insufficient attention within traditional human rights frameworks focused on physical detention, torture, and disappearances. International organizations should ensure that country-specific mechanisms—including the UN Fact-Finding Mission on Venezuela, Inter-American Commission rapporteurs, and OAS monitoring processes—systematically investigate surveillance infrastructure, analyze technology-enabled repression, document supply chains, and integrate digital rights expertise into all Venezuela-related work. This institutional integration ensures surveillance receives appropriate priority alongside physical violence and detention.

These recommendations focus on the immediate operational needs of those who are most vulnerable to Venezuela's surveillance apparatus. They outline specific actions that governments and international organizations can take to limit repressive infrastructure, enhance the capacity of civil society, and hold technology vendors accountable for their role in enabling repression. Implementing these actions requires a sustained commitment from various stakeholders, coordination across different organizations, and a recognition that surveillance is a key aspect of authoritarian control. This matter demands dedicated response strategies rather than being treated as a minor concern within broader human rights discussions. During this transitional period, international actors must take decisive action to ensure that outcomes protect fundamental rights instead of allowing surveillance capabilities to strengthen under new regime leadership.

References

1. "Informe de Transparencia en las Comunicaciones 2021" ("Communications Transparency Report 2021"), Telefónica, June 18, 2022, https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf..
2. "Fact Sheet: President Donald J. Trump Safeguards Venezuelan Oil Revenue for the Good of the American and Venezuelan People," The White House, January 9, 2026,. https://www.whitehouse.gov/fact-sheets/2026/01/fact-sheet-president-donald-j-trump-safeguards-venezuelan-oil-revenue-for-the-good-of-the-american-and-venezuelan-people/.
3. Simon Lewis and Patricia Zengerie, "Rubio Says US Plan for Venezuela Is Stability, Recovery, Then Transition," Reuters, January 7, 2026, https://www.reuters.com/world/us/rubio-says-us-plan-venezuela-is-stability-recovery-then-transition-2026-01-07.
4. Iria Puyosa, "Delcy Rodríguez's untenable balancing act," Atlantic Council, January 8, 2026, https://www.atlanticcouncil.org/dispatches/delcy-rodriguezs-untenable-balancing-act/.
5. "Comprehensive Strategic Partnership and Cooperation Agreement between the Russian Federation and the Bolivarian Republic of Venezuela," President of Russia, May 7, 2025,, http://en.kremlin.ru/acts/news/78304.
6. "Fact Sheet: President Trump Restoring Prosperity, Safety, and Security to the United States and Venezuela," US Department of Energy, January 7, 2026, https://www.energy.gov/articles/fact-sheet-president-trump-restoring-prosperity-safety-and-security-united-states-and.
7. "Russian Companies Forced Out of Venezuela After U.S. Capture of Maduro, Lavrov Says," The Moscow Times, February 5, 2026, https://www.themoscowtimes.com/2026/02/05/russian-companies-forced-out-of-venezuela-after-us-capture-of-maduro-lavrov-says-a91872.
8. On February 28, the United States and Israel attacked Iran, resulting in the deaths of several high-ranking Iranian officials, including Supreme Leader Ayatollah Ali Khamenei. At the time this report was completed, Iran was experiencing political instability, and the continuity of its operations in Venezuela or elsewhere remained uncertain.
9. "Treasury Targets Iran-Venezuela Weapons Trade," US Department of the Treasury, December 30, 2025, , https://home.treasury.gov/news/press-releases/sb0347.
10. "Secretary of State Marco Rubio Before the Senate Committee on Foreign Relations on US Policy Towards Venezuela," US Department of State, January 28, 2026, https://www.state.gov/releases/office-of-the-spokesperson/2026/01/secretary-of-state-marco-rubio-before-the-senate-committee-on-foreign-relations-on-u-s-policy-towards-venezuela.
11. "El Ilyushin ha realizado seis vuelos de repatriación de cubanos desde Venezuela tras la captura de Maduro" ("Ilyushin carried out six repatriation flights for Cubans from Venezuela following the capture of Maduro"), 14ymedio, January 20, 2026. https://www.14ymedio.com/cuba/ilyush-in-realizado-seis-vuelos-repatriacion_1_1122898.html.
12. Marleidy Múñoz and Raúl Medina, "The Footprints of Cuban Intelligence in Venezuela," El Toque, August 20, 2024, https://eltoque.com/en/the-footprints-of-cuban-intelligence-in-venezuela.
13. "Transición en Venezuela: Delcy Rodríguez eliminó por decreto programas sociales y entes emblemáticos del entramado chavista" ["Transition in Venezuela: Delcy Rodríguez Eliminated by Decree Social Programs and Emblematic Entities of the Chavista Framework"], Infobae, February 15, 2026, https://www.infobae.com/venezuela/2026/02/15/transicion-en-venezuela-delcy-rodriguez-elimino-por-decreto-programas-sociales-y-entes-emblematicos-del-entramado-chavista/.
14. Justicia, Encuentro y Perdón (@JEPvzla), "#ATENCIÓN En el marco de nuestro proceso…" X, March 2, 2026. https://x.com/jepvzla/status/2028490743937950060.
15. Regina Garcia Cano and Megan Janetsky, "Hundreds more in Venezuela say their loved ones are 'political prisoners,'" The Washington Post, January 14, 2026, Regina Garcia Cano and Megan Janetsky, "Hundreds more in Venezuela say their loved ones are 'political prisoners,'" The Washington Post, January 14, 2026, https://www.washingtonpost.com/world/2026/01/13/venezuela-prisoners-released-us-maduro-rodriguez/798bed6a-f097-11f0-a4dc-effc74cb25af_story.html.
16. "Censored Network: Restrictions on #InternetVE," VE sin Filtro, January 17, 2026, https://vesinfiltro.org/noticias/2025-censorship-report/.
17. "Venezuela: Serious Human Rights Violations in Connection with the Elections," Inter-American Commission on Human Rights, December 27, 2024, https://www.oas.org/en/iachr/reports/pdfs/2025/report-venezuela-serioushhrr-violations-connections-elections.pdf.
18. "Rodríguez Torres anuncia instalación de 30 mil cámaras de seguridad en zonas de incidencia delictiva" ("Rodríguez Torres announces the installation of 30,000 security cameras in areas with high crime rates"), Diario La Voz, October 28, 2013, https://diariolavoz.net/2013/10/28/rodriguez-torres-anuncia-instalacion-de-30-mil-camaras-de-seguridad-en-zonas-de-incidencia-delictiva/.
19. "Peace Quadrants ("Cuadrantes de Paz") are geographically delimited basic territorial units that form part of Venezuela's Popular Protection System for Peace (SP3) and Integral Defense of the Nation. See: "Gran Misión Cuadrantes de Paz" ("Great Mission Peace Quadrants"), Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz, Gobierno Bolivariano de Venezuela, https://www.mpprijp.gob.ve/biblioteca/cuadrantes.; "Sistemas de videovigilancia y atención de emergencias en Venezuela" ("Video surveillance and emergency response systems in Venezuela"), Transparencia Venezuela, 2022, https://transparenciave.org/wp-content/uploads/2022/01/Sistemas-de-videovigilan-

