


DIGITAL RIGHTS

VENEZUELA 2024

Report on the relationship between
the political and social crisis and the
exercise of fundamental rights in
digital environments





My main concern is that “everything
you say can be used against you, in a
country without the rule of law, where
with just one post, you can be
sentenced to jail, even if you only
share one post”

Testimony of a journalist

Index

Summary	1
Context	2
Research scope	3
Methodology	5
Documentary Sources	6
Field work and collection of opinions	7
Data Analysis	7
History of censorship and internet blocking in authoritarian countries	8
Legislation on Digital Human Rights in Venezuela	10
Freedom of expression on the internet	19
Blocking web portals	19
Information blocking strategies	20
Punitive hashtags	21
Organizations and companies of the Venezuelan State involved	24
Accessibility to information	25
Affection of the population by the crisis of services	25
Historical Patterns between Power Outages and Connectivity	28
Training defenders on cybersecurity	29
Institutional cyber violence	30
Pre-election perception of digital security	30
Post-electoral situation of digital security	39
Dismissal of public sector workers	48
Patterns of persecution associated with the exercise of digital rights	49
Institutional violence towards women	51
Legal provisions violated	52
Conclusions	55
Recommendations	57
Bibliographic references	60

Summary

This report addresses the relationship of the political and social crisis on the exercise of fundamental rights in digital environments in Venezuela, in a context characterized by censorship, state surveillance and restrictions on access to information, highlighting that this study focuses on three axes: freedom of expression on the Internet, institutional cyberviolence and accessibility to information.

It was prepared between the months of July and November with information collected in collaboration with human rights defenders, journalists, union leaders and electoral observers from the states of Bolívar, Lara, Táchira and Yaracuy, using a methodology that combines documentary review and citizen testimonies. , however, not only documents the current situation, but also seeks to propose recommendations to promote a freer and fairer digital environment, and encourage constructive dialogue between academics, human rights defenders and civil society.

The report on the monitoring of digital rights in Venezuela in 2024 states that 90% of the defenders surveyed decreased the number of their publications after the presidential elections, and that at least 33 blocks of web portals were registered; For this reason, it is a call to action and reflection on the role of technology in contemporary societies, through a rigorous and collaborative analysis, with which it was proposed to offer a clear panorama of the reality that Venezuela faces in the digital sphere. , while opening spaces for dialogue and possible solutions to guarantee the respect and promotion of digital rights in a challenging environment.

Context

The accelerated digitalization that has transformed not only the way we communicate, but also how we exercise our fundamental rights, including digital rights, has meant in Venezuela going through a complex phenomenon, where the institutional crisis and restrictions on civil liberties have been compromised by a series of decisions emanating from the Venezuelan State, both legal and extra-legal in nature. The year 2024 stands as a crucial moment to reflect on the state of digital rights in the country, given that complaints have increased about systematic violations of privacy, freedom of expression, access to information, but more. Even more worrying is the use of digital space to exercise institutional violence against citizens.

In Venezuela, the political and social crisis has been accompanied by tight control by the State over the digital space, through the implementation of laws that limit access to information and mass surveillance of citizens have configured an environment where Exercising digital rights has become risky. Censorship in the media, both traditional and on digital platforms, has been increasing, in an attempt to silence critical voices, considering that prior to the campaign for the presidential elections, 53 news websites were already blocked. Content blocking and filtering policies have restricted access to relevant information, especially the organization of social movements that seek to defend human rights and democracy.

The main objective of this report was to carry out an exhaustive analysis of the situation of digital rights in Venezuela during the year 2024, focusing on three fundamental axes: freedom of expression on the internet, citizenship as part of the group of victims of institutional cyber violence and accessibility to information; To this end, a methodology was implemented that combines the review of documentary material, including laws, doctrines and opinions of international organizations, as well as field research that allows capturing the experience of citizens in their interaction with the digital space.

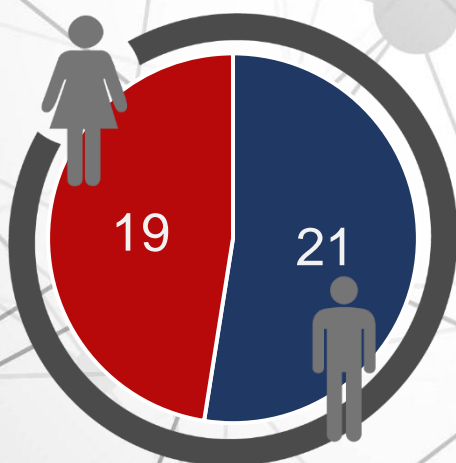
The investigation was not exclusively focused on documenting the current situation, but also on recommending actions that contribute to strengthening digital rights in Venezuela, at a time where technology can be a powerful tool for the defense of human rights, it is imperative that these tools are used to empower citizens and not to repress their voice.

Research scope

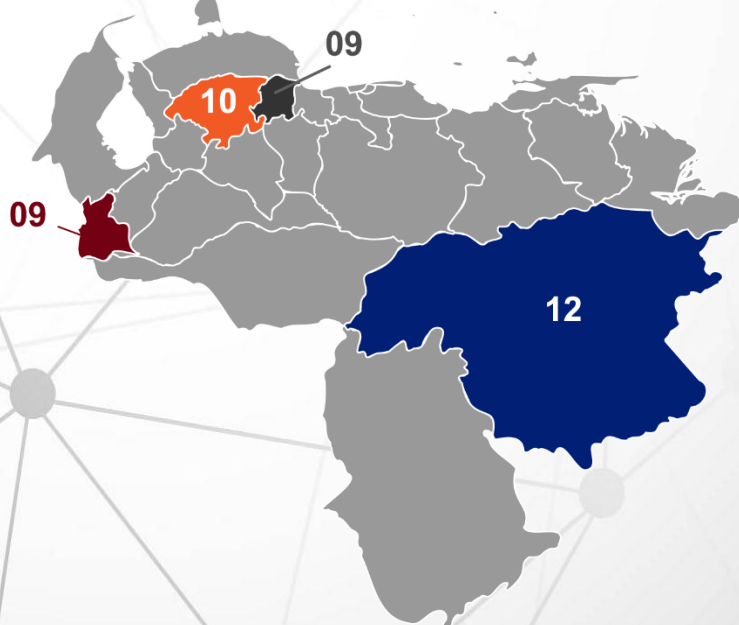
This study, whose objective is to analyze the effects of the political crisis linked to the presidential elections on the exercise of fundamental rights in digital environments in Venezuela, was developed in four months from July to November 2024.

For this, 40 human rights defenders participated, including journalists, union leaders, activists from non-governmental organizations and electoral observers, distributed among those surveyed in the states of Bolívar (30%), Lara (25%), Táchira (22.5%) and Yaracuy (22.5%).

GENDER DISTRIBUTION



GEOGRAPHIC AREA



The ages of the study subjects are between 21 and 65 years old, with a predominance of the group comprised of young people (40% of the sample), the distribution being expressed as follows:

AGE RANGE



These entities have in common a very active long-standing union agenda and have registered cases of persecution of public sector workers and against the population in general due to the tendency to raise their critical voice against the arbitrary actions of the State towards the population. Venezuelan.

Likewise, they have been subject to constant electrical interruptions and voltage fluctuations, which the government of Nicolás Maduro has attributed to alleged plans of the opposition to "destabilize" society and the economy, for which they have exercised repressive actions and maintain a policy of intimidation against those who make complaints about the situation of this public service, and especially, making use of social networks.

In the four selected states there is a presence of the groups considered as objects of study in the current investigation, taking into account that in the context of the presidential elections they have been in charge of investigating, documenting, monitoring, denouncing and reporting on any irregular event that contrast with the statements of figures from the ruling party.



Methodology

In Venezuela, the collection of information on digital rights related to human rights on the Internet has required the use of various methodologies to study the relationship between technology and the defense of human rights.

In this research, one of the most used has been the documentation of specific cases of digital rights violations, which consisted of collecting information on incidents of censorship, online harassment, privacy violations and other abuses.

Likewise, we resorted to the use of surveys, which allowed various entities to measure the population's perception of freedom of expression and access to online information, thus obtaining quantifiable data that allows us to visualize trends in digital rights.

As a complement, it was also chosen to address a participatory research approach, in which the affected communities were involved in the data collection process, adapting to the context covered by the research, highlighting that this method not only empowers people in documenting their experiences, but also ensuring that the data collected is representative and contextualized.

The use of data analysis tools has grown in popularity in the context of digital rights. Research analyzing patterns of censorship or harassment on social media platforms has become common.

Another relevant methodology has been the holding of training workshops and workshops on digital protection and human rights. Through these initiatives, activists and journalists are trained in the secure collection and handling of information, ensuring they understand the importance of documenting and reporting violations, as well as the best practices for doing so.

The preparation of the report on the situation of Internet freedom and human rights in Venezuela has required a comprehensive methodological approach that combines an exhaustive review of documentary sources and a detailed analysis of empirical data collected from field work. This process has allowed us to understand the complexity of the digital environment in Venezuela, where censorship and repression are palpable realities for human rights defenders and citizens in general.

