

## [In Venezuela, Digital Freedom Is a Threat to Dictators](#)

Story by Jorge Jraissati



In Venezuela, Digital Freedom Is a Threat to Dictators

© Reason

As Nicolás Maduro [bans](#) X and Signal, the role of technology in Venezuela becomes undeniable. Now more than ever, people's freedom lies in their ability to communicate and access information with privacy and security. This is true not only in Venezuela but also in the United States.

### **Maduro's Repression**

"I feel like a Jew in Nazi Germany. The regime's security forces are going door by door, arresting human rights activists," a 21-year-old activist from Barquisimeto in northwest Venezuela, who asked to remain anonymous, told me.

His words reflect the terrifying reality for many Venezuelans today. About [2,000 activists](#) have been detained by the government in the aftermath of the country's July 28 presidential election—an election marred by Maduro's blatant [manipulation](#) to secure his grip on power.

Just as the Soviets once did, Maduro is encouraging people to report citizens who sympathize with the opposition. But unlike before, Venezuelans can use an app called VenApp. Launched by Maduro, the app was originally [designed](#) to receive public complaints, such as power outage reports.

In the past two weeks, security forces have been systematically stopping citizens to inspect their phones, including photos, social media profiles, and WhatsApp conversations. Detainees are often held based on content uncovered during these searches, such as images or conversations related to protests or anti-government expressions.

This shows Maduro's willingness to crack down on dissent. It also shows the crucial role of technology in this fight for freedom. We use privacy messaging apps like Signal to communicate sensitive

information. We rely on X and Nostr to share public information with the Venezuelan people. And we use bitcoin to overcome Maduro's financial surveillance.

Regimes know this, which is why the Maduro government has been updating its surveillance system. They are doing this in cooperation with other autocratic regimes. For example, the Chinese company ZTE has been supplying Maduro with advanced surveillance technology, [according](#) to nongovernmental organizations.

This is also why Maduro [banned](#) X and Signal for 10 days across Venezuela, claiming his opponents were using these platforms to incite political unrest. This unprecedented measure in the Western hemisphere sets a dangerous precedent in the region. It also shows how regimes can restrict essential technologies, including their privacy tools and communication platforms.

### **Building a Tech-Based Strategy**

In today's digital age, privacy technology is not just a tool; it's a critical battleground in the fight against authoritarianism and a vital means of defending human rights. To protect our freedoms—whether in information, communication, or finance—we must develop and implement a comprehensive strategy based on privacy technology that empowers individuals living under repressive regimes.

Central to this strategy is the promotion and protection of freedom technologies. This includes the development and investment in the decentralized ecosystem of bitcoin and Nostr, as well as private communication platforms like X and SimpleX. These privacy tools are lifelines to activists and ordinary citizens, enabling them to bypass censorship, protect their financial autonomy, and organize without fear of surveillance.

A close collaboration between activists and technologists would also help ensure that new freedom tech tools and platforms are developed with the specific needs of those under repression in mind. We need more initiatives that unite software developers, youth leaders, freedom activists, and nonprofit organizations to create solutions that protect privacy, facilitate secure communication, and enable digital organizing.

But perhaps more importantly, we should challenge democratic governments to stop enacting policies that undermine freedom and privacy. Laws that erode our digital privacy are not only incompatible with a free society, but they also empower dictators. When democracies undermine people's privacy, they give dictators the legitimacy to do the same.

In the financial sector, for example, governments have enormous power over citizens' bank accounts. Global regulations meant to tackle financial crimes allow governments to arbitrarily block people's bank accounts, freeze their assets, and access their banking data, among other measures. This means that the financial data of any American can be attacked by states and competitors all over the world, including Chinese firms. Most Americans are shocked when I talk to them about this.

Unfortunately, financial laws are being misused by regimes to oppress their dissidents at home and in exile. For example, in 2022, the Canadian government [froze the bank accounts](#) of the truck drivers protesting the cross-border vaccine mandate between Canada and the U.S. This issue must be urgently addressed. It's a global reform process that my organization, the Economic Inclusion Group, started back in 2023.

A similar situation occurs in the bitcoin space. Around the world, activists in autocratic countries use bitcoin to circumvent regime surveillance and repression. Without bitcoin, they would struggle to receive donations, distribute funds, and maintain a semblance of normalcy in their lives. For them, bitcoin has become a powerful tool against autocracy.

For this reason, policymakers in the West should be promoting and celebrating the use of bitcoin worldwide, especially since this freedom technology was created and is developing in Western democracies. Instead, they remain fixated on concerns that bitcoin's privacy features might enable criminal activity and money laundering. While this allegation was [disproved](#) by institutions like the U.S. Treasury Financial Crimes Enforcement Network (FinCEN), these concerns continue to be propagated by lawmakers such as Sen. Elizabeth Warren (D–Mass.).

Ultimately, the situation in Venezuela illustrates the importance of freedom technologies in safeguarding liberty. China and other authoritarian regimes recognize the value of these digital freedoms and have responded by cracking down on them. Protecting privacy tools is not just a matter of personal freedom; it is a national security issue and essential for the future of democracy globally. American policymakers must lead on this front to ensure that democracy prevails during this difficult time in history. Whether in Venezuela or the West, the fight for freedom will be determined in the technological arena. It's a fight we cannot afford to lose.

The post [In Venezuela, Digital Freedom Is a Threat to Dictators](#) appeared first on [Reason.com](#).

**\*The Open Dialogue Foundation, Inc. is registered as an agent of the Open Dialogue Foundation located in Brussels, Belgium under 22 U.S.C. § 611 et seq.**

**These materials are distributed by the Open Dialogue Foundation, Inc. on behalf of the Open Dialogue Foundation.**

**Further information is on file with the Department of Justice, Washington, DC.**