cia-y-atencio%CC%81n-de-emergencias-en-Venezuela.pdf.

20. "Venezuela has more than 3 thousand video surveillance cameras throughout the country (+VEN 911)," Con el Mazo Dando, June 12, 2025, https://mazo4f.com/en/venezuela-has-more-than-3-thousand-video-surveillance-cameras-throughout-the-country-ven-911.

21. Con el Mazo Dando, Programa N° 554, December 3, 2025, https://www.youtube.com/watch?v=AeYvh7JvHdI.

22. "El vicepresidente sectorial de Política, Seguridad Ciudadana y Paz, Diosdado Cabello, ha afirmado que las cámaras del 911 están activas en todas las calles del país,", ("The sectoral vice president for Politics, Citizen Security and Peace, Diosdado Cabello, has stated that the 911 cameras are active on all the streets of the country"), Globovisión (@globovision), Instagram, April 3, 2025, https://www.instagram.com/reels/DH_bkKvptcV/.

23. "Instalan cámaras en hospitales públicos de Venezuela para «erradicar» supuestos sabotajes" ("Cameras are being installed in public hospitals in Venezuela to 'eradicate' alleged acts of sabotage"), SWI swissin, June 22, 2025, https://www.swissinfo.ch/spa/instalan-c%c3%a1maras-en-hospitales-p%c3%bablicos-de-venezuela-para-%22erradicar%22-supuestos-sabotajes/89562579.

24. "Carmen Meléndez: Instalaremos cámaras inteligentes 'en cada esquina y en cada semáforo en Caracas'" ("Carmen Meléndez: We will install smart cameras 'on every corner and at every traffic light in Caracas'"), El Universal, August 15, 2025,https://www.eluniversal.com/caracas/212222/carmen-melendez-instalaremos-camaras-inteligentes-en-cada-esquina-y-en-cada-semaforo-en-caracas.

25. ,"ZTE Smart City Full Solution," ZTE Corporation, accessed February 28, 2026, , https://www.zte.com.cn/global/solutions/digital_transformation/government/ztesmartcityfullsolution.html.

26. "ZTE Government Cloud Solution," ZTE Corporation, accessed February 28, 2026, https://www.zte.com.cn/global/solutions/digital_transformation/government/20170901004.html.

27. "Ministro Cabello: 'Guaicaipuro tiene un sistema de cámaras que es extraordinario,'" ("Minister Cabello: 'Guaicaipuro has an extraordinary camera system'") Alcaldía de Guaicaipuro, November 13, 2025, .https://alcaldiadeguaicaipuro.gob.ve/2025/11/13/ministro-cabello-guaicaipuro-tiene-un-sistema-de-camaras-que-es-extraordinario/.

28. "Proyecto «Caracas Inteligente» promete garantizar seguridad en la capital" "The 'Smart Caracas' project promises to guarantee security in the capital"), Correo del Orinoco. December 4, 2024, https://www.correodelorinoco.gob.ve/proyecto-caracas-inteligente-promete-garantizar-seguridad-en-la-capital/.

29. Díaz, Floralbert, "Avanzan en la instalación de paradas inteligentes en Caracas" "Progress is being made on the installation of smart bus stops in Caracas") Ciudad CCS, https://www.ciudadccs.info/publicacion/34076."En trabajo conjunto con el equipo de @caracasinteligente, se lleva a cabo la instalación de un novedoso sistema de circuito cerrado, el cual comprende la colocación de cámaras de seguridad y vigilancia en los diferentes espacios del Terminal La Bandera" ("Working together with the @caracasinteligente team, we are installing a new closed-circuit system, which includes placing security and surveillance cameras in different areas of the La Bandera Terminal"), INTRAVIALCA (@intravialca_ccs), Instagram, March 7, 2025, https://www.instagram.com/p/DG6THzchFXK/.