Documentary Sources

A documentary analysis was carried out that covered multiple sources, including: current laws, regulatory standards and public policies that affect freedom of expression and access to information in the digital environment, being essential to identify the legislative tools that the State has used to justify censorship and

surveillance of citizens. In addition, documents prepared by experts in digital matters, academic research and reports from non-governmental organizations that have monitored the human rights situation in Venezuela were consulted. These documents provided critical context and evidence about the control and repression policies implemented in the country.

Field work and collection of opinions

Field work actions were carried out that included the application of surveys to Internet users in various regions of Venezuela. These surveys were designed to capture citizens' experiences and perceptions of freedom in the digital space, as well as to identify the challenges they face daily when trying to access information and communicate online. Questions were included about self-censorship, fear of retaliation for expressing opinions, and perceptions of digital security.

In addition, in-depth interviews were conducted with human rights defenders, activists and technology specialists who have directly experienced state repression in the digital environment. These interviews provided valuable qualitative information, revealing both their personal experiences and their views on resistance strategies against censorship.

Data Analysis

Once the documentary and empirical data were collected, an analysis was carried out that combined qualitative and quantitative methods. Survey data were analyzed statistically to identify trends and patterns, while interviews were analyzed using a qualitative approach that allowed recurring themes and meaningful narratives to be extracted. This triangulation of methodologies guaranteed a deeper and more robust understanding of the phenomenon studied, by integrating both the legal perspective and the real experiences of citizens in the context of Internet freedom.

History of censorship and internet blocking in authoritarian countries

Censorship in the digital sphere is a phenomenon that has been seen and intensified in various parts of the world; each government has its own justifications and methods to implement it. Below is some relevant background information in different contexts and countries:

China

1. *Great Firewall*: A complex internet filtering and censorship system is used to block access to websites and control the information that circulates on the network. This includes foreign social media platforms such as Facebook and social networks.
2. *Content control*: The Chinese government closely controls content published on national platforms, censoring any criticism of the Communist Party or its leaders. It has also used strategies such as buying advertising overwhelmingly to display its propaganda and narratives, as happened with Twitter today "X", during the Hong Kong protests of 2021, despite the fact that this network has been blocked in China since 2009.

Russia

1. *Blogging Law*: Since 2014, Russia implemented laws requiring bloggers and website owners that have more than 3,000 daily visitors to register and comply with state regulations. This allows the government to monitor and censor content.
2. *Social media control*: The Kremlin has blocked or restricted access to social networks such as LinkedIn and has threatened sanctions to platforms that do not comply with its data laws, this is the case of the Roskomnadzor agency, which is The Federal Supervision Service Telecommunications, Information Technology and Media, blocked Twitter and Facebook in 2022, during the beginning of the Russian invasion of Ukraine.

Iran

1. *State censorship*: Iran regularly blocks access to a number of platforms and websites, including Facebook and Twitter, arguing that they are tools of social and political destabilization. Different leaders of the country have been responsible for filtering information from the Internet that is not aligned with the Islamist current of the ruling party.

2. *Surveillance*: The Iranian government also uses surveillance technology to monitor and silence dissidents online, especially during periods of protests.

Nicaragua

1. *Press restrictions*: Since 2018, the Nicaraguan government has intensified its control over the media and has closed or censored critical outlets. The repression has extended to digital platforms.

2. *Site blocking*: Several organizations have denounced the blocking of news portals and social networks, particularly those that report on human rights violations. On October 27, 2020, the Nicaraguan government approved the Cybercrime Law in the Nicaraguan Congress, to combat what the Ortega government defines as false news.

Cuba

1. *Strict control*: The Cuban government controls access to the internet and limits platforms that allow free expression. Although internet access has opened up in recent years, censorship remains a problem.

2. *Temporary disconnections*: During protest or criticism events, temporary disconnections of internet service have been reported. In 2019, Decree 370 came into force, which regulates and penalizes the use of the internet to penalize those who publish and share information that is considered contrary to the government.

In general, digital censorship is a global phenomenon that manifests itself in different ways and with different justifications. The trend is towards greater State control over digital information, especially in tense political contexts or in preparation for elections.

Legislation on Digital Human Rights in Venezuela

In Venezuela, several laws and regulations have been considered restrictive of digital rights and freedom of expression in the digital environment. Below are some of the most relevant laws in this context:

Law on Social Responsibility in Radio, Television and Electronic Media (Spring Law): Enacted in 2004, this law regulates media content, including digital platforms. It establishes strict requirements on the transmission of information and sanctions the dissemination of content considered "destabilizing" or that contravenes the "values" of the nation. This has led to censorship and self-censorship of many media.

Organic Telecommunications Law: This law, in force since 2000 and reformed on several occasions, grants the State broad powers to regulate telecommunications in the country. It allows State intervention in access and use of the Internet, as well as the possibility of blocking websites and digital platforms under certain justifications.

Law for the Defense of Territorial Sovereignty and Integrity: Enacted in 2010, this law allows the government to take action against any content it considers to violate national sovereignty, including monitoring and blocking digital platforms and social networks that spread information that is considered harmful.

Computer Crime Law: These laws (there are several proposals and versions) have been criticized for their possible use to limit freedom of expression and persecute those who criticize the government. "Cybercrime" provisions can be interpreted broadly and potentially abusively, creating a climate of fear for free expression online.

Law against hate: The Constitutional Law against Hate, Intolerance and for Peaceful Coexistence, sanctioned by the National Constituent Assembly of Venezuela in 2017, is considered a restrictive law of digital rights. This law has been criticized both nationally and internationally, as it is argued that it is used to control freedom of expression and silence political opponents, especially in the context of online dissent.

- Article 1 - Scope of the Law

It states that the law aims to punish and prevent hatred and intolerance in all its forms, which provides a broad and ambiguous basis for the interpretation and application of the law.

- Article 3 - Definition of the right to "Peace"

It introduces vague and open concepts about what is considered "hate", "intolerance" and "peaceful coexistence". These definitions can be used to restrict a wide range of expressions and opinions.

- Article 11 - Prohibition of Incitement to Hate

It prohibits incitement to hatred and violence, but its interpretation can lead to censorship of any criticism or negative comments about the government or public figures, which affects freedom of expression.

- Article 20 - Criminal Liability

Establishes criminal sanctions for those considered responsible for acts that promote hatred. This can include everything from information spread on social networks to political speeches, which creates a climate of fear for those who wish to express themselves freely.

- Article 21 - Aggravating circumstances

It allows the imposition of the maximum limit of the sentence, using vague and discretionary terms that can be considered aggravating, which can lead to the failure to adequately discriminate against related crimes.

- Article 22 - Economic sanctions

It establishes mechanisms for the monitoring and control of communication and publications in public and private media, allowing constant monitoring of activity in radio spaces and its eventual sanction in case of allowing hate messages on its platform.

- Article 23 - Obligation to collaborate

It obliges digital platforms to collaborate with the State in the dissemination of messages for the promotion of peace, as well as the elimination of content that is considered offensive or hateful, which can result in censorship and arbitrary elimination of publications.

The Constitutional Law against Hate has been denounced by human rights and civil liberties organizations as a tool to restrict freedom of expression, especially in digital media. The vagueness in the definitions and the breadth of the sanctions generate an environment conducive to self-censorship and limit political and social discussion in the country.

Law against Fascism and Similar Expressions: The proposed Law against Fascism and Similar Expressions, discussed by the National Assembly of Venezuela in 2021, has been considered by many as a potential instrument of persecution and criminalization of digital rights. Although it is presented under the pretext of combating extremist ideologies and protecting peaceful coexistence, its implications for freedom of expression and digital rights have raised serious concerns.

Reasons why it is considered restrictive:

- The bill includes broad and vague definitions of what constitutes "fascism" and "similar expressions," allowing for subjective and potentially abusive interpretation. This could lead to censorship of any criticism of the government or ideas that are considered contrary to the official narrative.
- It provides criminal sanctions for those accused of promoting ideologies that are considered "fascist", which could include political speeches, comments on social networks and content on digital media. This creates an environment of fear where people might refrain from expressing critical opinions.
- It could allow greater control by the State over media platforms and social networks, forcing them to collaborate in the identification and removal of content considered dangerous or unacceptable. This encourages self-censorship and limits the exchange of ideas.
- There are concerns that this law will be used as a tool to persecute political opponents, activists and citizens who criticize the government, promoting a climate of repression rather than constructive dialogue.
- The implementation of this law could severely limit freedom of expression online, affecting journalists, bloggers and ordinary users in their abilities to express opinions and share information.
- The proposed Law against Fascism and Similar Expressions joins a set of regulations that have sought to restrict digital rights and limit freedom of expression in Venezuela. The political and social environment in the country has been marked by the repression of dissident voices, and such laws contribute to a legal framework that can be used to criminalize criticism and dissent. Human rights organizations and critical voices continue to denounce these initiatives as violations of citizens' fundamental rights.

On the other hand, Nicolas Maduro in his censorship and communication control plan on August 12, 2024 through the **Decree No. 4,975**, created the National Cybersecurity Council. This Decree was generated in the midst of a post-electoral context where protests, excessive repression and unrest in the country were in full

development before the announcement of the first official bulletin made by the National Electoral Council.

It is important to highlight that said decree issued by the Venezuelan executive raises several concerns in relation to the exercise of digital rights and the possible harm to human rights. Some of the worrying aspects that can be observed include:

The decree could contain provisions that restrict freedom of expression, especially in digital media, which would limit the ability of citizens to express their opinions and criticism of the government. The mention of "political effectiveness" may imply an increase in government surveillance over citizens' online activities, which could result in the monitoring of digital communications and the criminalization of dissenting opinions and this leads to a lack of clarity under the terms and conditions established in the decree can lead to abuses of power, allowing authorities to act arbitrarily without accountability, which would affect transparency and the rule of law.

Likewise, if the decree provides for restrictions on access to digital platforms or online information, this harms the right of citizens to inform themselves and communicate freely, any provision that imposes severe sanctions for the dissemination of information or the performance of online activities considered "subversive" could lead to fear of self-censorship among citizens.

The decree could disproportionately affect human rights defenders and activists who use digital platforms to advocate for social change, exposing them to retaliation and harassment. Just as digital restrictions could severely impact already vulnerable groups, denying them the ability to express themselves and defend their rights in a safe environment.

The broad and ambiguous interpretation of the terms of the decree could result in the indiscriminate and arbitrary application of the law, which would generate a climate of legal insecurity.

These concerns reflect a context in which the regulation of the use of digital technologies can be used as a tool of social control, limiting the fundamental rights of citizens in Venezuela.

In the continuation of Decree No. 4,975, other worrying aspects related to the improper use of communication and information technologies, as well as the potential harm to fundamental rights, can be identified:

The reference to "cybercrime" can be used as a justification to implement repressive measures that limit the use of the Internet and telecommunications, affecting civil liberties. That is, the lack of clarity in the definition of what constitutes "cybercrime" can lead to a broad and subjective interpretation, allowing the criminalization of activities that are not necessarily criminal.

The implementation of a state policy focused on digital security can lead to a concentration of power in the hands of the government, weakening the ability of citizens to challenge or question these policies. Greater state control over communication technologies can result in the invasion of citizens' privacy, with potential violations of the confidentiality of personal information.

No less worrying is the mention of international cooperation to confront cybercrime, which can lead to agreements that compromise the country's sovereignty and affect the protection of data and citizens' rights, taking into account a no small issue: surveillance policies. and control can discourage innovation in the digital sector, due to fear of retaliation or sanctions for legitimate online activities.

Tools and policies aimed at combating cybercrime may also be directed at civil society organizations, restricting their ability to operate and advocate for human rights, by establishing a legal framework to "protect" society, they are likely to intensify. online censorship practices, affecting access to diverse and critical information.

It is also worth noting that the importance of education and digital literacy for citizens is not explicitly mentioned, which is essential to empower the population and prevent

cybercrime effectively. For this reason, it is stated that the State's response could be disproportionate, focusing on population control instead of addressing the underlying causes of cybercrime.

These additional aspects highlight the worrying possibility that measures taken under the pretext of ensuring national security may actually undermine citizens' fundamental rights and freedoms.

National Cybersecurity Council: In article 1 of the Decree, several worrying aspects can be identified. Being an advisory and consultative body dependent on the president, there is a risk that the Council is aligned with the political interests of the government, which can compromise its impartiality and objectivity. . The nature of this council as a dependent body can lead to a lack of independent oversight mechanisms, increasing the risk of abuses of power.

The creation of a council dealing with the "prevention of criminal uses" may allow for broad interpretations of what is considered criminal, facilitating the crackdown on activities that are not inherently illegal. Depending on how it works, the council could propose regulations that further restrict internet access and freedom of expression, in the name of cybersecurity.

The council's description does not mention the inclusion of civil society representatives, which could lead to decisions that do not consider citizens' voices and concerns. Concentrating cybersecurity management in a single council under the control of the Executive can lead to a centralization of power, limiting the diversity of approaches and solutions to cyber risks. In this sense, the focus on "prevention of criminal uses" could imply the implementation of stricter surveillance systems and control over circulating information, affecting the privacy of citizens.

The existence of this council could set a precedent for the creation of other structures that seek to criminalize the use of communication technologies, affecting innovation and digital development. This is stated because the decree does not clearly specify what the council's powers and powers will be, which could lead to diverse

interpretations and the adoption of non-transparent measures. Although the intent is to combat cybercrime, the lack of a comprehensive approach that includes education and prevention can result in a reactive and punitive response that does not address the causes of cybercrime.

These aspects highlight the need for a broader debate and the consideration of mechanisms that guarantee respect for human rights and civil liberties within the framework of cybersecurity.

In article 2, which details the functions of the National Cybersecurity Council, several relevant and worrying aspects can be observed. Here some of them:

The council is tasked with advising not only the President, but also the National Defense Council, which may lead to an integration of cybersecurity with national defense, raising concerns about the militarization of cybersecurity, by raising proposals of regulations and laws related to the use of information technologies, there is a risk that regulations will be enacted that limit civil liberties and fundamental rights in the name of security.

The mention of the prevention of "criminal uses" of information technologies could lead to an ambiguous interpretation, allowing the criminalization of activities that are not necessarily illicit, affecting freedom of expression and access to information, in this sense the function of verifying the degree of compliance with plans and regulations could lead to excessive surveillance and the creation of an environment of fear and self-censorship, instead of promoting a responsible cybersecurity culture.

The obligation to formulate proposals in harmony with the "interests and objectives of the Nation" can lead to the council's recommendations being more aligned with the government's political agenda than with the real cybersecurity needs of the population. The continuous assessment of risks and threats in terms of computer security must be carried out in a transparent and objective manner; Otherwise, it could be used as justification to implement excessive or repressive measures.

Likewise, there is no mention of the participation of diverse sectors (such as civil society, academics or technology experts) in policy formulation, which could limit the approach towards inclusive and effective security, just as the functions of the council may be in depending on the political context of the moment, which may affect its effectiveness and its ability to offer adequate and timely solutions to emerging cybersecurity problems.

These aspects highlight the need for a clear, balanced and respectful regulatory framework of human rights to guide the functions of the National Cybersecurity Council, as well as adequate supervision of its activities.

Articles three, four and five establish which institutions will make up the council, its mechanism and how the representation of this commission for national cybersecurity will be distributed, which is basically made up of military police organizations that make evident the nature of the police of the Venezuelan State in matters of digital rights.

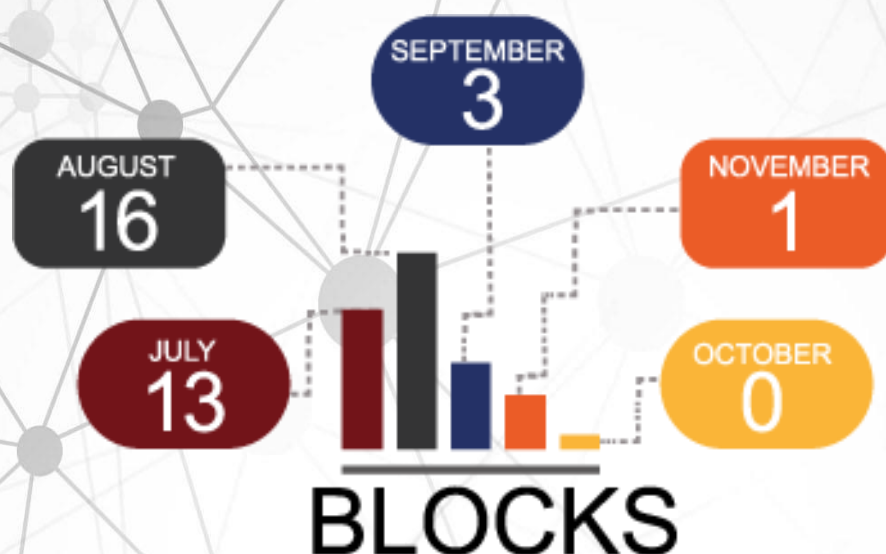
Freedom of expression on the internet

Blocking web portals

The Venezuelan State, in its hegemonic vision of controlling all media and information, has executed a series of blockades against different web portals to which Venezuelans have had access in different spheres. Since Nicolás Maduro decreed the so-called “Furia Bolivariana” on January 23, 2024, a raid was carried out against different radio and digital news media, these being the largest channel of information for Venezuelans through their smartphones, tablets or computers. In the case of (digital) informative web portals, these have represented spaces that had managed to circumvent state censorship.

Among the decrees and arbitrary decisions of the State, the blocking of the social networks arguing that the platform is being used to threaten members of chavismo.

Different Venezuelan organizations such as Venezuela Sin Filtro, Espacio Público and Redes Ayuda have constantly monitored the restrictions that information portals have suffered, but their web portals have also been targets of government blockades, as have digital security provision services. and large-scale social networks such as X (former Twitter).