30. "El presidente de la Fundación Caracas Inteligente y la Oficina de la Tecnología de la Información y la Comunicación, Ing. Darwin Vargas, participó en la instalación del botón de emergencia en la Plaza de la Victoria en Plaza Venezuela." ("The president of the Caracas Smart City Foundation and the Office of Information and Communication Technology, Eng. Darwin Vargas, participated in the installation of the emergency button in Plaza de la Victoria in Plaza Venezuela"), Fundación para La Caracas Inteligente (@caracasinteligente), Instagram, November 12, 2025, https://www.instagram.com/p/DQ-AQiPjxvr/.

31. "US blacklists 28 Chinese companies and government agencies over Uighur repression," The Guardian, October 8, 2019, https://www.theguardian.com/world/2019/oct/08/us-blacklists-28-chinese-companies-and-government-agencies-over-uighur-repression.

32. "El presidente de la Fundación Caracas Inteligente y la Oficina de la Tecnología de la Información y la Comunicación, Ing. Darwin Vargas, participó en la instalación del botón de emergencia en la Plaza de la "Victoria en Plaza Venezuela," ([The president of the Caracas Smart City Foundation and the Office of Information and Communication Technology, Eng. Darwin Vargas, participated in the installation of the emergency button in Victory Square in Venezuela Square."), Fundación Caracas Inteligente (@caracasinteligente), Instagram, November 12, 2025, https://www.instagram.com/reel/DQ-AQiPjxvr/.

33. "Desde nuestro Integral de Seguridad Ciudadana comparto con ustedes algunas de las calles y avenidas que se pueden ver gracias a una inversión importante en cámaras de seguridad" ("From our Integrated Citizen Security system, I'm sharing with you some of the streets and avenues that can be viewed thanks to a significant investment in security cameras") Gustavo Duque (@gustavoduquesaez), Instagram, August 12, 2025, https://www.instagram.com/reels/DNR0KiPxR_b/.

34. Interview with a security official in Caracas, who requested to remain anonymous for security reasons, January 2026.

35. Ibid.

36. Interview with a security official in Caracas, who requested to remain anonymous for security reasons, January 2026.

37. "El monitoreo de cámaras en el #VEN911Baruta es un sistema de videovigilancia y videoprotección que utiliza una red de cámaras instaladas en puntos estratégicos de las ciudades y vías del país . Este sistema opera de manera centralizada desde los Centros de Comando, Control y Telecomunicaciones (VEN 9-1-1)," Ven911baruta (@ven911baruta), Instagram, October 30, 2025, https://www.instagram.com/p/DQcI1rZjpE5/.

38. "Desde el Centro de Control Integral de El Hatillo (CCI), se canalizan todas las denuncias en el menor tiempo posible," PoliHatillo (@polihatillo), Instagram, August 15, 2023, https://www.instagram.com/p/Cv-PMIaLAMX/.

39. "Gobierno Bolivariano fortalece sistema de seguridad con expansión masiva de videovigilancia" ("Bolivarian Government strengthens security system with massive expansion of video surveillance"), Ministerio de Interior, Justicia y Paz (@minjusticia_ve), December 20, 2025, https://www.instagram.com/p/DSfy86EEWFm/?img_index=4.

40. Yugreilis Martínez, "Las cámaras de seguridad han sido un apoyo para desarticular bandas delictivas en Guaicaipuro" ("Security cameras have been instrumental in dismantling criminal gangs in Guaicaipuro"), Alcaldía de Guaicaipuro, September 26, 2022, .https://alcaldiadeguaicaipuro.gob.ve/2022/09/26/guaicaipuro-seguridad-ciudadana-31/.

41. "Promesa cumplida: Más ojos en la calle para tu tranquilidad" ("Promise fulfilled: More eyes on the street for your peace of mind"), Farith Fraija (@farithf), Instagram, December 22, 2025, https://www.instagram.com/p/DSkL6-VjaxK/.

42. "Guaicaipuro tiene un sistema de cámaras que es extraordinario," ("Guaicaipuro has an extraordinary camera system, ") Alcaldía de Guaicaipuro, November 13, 2025, https://alcaldiadeguaicaipuro.gob.ve/2025/11/13/ministro-cabello-guaicaipuro-tiene-un-sistema-de-camaras-que-es-extraordinario/.

43. "En materia de seguridad, no se improvisa, hace año y medio pusimos en marcha la instalación de cámaras de seguridad en nuestro municipio" ("When it comes to security, there's no room for improvisation. A year and a half ago, we began installing security cameras in our municipality"), Farith Fraija (@farithf), Instagram, October 25, 2025, Octubre 25, 2025, https://www.instagram.com/reels/DQMMsfKDawr/.

44. Farith Fraija, TikTok video, October 23, 2025, https://www.tiktok.com/@farithf/video/7564491133028420920.

45. "The installation of video surveillance cameras has begun on Bolívar Avenue in the municipality of Valera, as part of the Great Peace Quadrants Mission," Government of Trujillo (@gobtrujillo), Instagram, March 6, 2024,. https://www.instagram.com/reels/C4LZLkJr_i6/.

46. "Bolivarian Government relaunches the 1x10 Good Governance program," Ministry of Science and Technology, October 25, 2025, https://mincyt.gob.ve/gobierno-bolivariano-relanza-del-1x10-del-buen-gobierno/.

47. "Networks of Control: Censorship and Digital Repression in the Presidential Elections in Venezuela," VE sin Filtro, March 26, 2025, https://vesinfiltro.org/noticias/2025-03-26-venezuela-digital-repression-elections/.