In Venezuela, a state policy has been implemented that is made up of a series of tactics to generate information blockades that limit access to critical information and restrict both the right to information and the right to freedom of expression. This technical analysis addresses the strategies used and the state companies involved in these blockades, which have forced the population to download a VPN to stay informed in the absence of freedom of expression in traditional media.

Information Blocking Strategies

1. **Website Blocking:** The government uses network-level filtering techniques to block access to news websites, social media platforms, and information portals that are critical of the regime. This is done through the implementation of blacklists of URLs that are blocked by Internet Service Providers (ISPs).
2. **Monitoring and Censorship Systems:** Monitoring systems have been implemented that allow the government to identify and censor content in real time. This includes

deep packet inspection (DPI) techniques that allow the state to monitor Internet traffic and block unwanted content.

3. Interference in Social Media: Interference in the operation of social media platforms is another common tactic. This includes slowing down the speed of access to these platforms or in some cases, completely blocking access at critical moments, during protests or important political events such as the cases of “X” blocked on August 9 and TikTok blocked on August 28. September 2024 by the Venezuelan national executive.

4. Control of Internet Service Providers: The State exercises control over the country's main ISPs, forcing them to comply with censorship orders and facilitate the monitoring of data traffic. This includes both state-owned companies and some private ones that operate under strict regulations, in which under no circumstances can either the state-owned CANTV or private internet provision services fail to comply with blocking instructions.

5. Disinformation and Manipulation of Information: In addition to blockades, the State has also used disinformation techniques through state media and controlled accounts on social networks to saturate the flow of information, promoting narratives that favor the regime and displacing voices. criticisms, ranging from stigmatization campaigns to the use of unverified or false information to saturate public opinion.

Punitive hashtags

The year 2024 has been characterized by the coordination between the official discourse that has materialized in reality, but previously there has been a projection on social networks where a narrative is wielded that has dangerously permeated the real world.

This has fundamentally been the trend, which can be analyzed in several periods, specifically there could be three.

From the monitoring, it has been possible to analyze three blocks of time between January and April, between May and July 28 and between July 29 and mid-October of the current year, with totally different scenarios and even with speeches specifically directed toward people of that specific group

#LaFuriaBolivariana

Brought back to reality on January 23, 2024 during a speech by President Nicolás Maduro, where he ordered his bases of the United Socialist Party of Venezuela to unleash Bolivarian fury. Already in 2020 it had been implemented between January and April of that year, but in the present, it has been used to, according to the official narrative, prevent the party in government from de facto ceasing its functions and therefore its bases had to monitor and mark opponents even in their homes, this also accompanied by the narrative of alleged attacks against the physical integrity of President Nicolás Maduro.

During this period, more than a label or hashtag, it became a phrase that accompanied other campaigns linked to the official narrative. It was resumed as the most frequently used tag beginning in the months of October and in the month of November and early December where publications with the aforementioned term were also observed.

During the second period between April and July, the campaigns were mostly directed towards disqualifying the image of both the opposition leader María Corina Machado and the members of her political party. Disqualifying mentions were also observed on social networks against the members of the different volunteers who participated in the electoral process of July 28, 2024.

#TunTunLlegoLaPaz

The most aggressive campaign that has been developed by the Venezuelan state towards citizens, with an aggressive police deployment campaign against the people who participated in the electoral process, those who were also involved in citizen mobilizations such as marches, rallies and all kinds of popular expression and finally

the people who made comments on their personal network's contrary to the national government.

During the last two days of July and the following seven weeks of both August and September, videos stand out in which opponents were subjected to public ridicule, such as the case of María Oropeza who was arrested in her home in the city of Guanare, Portuguesa state, with a video projected with background music from a horror movie.

The videos where opponents who made calls for protest were mocked and subsequently presented after having been arrested, with the well-known joke or meme, of the "three Doritos later", used largely in sports such as boxing and football.

Like these other labels such as #ComanditosDelTerror #TunTunSinLloradera #GuarimberoLloronPaTocoron, they represent within the aggressive language itself a great campaign of intimidation against the population in the most critical days of protest over the results of July 28 presented by the National Electoral Council.

At least 27 tags were counted on Twitter and TikTok, alluding to intimidation, stigmatization and defamation against opponents, of which 11 with high interaction could be identified directed towards the free opposition member María Corina Machado, two against the Human Rights defender, Rocío San Miguel and the rest directed at other scenarios and personalities from the world of politics and Venezuelan civil society.

Organizations and companies of the Venezuelan State involved

1. CANTV (National Telephone Company of Venezuela): It is the main provider of telecommunications services in the country and is under state control. This telephone company is responsible for the majority of Internet traffic in Venezuela, it has implemented blocks and censorship following government orders.

2. **Movilnet:** This is the CANTV subsidiary dedicated to mobile services. It has also been used to access private information via SMS and other communication services that facilitate the organization and dissemination of critical information.

3. **Ministry of Popular Power for Communication and Information:** This ministry oversees the State's communication policy and is responsible for regulating the media in the country. It is responsible for issuing regulations on the content that the media can disseminate and coordinating censorship actions.

4. **National Public Media System:** It includes a network of state media that are used to disseminate information favorable to the government and deny or discredit negative information.

5. **CONATEL (National Telecommunications Commission):** It is the regulatory entity that supervises telecommunications services in Venezuela. CONATEL exercises control over media and frequency concessions and may impose sanctions on media outlets that do not comply with State guidelines.

The Venezuelan State has developed a complex system of tactics to generate information blockades, which combines direct censorship and control of telecommunications infrastructure with the use of disinformation. The combination of state companies such as CANTV, Movilnet and CONATEL, among others, allows the government to exercise effective control over the flow of information and limit citizens' digital freedoms. The implications of these actions are profound, as they affect people's ability to access accurate information and participate in public discourse.

Accessibility to information

Affectation of the population by the crisis of services

Power outages have had a significant impact on the speed and quality of Internet access in the country. The recording of Internet speed in the country varies significantly by region due to factors such as available infrastructure, the quality of

service of Internet providers and electricity outages. In this context, interruptions affect activists from different perspectives: psychological, economic, technical and labor.

Venezuela is one of the countries with the slowest internet, according to Ookla, in the country for April 2024, the median speed of residential fixed Internet was 45.84 Mbps for upload and 48.77 Mbps for download. In the case of the median speed of mobile Internet it was 6.29 for uploading and 11.66 Mbps for downloading, a factor for which there are people who have inhibited themselves from posting on social networks.

- Psychological Impact:

Prolonged blackouts generate different types of reactions in society, from anger, sadness and anxiety in citizens, a situation that is no different in those who depend on technology to carry out their activism work. Digital activists, who often use online platforms to organize, communicate their ideas and disseminate information, face a hostile environment where electricity service and internet access are restrictive. This lack of stability can lead to feelings of frustration, helplessness, and hopelessness, severely impacting your ability to maintain a positive focus on your mission.

Recent research, such as that carried out by the World Health Organization (WHO) and other institutions, has shown that prolonged stress can lead not only to mental health problems, such as anxiety and depression, but also to a deterioration in cognitive performance. In a country where instability is the norm, blackouts add to the emotional burden that activists already face, creating a vicious cycle of demotivation and distrust.

This is the case of Mariana (pseudonym), a journalist in Bolívar: "Every blackout is a new wave of anxiety. You never know when the light will come back on, and that makes me feel helpless, sometimes helpless but other times resigned. I am constantly worried about how to continue continue with our activities in the diary. I have had nights in which my sleeping hours are simply modified, thinking about

everything we have to do and how the blackouts stop us. I feel emotionally exhausted, to that we must add. that, to get fuel in Puerto Ordaz, sometimes you have to wait in lines for more than 4 hours. What affects me the most is the heat when there is a blackout, it exhausts you physically and emotionally to a level that you have to postpone what you are doing to. another day.”

- **Economic Impact:**

Economically, blackouts affect the ability of digital activists to do their work. Many of them depend on digital technologies and internet access to obtain financing, manage campaigns and collaborate with international organizations. Lack of electricity not only limits your access to these tools, but also increases operating costs.

According to the 2021 World Bank report, the economic crisis in Venezuela has been exacerbated by instability in transportation and logistics, largely due to a lack of energy. Activists seeking financial support often face difficulties in communicating their funding needs to potential donors, leaving them in a vulnerable position, unable to carry out their projects and receive adequate support.

Testimony from “Giovanni”, union activist and merchant in Yaracuy state: “The blackouts not only interrupt our communication, but also affect our budget as entrepreneurs. “We have had to spend more on generators and fuel, which has limited our ability to carry out our activity, so the ability to participate in civic affairs is limited and practically non-existent.”

- **Technical Impact:**

From a technical point of view, blackouts also limit access to digital tools and infrastructure necessary for activism. Lack of power means servers, content management platforms and other essential digital resources cannot be accessed. This creates a gap in communication and in the organization of activities, weakening the capacity of activists to mobilize civil society and generate effective impacts.

In addition, repeated interruptions in electrical service can damage sensitive equipment, such as computers and storage devices, resulting in irrecoverable losses of data important for activism and the defense of human rights. As Winston Cabas, president of the National Electrical Commission of the College of Engineers of Venezuela, mentioned, the losses due to equipment damage are countless, "We must tell the country the truth..., tell Venezuelans from what time to what time "they are rationing so that they disconnect their equipment, so that when the supply returns, which is when the appliances are damaged, they are already disconnected."

Testimony from "Laura" activist from the state of Táchira: "Every time there is a blackout, we lose much more than just a few minutes of work. I have had to face the loss of essential data. On one occasion, while we were working on an important report, The power went out and we lost hours of research. I try to make backups, but sometimes it is impossible to access the servers. This has weakened our ability to communicate and collaborate effectively. We used to have external funding, but now we don't. "To be able to show results due to the lack of light and connection, several donors have decided to suspend their support. Our work has become more expensive and difficult."

- Labor Impact:

Blackouts also have a labor impact in the broadest sense. Many civil society organizations depend on digital tasks for their operation. When access to electricity is irregular, the continuity of projects that require constant and well-planned effort is put at risk. This can result in job losses and layoffs of staff who are unable to fulfill their responsibilities due to lack of resources.

Testimony of "Eduardo", a young activist in the humanitarian sector in the state of Lara: "I am part of a team that works in the humanitarian sector, but the blackouts have been devastating for us. Many of my colleagues have had to leave their jobs because they cannot fulfill their responsibilities. One of my best friends left the country because he felt frustrated about not being able to do anything. The truth

is that I see less and less of a future in this, and how the blackouts are causing talent to be lost. see how Job instability affects so many who just want to make a change.”

Historical Patterns between Power Outages and Connectivity

Frequency of Outages: Since the collapse of the electrical system in Venezuela, power outages have become frequent and prolonged, coinciding with a notable drop in Internet quality and speed. In periods of extended blackouts, such as the national blackout in March 2019, drastic drops in internet access have been reported nationwide.

Power outages cause disruption of supply to critical infrastructure such as servers, data centers and Internet distribution nodes. This results in loss of connectivity for extended periods, preventing network access.

When power is restored, it is common for there to be a sudden increase in demand from users trying to reconnect their devices and access the Internet. This overload can affect connection speed, resulting in slowness and difficulty accessing online services. The situation underlines the urgent need for a comprehensive reform in the electricity and telecommunications sector to guarantee stable and quality access to the Internet in Venezuela.

Seasonality: Connectivity often improves temporarily during peak electricity production seasons (such as the rainy season), but plummets in dry seasons due to the decline in the power generation capacity of hydroelectric plants, which are the main source. of electricity in the country.

Regional inequalities: Rural and less developed areas generally suffer more due to instability in power supply, resulting in poor connectivity and lower internet speeds. Urban areas may experience outages, but often have more consistent access to alternative energy sources, such as generators.

Disconnecting Network Equipment: Essential equipment, including routers, switches and other network devices, require power to operate. During outages, these devices are turned off, which can lead to drops in connectivity in specific areas.

Effects on productivity: The repeated instability of energy supply and its impact on connectivity has led to numerous complications for productive sectors that depend on the Internet to operate, including companies, businesses and educational institutions.

Training defenders on cybersecurity

In the state of Lara, the trainings were carried out in the same way from July 25 to 27 in person, and others were carried out remotely on September 12 and 13, 2024, with a total of 11 participants. The training was led by engineer José Millán, an expert in augmented reality who graduated from the Universidad de Oriente. Similarly, in Yaracuy, 24 people were trained in person from July 25 to 27 and online on September 12 and 13.

The training was led by engineer José Millán, an expert in augmented reality who graduated from the Universidad de Oriente, and the topic addressed was: basic notions about digital security, tools to identify risks on social networks, the most common fraudulent messages such as fishing and spyware, as well as an illustration of some of the protection measures that civil society activists should know to avoid being the target of surveillance on social networks, the theft of information, as well as the protection of bank accounts as one of the mechanisms of persecution towards members of civil society.

In this regard, in Táchira, a series of workshops were held on July 25 and 26 in person and additionally a virtual session on September 5, in which six people were present.

The training was led by social media expert Adolfo Baptista, and the content taught focused on protection mechanisms in the digital area to exercise documentation, as one of the main functions of Human Rights defenders. Likewise, basic notions about

digital security such as double authentication, use of VPN and identification of possible threats were provided.

For its part, in the state of Bolívar, in-person training was held on August 26 and 27, which were later complemented remotely, on August 29 and 30, in which there were a total of 11 participants, under tutoring by Simón Arreaza, expert in social networks at the Andrés Bello Catholic University, Guayana core. In this participation, a topic was taught on the use of secure connections such as VPN, double authentication for accessing personal and institutional accounts, as well as basic notions to identify possible threats.



Institutional cyber violence

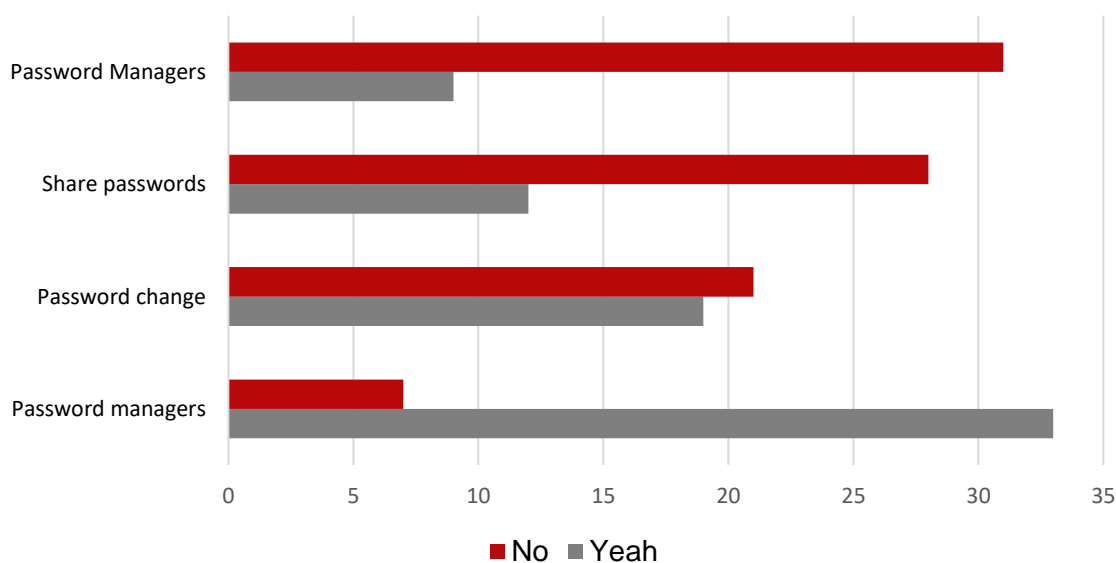
Pre-election perception of digital security

To measure this indicator, two surveys were carried out, the first on July 25, 2024, prior to the presidential elections in the country, among human rights defenders and social communicators, in order to know their position or expectations regarding the management of social networks. in Venezuela and the risk of surveillance or persecution by State institutions and supporters of the ruling party. The following results were obtained:

Table 1. Confidentiality

Item	In managing your social networks and email, you:	Yeah		No	
		f	%	f	%
1	Do you use strong, unique passwords for your accounts?	33	82,5	7	17,4
2	Do you regularly change your passwords?	19	47,5	21	52,5
3	Have you ever shared passwords or login information with others?	12	30	28	70
4	Have you implemented additional security measures such as the use of password managers?	9	22,5	31	77,5