48. "The installation of video surveillance cameras has begun on Bolívar Avenue in the municipality of Valera, as part of the Great Peace Quadrants Mission," Government of Trujillo (@gobtrujillo), Instagram, March 6, 2024,. https://www.instagram.com/reels/C4LZLkJr_i6/.

49. "Sistemas de videovigilancia y atención de emergencias en Venezuela"("Video surveillance and emergency response systems in Venezuela"), Transparencia Venezuela, January 2022, https://transparenciave.org/wp-content/uploads/2022/01/Sistemas-de-videovigilancia-y-atencio%CC%81n-de-emergencias-en-Venezuela.pdf.

50. "Public Safety and Homeland Security Bureau announces addition of uncrewed aircraft systems (UAS) and UAS critical components produced abroad, and equipment and services listed in section 1709 of the FY2025 NDAA, to FCC covered list", Federal Communications Commission Public Notice, DA-25-1086A1, December 22, 2025,. https://docs.fcc.gov/public/attachments/DA-25-1086A1.pdf.

51. Ibid.

52. "Treasury Sanctions CEIEC for Supporting the Illegitimate Maduro Regime's Efforts to Undermine Venezuelan Democracy," U.S. Department of the Treasury, November 30, 2020, https://home.treasury.gov/news/press-releases/sm1194.

53. MinServicioPenitenciario, "Delegación China comprueba óptimo funcionamiento del Sitesep" ("Chinese Delegation Verifies Optimal Functioning of Sitesep"), YouTube video, December 2, 2018,, https://www.youtube.com/watch?v=eJRoEuJPmAY."Sistemas de videovigilancia y atención de emergencias en Venezuela" ("Video surveillance and emergency response systems in Venezuela"), Transparencia Venezuela, January 2022, https://transparenciave.org/wp-content/uploads/2022/01/Sistemas-de-videovigilancia-y-atencio%CC%81n-de-emergencias-en-Venezuela.pdf.

54. Scilla Alecci, "US Blacklists Chinese Companies Linked to Uighur Abuses," International Consortium of Investigative Journalists, May 28, 2020, https://www.icij.org/investigations/china-cables/us-blacklists-chinese-companies-linked-to-uighur-abuses/.

55. "¿Conoces los nuevos botones de emergencia instalados por nuestro alcalde @gustavoduquesaez?" (Are you familiar with the new emergency buttons installed by our mayor @gustavoduquesaez?), Policía Municipal de Chacao (@polichacao), Instagram, April 2, 2024, https://www.instagram.com/reels/C5RiA8dOUW0/.

56. "We are pleased to announce that the Caracas Intelligent Foundation has implemented panic buttons at strategic locations throughout our city," Caracas Intelligent Foundation (@caracasinteligente), Instagram, December 18, 2024, https://www.instagram.com/reels/DDu8__iPKO6/.

57. Scilla Alecci, "US Blacklists Chinese Companies Linked to Uighur Abuses," International Consortium of Investigative Journalists, May 28, 2020, https://www.icij.org/investigations/china-cables/us-blacklists-chinese-companies-linked-to-uighur-abuses/.

58. "KIPOD in Venezuela," BELPOL, October 9, 2024, https://belpol.pro/en/kipod-v-venesuele/.

59. "US Treasury Targets Belarusian Support for Russian Invasion of Ukraine", US Department of the Treasury, February 24, 2022, https://home.treasury.gov/news/press-releases/jy0607.

60. Letter from Director A. P. Knysh of the Belarusian company 24x7 Panoptes addressed to Remigio Ceballos, Minister of People's Power for Interior Relations and Justice, provided by BELPOL.

61. "Венесуэльский адмирал изучил работу центра мониторинга общественной безопасности ГУВД Минска" ("Venezuelan Admiral Studies Work of Public Safety Monitoring Center of Minsk Police"), BelTA, November 28, 2023, https://belta.by/society/view/venesuelskij-admiral-izuchil-rabotu-tsentra-monitoringa-obschestven-

noj-bezopasnosti-guvd-minska-602226-2023/.

62. "Diosdado Cabello affirms that now 'there are cameras everywhere': 'Behave yourselves, they are watching you,' Contrapunto, July 17, 2025, https://contrapunto.com/nacional/gobierno/diosdado-cabello-afirma-que-now-there-are-cameras-everywhere-behave-yourselves-they-are-watching-you/.

63. "Security forces thwart terrorist attack in Plaza Venezuela," Últimas Noticias, August 7, 2025, https://www.youtube.com/watch?v=nf1qeRaP.

64. "Relatives of political prisoners in Zone 7 denounce the installation of security cameras in the area where the camps where they spend the night are located," Cristian Crespo F (@cristiancrespoj), X, January 21, 2026, https://x.com/cristiancrespoj/status/2014110234218815677.

65. "Relatives of political prisoners in Zone 7 denounce the installation of security cameras in the area where the camps where they spend the night are located," Cristian Crespo F (@cristiancrespoj), X, January 21, 2026, https://x.com/cristiancrespoj/status/2014110234218815677.

66. "Sistemas de videovigilancia y atención de emergencias en Venezuela," Transparencia Venezuela, January 2021, https://transparenciave.org/wp-content/uploads/2022/01/Sistemas-de-videovigilancia-y-atencio%CC%81n-de-emergencias-en-Venezuela.pdf.

67. "Networks of Control: Censorship and Digital Repression in the Presidential Elections in Venezuela," VE sin Filtro, July 2024, https://vesinfiltro.org/noticias/2024-2025.