Confidentiality

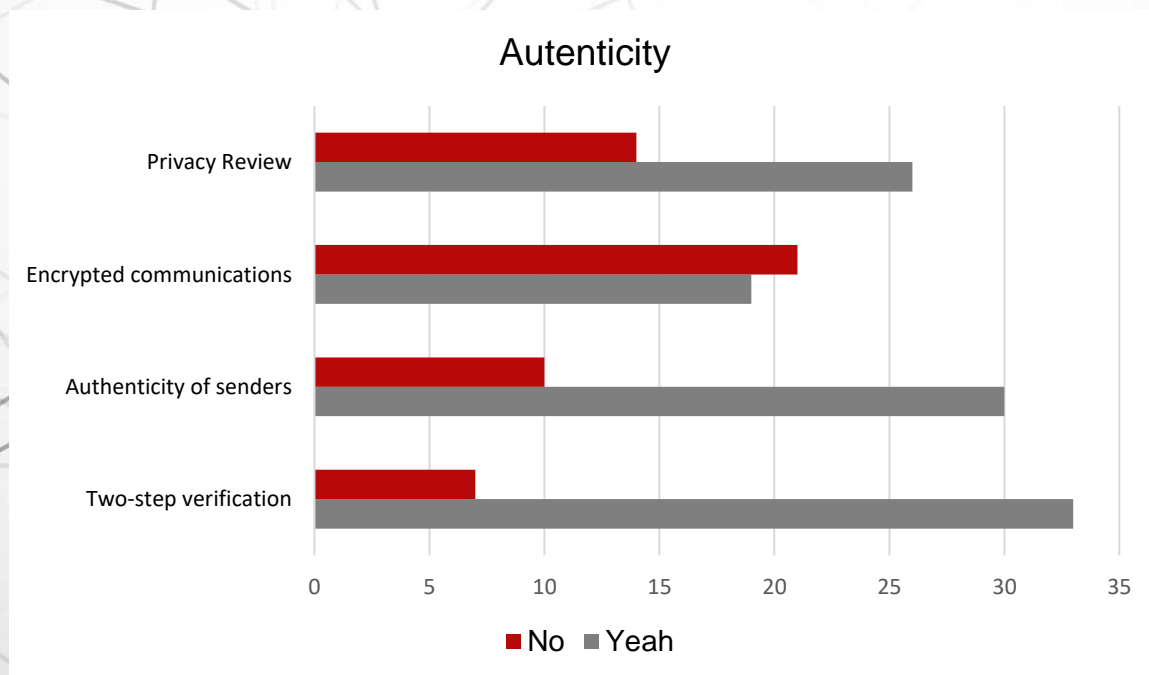


Confidentiality refers to protecting information from unauthorized access, establishing privacy for the data of the person or organization, preventing cyberattacks or espionage situations.

Even though the basis of this pillar is access control through password authentication, it is important that respondents manage other mechanisms such as biometric scanning and encryption, because they have generated favorable results in this sense, since 30% have shared your passwords.

Table 2. Authenticity

Item	In managing your social networks and email, you:	Yeah		No	
		f	%	f	%
5	Do you enable two-step authentication on your online accounts?	33	82,5	7	17,5
6	Do you check the authenticity of senders before clicking on links?	30	75	10	25
7	Do you encrypt your sensitive communications when you send messages?	19	47,5	21	52,5
8	Do you regularly review the privacy settings of your accounts?	26	65	14	35

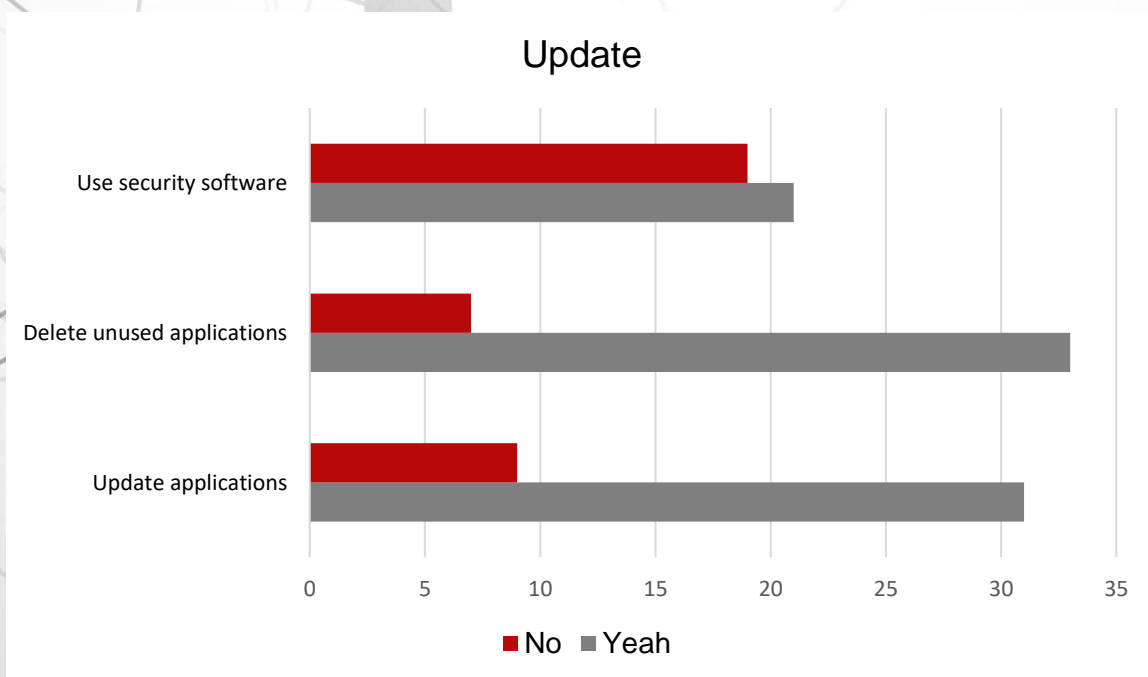


Authenticity is the confirmation that the data has legitimacy, that is, that there is no manipulation or external interventions by third parties posing as collaborators. To do this, it is necessary to document the actions carried out by users on the network and systems.

It should be noted that less than half of those surveyed (47.5%) expressed that they maintain encrypted communications, which places them in a position of vulnerability to possible cybersecurity attacks at a personal and organizational level, remembering that organizational data must have processes to identify its authenticity, for this it is recommended to configure an access log that helps confirm the veracity of a particular record.

Table 3. Update

Item	In managing your social networks and email, you:	Yeah		No	
		f	%	f	%
9	Do you update your devices and apps regularly?	31	77,5	9	22,5
10	Do you remove unused apps from your devices?	33	82,5	7	17,5
11	Do you use updated security software on your devices?	21	52,5	19	47,5



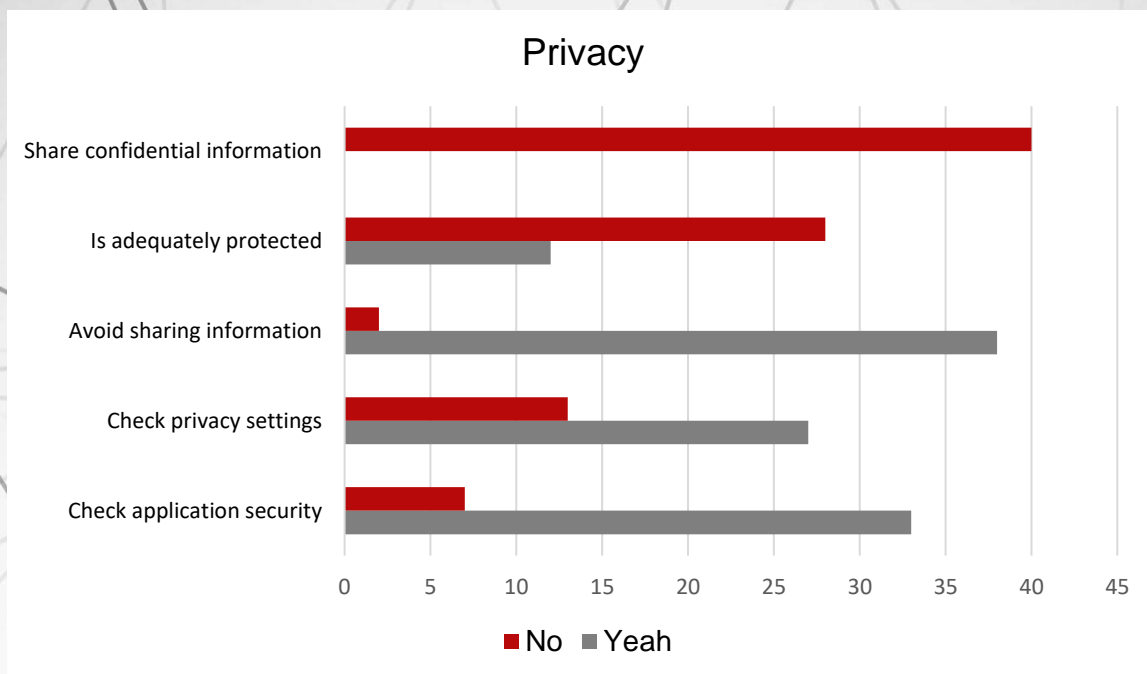
The results draw attention to the use of updated security software by those surveyed, because only a little more than half (52.5%) implement them to manage their social networks, and it is explained as follows: to any type of violation of their accounts or devices with which they are dedicated to the promotion, dissemination and defense of human rights in Venezuela.

According to the National Cybersecurity Institute in Spain, it is important to make frequent updates because *“Operating systems, web browsers, programs and applications are susceptible to security flaws. For this reason, they may need to be updated, regardless of the device on which they are installed. This includes the programs and operating systems of computers, tablets, smartphones, video game consoles and even smart televisions.”*

On the other hand, more than 75% of them remove and update applications frequently, which represents that they perform actions that help reduce risks, allowing code verification, changes in encryption, evaluation of unintentional encryption threats, encryption options, audit permissions and access rights.