68. "EVO Max 4T," Autel Robotics, accessed February 27, 2026, https://shop.autelrobotics.com/products/evo-max-4t-copy.

69. "Ukraine Acquires 2,000 Autel EVO Max 4T China-Made Drones," Army Recognition, October 10, 2023, https://www.armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/ukraine-acquires-2-000-autel-evo-max-4t-china-made-drones."Hunted from Above: Russia's Use of Drones to Attack Civilians in Kherson, Ukraine," Human Rights Watch, June 3, 2025, https://www.hrw.org/report/2025/06/03/hunted-from-above/russias-use-of-drones-to-attack-civilians-in-kherson-ukraine.

70. "Entities Identified as Chinese Military Companies Operating in the United States," U.S. Department of Defense, January 7, 2025, https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF.

71. "This image is for the world: a moment of intense concentration when the leader of the violent, vandalistic protests spoke," Delcy Rodríguez (@delcyrodriguezv), X, August 3, 2024, https://x.com/delcyrodriguezv/status/1819823973586153615.

72. "Autel DG-L35T Gimbal Zoom Effect Demo," Autel Robotics, https://www.autelrobotics.com/videos/autel-alpha/.

73. "Networks of Control: Censorship and Digital Repression in the Presidential Elections in Venezuela," VE sin Filtro, July 2024, https://vesinfiltro.org/noticias/2024-2025.

74. Ibid.

75. "El régimen de Maduro desplegó drones sobre Caracas para vigilar e infundir terror a los ciudadanos que salgan a protestar," Infobae, August 3, 2024, https://www.infobae.com/venezuela/2024/08/03/el-regimen-de-maduro-desplego-drones-sobre-caracas-para-vigilar-e-infundir-temor-a-los-ciudadanos-que-salgan-a-protestar/.

76. "ALERTA Desde hace unas horas, agentes del régimen han rodeado la casa de mi mamá, han puesto alcabalas en toda la urbanización y sobrevolado con drones. También 'se fue' la luz en la zona," M .C. Machado (@MariaCorinaYA), X, January 7, 2025, https://archive.is/5weYI.

77. "URGENTE!!! Los efectivos de la DAET y del SEBIN asedian la sede de la Embajada de Argentina en Caracas, protegida por Brasil. Ahora, sobrevuelan drones y también bloquean la señal móvil," Pedro Urruchurtu (@Urruchurtu), X, November 23, 2024, https://archive.is/EDEYy

78. "Government attributes explosions near Miraflores to drones and warning shots" Sumarium, January 6, 2026, https://sumarium.info/2026/01/05/se-producen-detonaciones-cerca-del-palacio-de-miraflores/.

79. TK-103 device documented by VEsinFiltro through visual matching of the device.

80. "CAR GSM/GPRS/GPS TRACKER SIM 12-24VDC WITH REMOTE TK103B" ABCLED https://abcled.ee/en/gps-tracker/5349-car-gsm-gprs-gps-tracker-sim-12-24vdc-with-remote-.html

81. "A device was installed in the vehicle of Margareth Baduel... during the Global Route for the Freedom of Political Prisoners event," VPItv (@VPITV), X, September 19, 2025, https://archive.ph/aNVky.

82. Kejal Vyas, "Venezuelan Army General Who Saved Hugo Chávez from Coup Dies in Jail," Wall Street Journal, October 13, 2021, https://www.wsj.com/world/americas/venezuelan-army-general-who-saved-hugo-chavez-from-coup-dies-in-jail-11634156236.

83. "URGENT REPORT: Officials fail to explain the nature of the device placed in Margareth Baduel's vehicle during the closure of the #GlobalRouteForJustice", Committee for the Freedom of Political Prisoners (@clippve), X, September, 19, 2025, https://archive.is/oUdtn.

84. "SinoTrack GPS Tracker for Vehicles,4G LTE GPS Tracking Device,ST-915L Real time Strong Magnetic Tracker for Car Motorcycle Taxi Truck Bus", SinoTrack on Amazon.com https://www.amazon.com/SinoTrack-ST-915L-Waterproof-Real-Time-Motorcycle/dp/B09K3SKM9F

85. Código Orgánico Procesal Penal. Art 295., http://www.mp.gob.ve/LEYES/CODIGO_OPP/index.html.

86. Iria Puyosa, Andrés Azpurua, and Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," Atlantic Council, July 2024, https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

87. WHOIS information, whois.patria.org.ve, accessed May 24, 2024, https://who.is/whois/patria.org.ve, https://archive.is/6ozvb.

88. Andrea Tosta, "El carrusel del PSUV: estocada final al voto

secreto," El Estímulo, December 19, 2017, https://elestimulo.com/climax/politica/2017-12-19/el-carrusel-del-psuv-estocada-final-al-voto-secreto/.

89. "Snitch Law," Wikipedia, last modified January 15, 2025, https://en.wikipedia.org/wiki/Snitch_Law.

90. Iria Puyosa, Andrés Azpurua, and Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," Atlantic Council, July 2024, https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

91. Iria Puyosa and Daniel Suárez Pérez, "How the Venezuelan regime weaponized video and messaging apps to persecute dissidents," Atlantic Council, September 2024, https://dfrlab.org/2024/09/23/venezuela-weaponizes-apps/.

92. "Conexión Venezuela-Panamá: ¿quiénes desarrollaron a VenApp?" ("Venezuela-Panama Connection: Who Developed VenApp?"), Cazadores de Fake News, May 20, 2022, https://www.cazadoresdefakenews.info/conexion-venezuela-panama-quienes-desarrollaron-a-venapp/.

93. "#TeExplicamos | ¿Qué es VenApp y por qué despierta alertas sobre vigilancia y control en Venezuela?", El Diario, October 27, 2025, https://eldiario.com/2025/10/27/teexplicamos-que-es-venapp-alertas-sobre-vigilancia-y-control-en-venezuela/.

94. "Gobierno pide crear un apartado en Venapp para la vigilancia vecinal" ("Government requests creation of section in VenApp for neighborhood surveillance"), Espacio Público, October 21, 2025, https://espaciopublico.ong/gobierno-pide-crear-un-apartado-en-venapp-para-la-vigilancia-vecinal/#footnote_3_43190.

95. "Manual Redes, Calles, Medios, Paredes y Radio Bemba," March 13, 2025, https://presidencia.gob.ve/Site/Web/Principal/imagenes/adjuntos/Web/Libros/PDF/Libro95.pdf.

96. Iria Puyosa, Andrés Azpurua, and Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," Atlantic Council, July 2024, https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

97. John Otis. "Pressure on Venezuela's Media Worsening," Committee to Protect Journalists, October 18, 2013, https://cpj.org/2013/10/pressure-on-venezuelas-media-worsening/.

98. "Networks of Control: Censorship and Digital Repression in the Presidential Elections in Venezuela," VE sin Filtro, July 2024. https://vesinfiltro.org/noticias/2024-2025.

99. Iria Puyosa and Daniel Suárez Pérez, "How the Venezuelan regime weaponized video and messaging apps to persecute dissidents," Atlantic Council, September 2024, https://dfrlab.org/2024/09/23/venezuela-weaponizes-apps/."Tun Tun: La maquinaria ciber represora del gobierno de Venezuela, al descubierto," Cazadores de Fake News, October 28, 2024, https://www.cazadores.info/tun-tun-la-maquinaria-ciber-represora-del-gobierno-de-venezuela-al-descubierto/.

100. "Tun Tun: La maquinaria ciber represora del gobierno de Venezuela, al descubierto," Cazadores de Fake News, October 28, 2024, https://www.cazadores.info/tun-tun-la-maquinaria-ciber-represora-del-gobierno-de-venezuela-al-descubierto/.

101. "Networks of Control: Censorship and Digital Repression in the Presidential Elections in Venezuela," VE sin Filtro, March 26, 2025, https://vesinfiltro.org/noticias/2025-03-26-venezuela-digital-repression-elections/.

102. "Operation Knock Knock: On the Hunt for Dissident Voices in Venezuela," Global Voices Advox, September 12, 2024, https://advox.globalvoices.org/2024/09/12/operation-knock-knock-on-the-hunt-for-dissident-voices-in-venezuela/. Iria Puyosa and Daniel Suárez Pérez, "How the Venezuelan regime weaponized video and messaging apps to persecute dissidents," Atlantic Council, September 2024. https://dfrlab.org/2024/09/23/venezuela-weaponizes-apps/.

103. "Networks of Control: Censorship and Digital Repression in the Presidential Elections in Venezuela," VE sin Filtro, March 26, 2025, https://vesinfiltro.org/noticias/2025-03-26-venezuela-digital-repression-elections/.

104. "Networks of Control: Censorship and Digital Repression in the Presidential Elections in Venezuela," VE sin Filtro, March 26, 2025, https://vesinfiltro.org/noticias/2025-03-26-venezuela-digital-repression-elections/.

105. "Venezuela's military counterintelligence agency posted a chilling video this morning of María Oropeza, a young organizer for the opposition campaign…", Alex Bare (@alexbaretv), X, August 8, 2024, https://x.com/alexbaretv/status/1821630754176086487, https://archive.is/PlLu7.

106. "Venezuela: Tech Companies Set Dangerous Precedent with App for Reporting Anti-Government Protesters," Amnesty International, August 28, 2024, https://www.amnesty.org/en/latest/news/2024/08/venezuela-tech-companies-set-dangerous-precedent-with-app-for-reporting-anti-government-protesters/.

107. "Corte de Apelaciones anula condena de 15 años contra estudiante de periodismo Juan Francisco Alvarado." Sindicato Nacional de Trabajadores de la Prensa, January 24, 2026,https://sntpvenezuela.org/corte-de-apelaciones-anula-condena-de-15-anos-contra-estudiante-de-periodismo-juan-francisco-alvarado/.

108. "Condenan a 30 años de prisión a una doctora por expresarse a través de un audio de WhatsApp," Espacio Público, November 18, 2025, https://espaciopublico.ong/condenan-a-30-anos-de-prision-a-una-doctora-por-expresarse/.

109. "Madre de Randal Telles, condenada a 15 años de prisión por un video en TikTok, clama su libertad," Espacio Público, November 22, 2025, https://espaciopublico.ong/madre-randal-telles-condenada-15-anos-video-tiktok-clama-libertad/.

110. "Nakary Mena, la única mujer periodista presa en Venezuela: no se puede tener arcoíris sin lluvia," Sindicato Nacional de Trabajadores de la Prensa, July 17, 2025, https://sntpvenezuela.org/nakary-mena-la-unica-mujer-periodista-presa-en-venezuela-no-se-puede-tener-arcoiris-sin-lluvia/.

111. "Hermana de Marcos Palma: Nunca pensamos que por la difusión de un audio lo pusieran preso y condenaran," Espacio Público, October 22, 2025, https://espaciopublico.ong/hermana-marcos-palma-nunca-pensamos-audio-preso/.