Table 4. Privacy

Item	In managing your social networks and email, you:	Yeah		No	
		f	%	f	%
12	Do you check the security of an app before downloading it?	33	82,5	7	17,5
13	Do you frequently review your privacy settings?	27	67,5	13	32,5
14	Do you avoid sharing sensitive personal information online?	38	95	2	5
15	Do you believe your personal information online is adequately protected?	12	30	28	70
16	Have you ever shared confidential information through a social network?	0	0	40	100



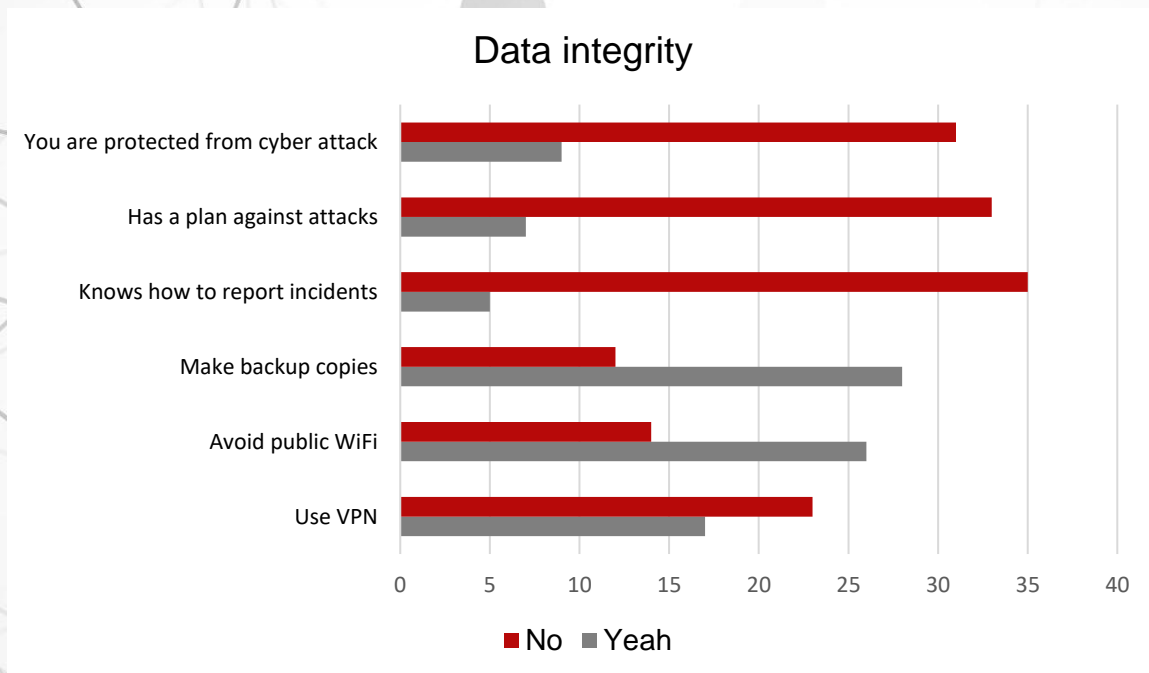
Privacy violations refer to unauthorized access to social media accounts, emails and online applications, which can have serious consequences for people's privacy and trust in digital platforms.

Only 30% of those surveyed consider that they are adequately protected against a possible violation of their privacy, which demonstrates the need to reinforce their knowledge in cybersecurity, although 100% of them do not share confidential information through their social network accounts.

The motives behind cyber-attacks can vary, but there are three main categories: criminal, political and personal, however, in Venezuela there has been an increased case of attackers with criminal motivations who seek economic benefits through the theft of money, and with political motivations they usually associate with State actors, non-governmental organizations or the opposition infrastructure.

Table 5. Data integrity

Item	In managing your social networks and email, you:	Yeah		No	
		f	%	f	%
17	Do you use a virtual private network (VPN) to browse safely online?	17	42,5	23	57,5
18	Do you avoid connecting to unsecured public Wi-Fi networks?	26	65	14	35
19	Do you back up your data regularly?	28	70	12	30
20	Do you know how to report digital security incidents to the relevant authorities?	5	12,5	35	87,5
21	Do you have a response plan for possible digital security incidents?	7	17,5	33	82,5
22	Do you think your accounts are protected from possible cyber-attacks?	9	22,5	31	77,5



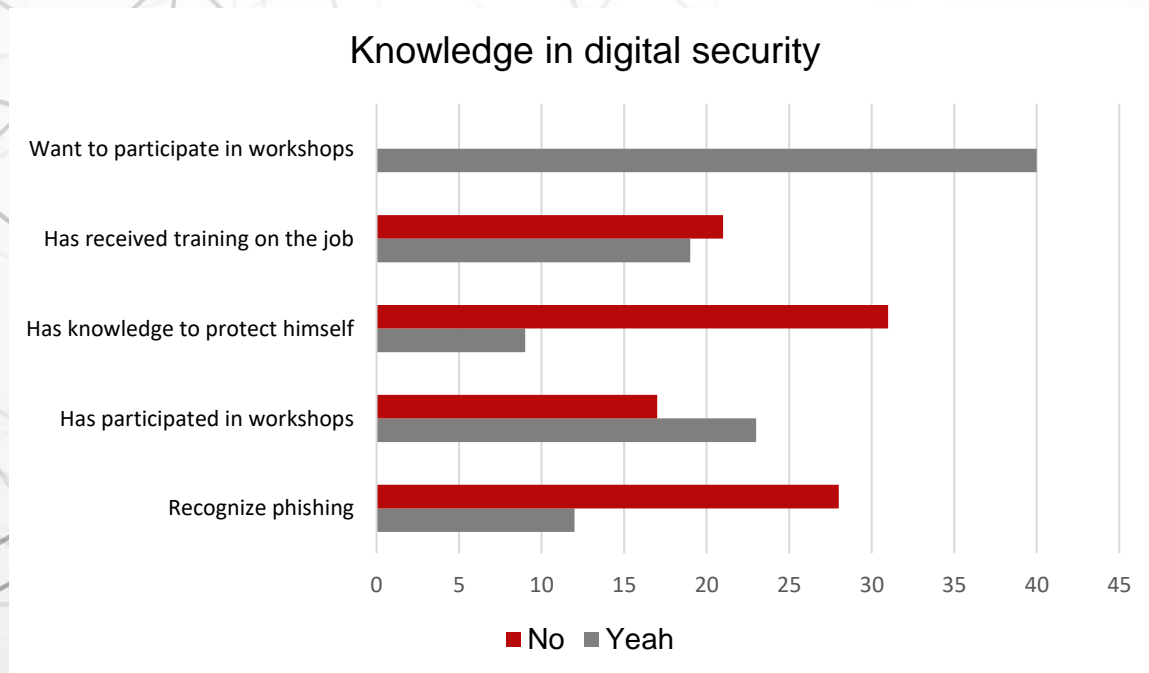
These results show that those surveyed prior to July 28 showed a lack of proactive digital security measures, which left them exposed to being victims of additional attacks to those already inherent to their work as human rights defenders, especially in a context where there are concerns about harassment, surveillance and threats.

It should be noted that more than 80% of the subjects did not have a response plan for the violation of their cybersecurity nor did they have knowledge of how to make the corresponding reports in the event of a possible digital attack.

If there is an improper alteration of the data, it means that there has been a loss of integrity, and it is necessary to implement control mechanisms to prevent unauthorized alteration of the information.

Table 6. Knowledge in digital security

Item	In managing your social networks and email, you:	Yeah		No	
		f	%	f	%
23	Do you recognize the signs of a possible phishing attack?	12	30	28	70
24	Have you participated in digital security training?	23	57,5	17	42,5
25	Do you think your level of digital security knowledge is sufficient to protect yourself online?	9	22,5	31	75,5
26	Have you received specific training on digital security in your work area?	19	47,5	21	52,5
27	Are you interested in participating in a digital security workshop?	40	100	0	0

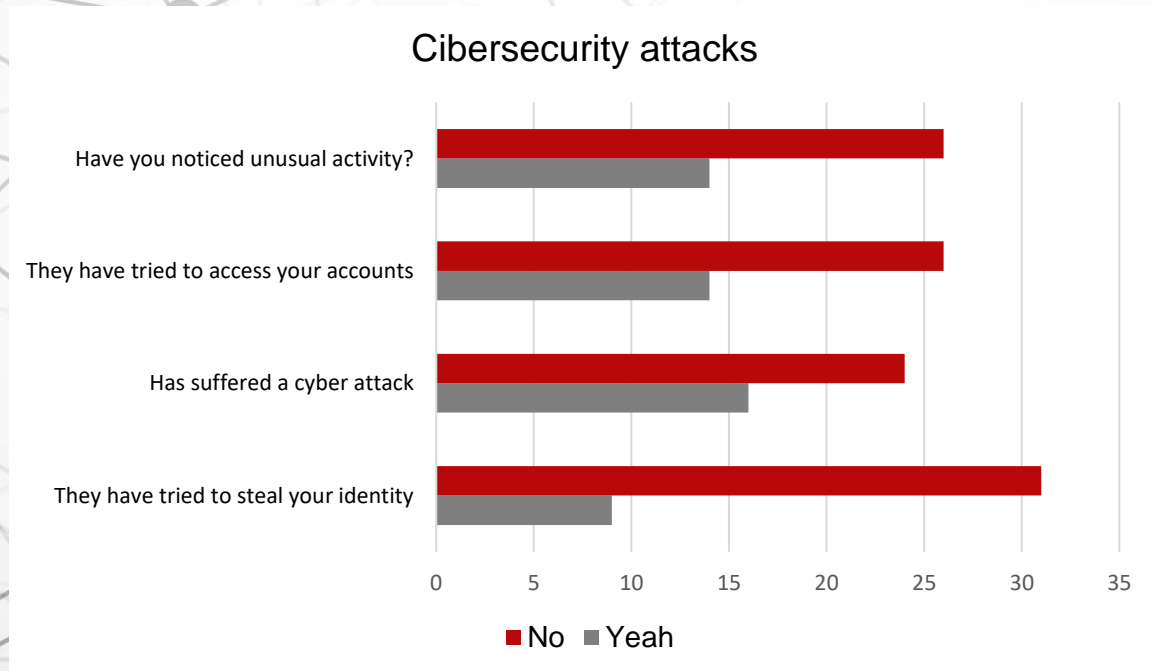


Having knowledge in cybersecurity allows the reduction of economic losses, in addition to creating protection mechanisms in processes, technology and people, not only against cyberattacks or information leaks, but also to guarantee security.