112. The historical Venezuelan flag originally featured seven stars, representing the seven provinces that signed the

Venezuelan Declaration of Independence on July 5, 1811. In 2006, President Chávez ordered the addition of an eighth star to symbolize the province of Guayana, which joined the independence camp in 1817. The Venezuelan opposition has consistently used the seven-star flag as part of its broader effort to contest Chávez's attempt to re-write the country's history.

113. "Jesús Gabriel Molina Sifontes (27), oficial activo de la Fuerza Armada Nacional Bolivariana y licenciado en Ciencias Navales, fue detenido arbitrariamente el 1 de agosto de 2024 tras culminar sus funciones en el Plan República durante las elecciones presidenciales del 28 de julio," Foro Penal (@ForoPenal), X, January 30, 2026, https://x.com/ForoPenal/status/2017298849128194547.

114. "Compartir imágenes de recompensas ofrecidas por EEUU le costó la libertad a Rory Branker," Sindicato Nacional de Trabajadores de la Prensa, January 31, 2026, https://sntpvenezuela.org/compartir-imagenes-de-recompensas-ofrecidas-por-eeuu-le-costo-la-libertad-a-rory-branker/.

115. "Detailed findings of the Independent International Fact-Finding Mission on the Bolivarian Republic of Venezuela (A/HRC/57/CRP.5)", UN OHCHR, October 15, 2024, https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session57/advance-versions/a-hrc-57-crp-5-en.pdf.

116. Constitution of the Bolivarian Republic of Venezuela (1999), Article 60. https://www.constituteproject.org/constitution/Venezuela_2009#s220.

117. Ley Orgánica de Telecomunicaciones ("Organic Law on Telecommunications"), Organization of American States, March 28, 2000, https://www.oas.org/juridico/spanish/cyb_ven_ley_telecomunicaciones.pdf.

118. Ley sobre Protección a la Privacidad de las Comunicaciones ("Law on Protection of Communication Privacy"), 1991, https://venezuela.justia.com/federales/leyes/ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones/gdoc/.

119. "Venezuela: Freedom on the Net—Country Report 2012," Freedom House, https://freedomhouse.org/sites/default/files/Venezuela%202012.pdf.

120. "Informe de Transparencia en las Comunicaciones 2021" ("Communications Transparency Report 2021"), Telefónica, June 18, 2022, https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf..

121. "Maduro administration is spying on Venezuelans at a massive scale", VEsinFiltro, June 22, 2022. https://vesinfiltro.org/noticias/venezuela-communications-spying/

122. Ibíd.

123. "Informe de Transparencia en las Comunicaciones 2021" ("Communications Transparency Report 2021"), Telefónica, June 18, 2022, https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf..

124. Iria Puyosa, Andrés Azpurua, and Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," Atlantic Council, July 2024, https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

125. "Informe de Transparencia en las Comunicaciones 2021" ("Communications Transparency Report 2021"), Telefónica, June 18, 2022, https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf..

126. Ibid.

127. "Maduro administration is spying on Venezuelans at a massive scale," VEsinFiltro, June 22, 2022, https://vesinfiltro.org/noticias/venezuela-communications-spying/.

128. Iria Puyosa, Andrés Azpurua, and Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," Atlantic Council, July 2024, https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

129. Criminal Processing Code, Article 291, https://tugacetaoficial.com/penal/copp-articulo-291/#:~:text=COPP%20Art%C3%ADculo%20291%20%2D%20C%C3%B3digo%20Penal%20y%20C%C3%B3digo%20Org%C3%A1nico%20Procesal%20Penal.

130. "Caracas: South Lighthouse, Fake Antenna Detention" and "Venezuelan Colombian Border," FaDe Project, March 2020, https://fadeproject.org/?project=caracas and https://fadeproject.org/?project=venezuelan-colombian-border.

131. Isabel Guerrero, "En estos puntos rojos tu celular es un libro abierto" ("In these red points your cell phone is an open book"), Armando.info, September 6, 2020, https://armando.info/en-estos-puntos-rojos-tu-celular-es-un-libro-abierto/.

132. Law on Protection of Communication Privacy, Venezuela, 2001, https://venezuela.justia.com/federales/leyes/ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones/gdoc/.

133. Organic Law on Telecommunications, Organization of American States, March 28, 2000, https://www.oas.org/juridico/spanish/cyb_ven_ley_telecomunicaciones.pdf.

134. "La Ley de Transparencia Aprobada por la Asamblea Nacional Consolida el Secretismo ("Transparency Law Approved by the National Assembly Consolidates Secrecy"), Transparencia Venezuela, September 17, 2021, https://transparenciave.org/la-ley-de-transparencia-aprobada-por-la-asamblea-nacional-consolida-el-secretismo/.

135. Iria Puyosa, Andrés Azpurua, and Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," Atlantic Council, July 2024, https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

136. Phishing is an attack that seeks to deceive the victim into taking action that exposes their security, privacy, device security, or causes financial loss through messages, calls, or websites that appear to be from other people or organizations.

137. Andrés Azpúrua and Carlos Guerra, "Phishing by Venezuelan Government Puts Activists and Internet Users at Risk," VE sin Filtro, February 15, 2019, https://vesinfiltro.com/noticias/Phishing_by_Venezuelan_government_targets_activists/.

138. Ibid.

139. WHOIS is a query and response protocol used to query databases storing registered users or assignees of internet resources such as domain names and IP addresses. See "WHOIS Protocol Specification," RFC 3912, https://www.rfc-editor.org/rfc/rfc3912.

140. The Tascón List is a database of Venezuelans who signed a petition requesting a recall referendum against then-President Hugo Chávez in 2003. For years, it was used to dismiss those appearing on it from public administration employment, deny them public services and passports, and subject them to other forms of discrimination.

141. "Especial IPYS: Bloqueos, robo de datos y contenidos falsos: la nueva forma de interceptar la red venezolana," IPYS Venezuela, February 20, 2019, https://ipysvenezuela.org/alerta/especial-ipys-bloqueos-robo-de-datos-y-contenidos-falsos-la-nueva-forma-de-interceptar-la-red-venezolana/.

142. "State-sponsored Phishing Against Healthcare Workers Amid COVID-19 Pandemic in Venezuela," VE sin Filtro, April 27, 2020, https://vesinfiltro.com/noticias/2020-04-26-phishing_healthcare_heroes.

143. "Phishing Campaign Targets Opposition Electoral Organizing," VE sin Filtro, June 27, 2024, https://vesinfiltro.org/noticias/2024-06-27-phishing-comandito/.

144. "Infiltrar, robar datos, estigmatizar, atacar," Cazadores de Fake News, August 26, 2024, https://www.cazadoresdefakenews.info/infiltrar-robar-datos-estigmatizar-atacar/.

145. "Hackean cuentas en Instagram de periodistas venezolanos," Espacio Público, September 16, 2024, https://espaciopublico.ong/hackean-cuentas-en-instagram-de-periodistas-venezolanos/.

146. "ME HACKEARON MI CUENTA DE X," Prakriti Maduro (@prakritimaduro), X, September 12, 2024, https://x.com/prakritimaduro/status/1834383254633509138.

147. Conversation between the surveillance target and Conexion Segura discussing digital security measures, December 2025.

148. Interview with a family member who assisted the journalist Nelson Bocaranda when trying to handle the case and recover his account.

149. Interviews with the victim, 2023.

150. "Networks of Control: Censorship and Digital Repression in the Presidential Elections in Venezuela," VE sin Filtro, March 26, 2025, https://vesinfiltro.org/noticias/2025-03-26-venezuela-digital-repression-elections/.

151. Ibid.

152. The username "LaListaMachado" is a reference to the Tascón List. This reference has been used previously as intimidation in relation to other phishing campaigns, including the campaign against VoluntariosXVenezuela.

153. "Networks of Control: Censorship and Digital Repression in the Presidential Elections in Venezuela," VE sin Filtro, March 26, 2025, https://vesinfiltro.org/noticias/2025-03-26-venezuela-digital-repression-elections/.

154. Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune, "Mapping FinFisher's Continuing Proliferation," Citizen Lab, October 15, 2015, https://citizenlab.ca/research/mapping-finfishers-continuing-proliferation/.

155. Katherine Pennacchio, "Hacking Team casi corona en Venezuela," Armando.info, July 18, 2015, https://armando.info/hacking-team-casi-corona-en-venezuela/.

156. "Hacking Team Email Archive,email ID 359273," WikiLeaks, https://wikileaks.org/hackingteam/emails/emailid/359273.

157. Katherine Pennacchio, "Hacking Team casi corona en Venezuela," Armando.info, July 15, 2015, https://armando.info/hacking-team-casi-corona-en-venezuela/.

158. "The Small Spyware Providers Who Operate Outside the Limelight," Intelligence Online, January 6, 2026, https://www.intelligenceonline.com/americas/2026/01/06/the-small-spyware-providers-who-operate-outside-the-limelight,110590674-art.

159. Laura Vidal, "Unveiling Venezuela's Repression: Surveillance and Censorship Following July's Presidential Election," Electronic Frontier Foundation, September 16, 2024, https://www.eff.org/deeplinks/2024/09/unveiling-venezuelas-repression-surveillance-and-censorship-following-julys.

160. "Estado de conmoción exterior en Venezuela: alcance y riesgos" ("State of External Commotion in Venezuela: Scope and Risks"), Acceso a la Justicia, January 15, 2026, https://accesoalajusticia.org/estado-conmocion-exterior-venezuela-alcance-riesgos/.

161. Venezuela's Constitution of 1999 nominally protects the inviolability of private communications in Article 48, but this protection has been systematically ignored by security forces, particularly during periods of political repression following contested elections. See "Balance #4Ago: 88 casos en medio de crisis política en Venezuela," Espacio Público, August 5, 2025, https://espaciopublico.ong/balance-4ago-88-casos-en-medio-de-crisis-politica-en-venezuela/.

162. VE sin Filtro, documentation of migration control procedures, January 2026.

163. "Autoridades de la UCV rechazan despliegue militar y policial durante visita de Delcy Rodríguez: «Es una violación a la autonomía»," El Pitazo, January 31, 2026, https://elpitazo.net/regiones/gran-caracas/autoridades-de-la-ucv-rechazan-despliegue-militar-y-policial-durante-visita-de-delcy-rodriguez-es-una-violacion-a-la-autonomia/.

164. The Venezuelan Constitution and the Law of National Universities guarantee territorial immunity for university campuses, meaning that police or military officers cannot enter these areas.

165. Oded Yaron, "Despite Sanctions, Israeli Firm Cellebrite Sold Phone-hacking Tech to Venezuela," Haaretz, September 10, 2020, https://www.haaretz.com/israel-news/tech-news/2020-09-10/ty-article/.premium/despite-sanctions-israeli-firm-sold-phone-hacking-tech-to-venezuela/0000017f-f355-df98-a5ff-f3fdba8c0000.

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

© 2026 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226
www.AtlanticCouncil.org