In this regard, 75.5% of those surveyed stated that their level of knowledge in digital security is sufficient to protect themselves online, which is why 100% expressed that they were interested in receiving training in cybersecurity, in order to minimize their level of digital vulnerability.

Table 7. Cybersecurity attacks

Item	In managing your social networks and email, you:	Yeah		No	
		f	%	f	%
28	Have you ever experienced an online phishing attempt?	9	22,5	31	77,5
29	Have you been a victim of any type of cyber-attack?	16	40	24	60
30	Have they tried to access your accounts without prior authorization?	14	35	26	65
31	Have you noticed unusual activity on your accounts that could indicate a security breach?	14	35	26	65

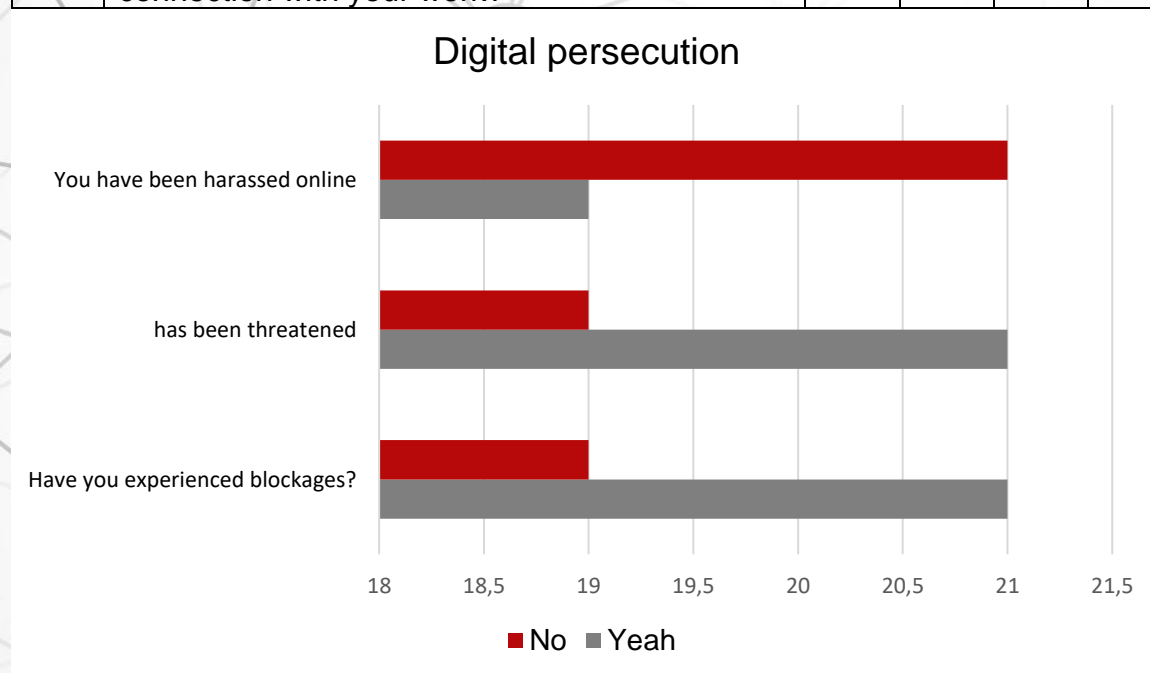


Before the presidential election, on average, the majority of respondents had not experienced phishing attempts on social media, which may indicate relatively high confidence in their online security practices or the security of the platforms they use. However, those people who had already been victims of this crime should be the subject of attention, because they are considered direct threats.

According to the technology company IBM “A cyber-attack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system, or digital device.”

Table 8. Digital persecution

Ítem	In managing your social networks and email, you:	Yeah		No	
		f	%	f	%
32	Have you experienced online crashes when trying to access certain content?	21	52,5	19	47,5
33	Have you received online threats related to your work?	21	52,5	19	47,5
34	Have you been subject to online harassment in connection with your work?	19	47,5	21	52,5



In relation to the receipt of threats or intimidation online among labor human rights defenders, journalists and electoral observers reveal that at least half of those surveyed have received threats or intimidation online, indicating that they face significant risks in their work. This figure implies a hostile environment for those dedicated to the defense of human rights, journalistic activity and electoral observation.

Online threats can have paralyzing effects, affecting the ability of these professionals to carry out their work. This could result in self-censorship, fear of retaliation, and a negative impact on content production or advocacy for important causes.

According to IBM, “the motives behind cyber-attacks can vary, but there are three main categories: criminal, political and personal”, however, in Venezuela, the persecution carried out by the State towards political dissidence has moved to the digital sphere, especially against public employees and human rights defenders.

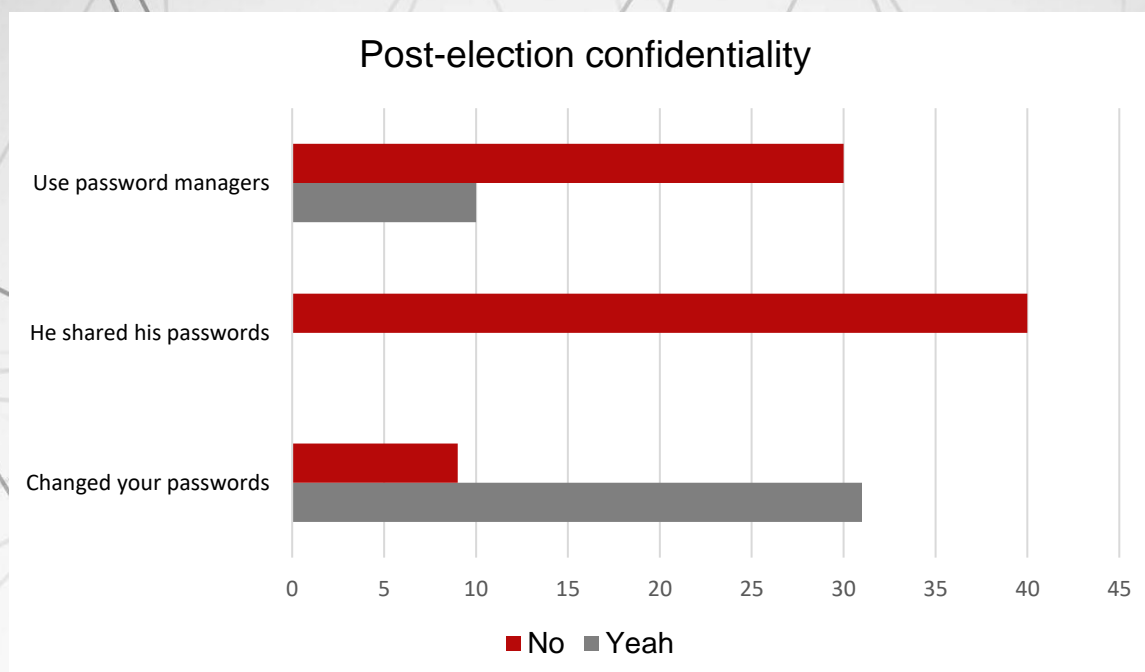
Given this situation, the implementation of protection measures is urgent, both at a personal and organizational level, this includes training in cybersecurity, the use of protection tools and the creation of response protocols against threats.

Post-electoral situation of digital security

After the presidential elections, a multiple-choice survey was applied, referring again to the perception of security in the use of digital channels for the dissemination, promotion and reporting of facts related to human rights, from which the following results were obtained:

Table 9. Post-election confidentiality

Ítem	After the presidential elections in Venezuela on July 28	Yeah		No	
		f	%	f	%
1	Have you changed the passwords for your social media accounts?	31	77,5	9	22,5
2	Have you shared your social media passwords with others?	0	0	40	100
3	Have you used password managers to protect the security of your social media accounts?	10	25	30	75

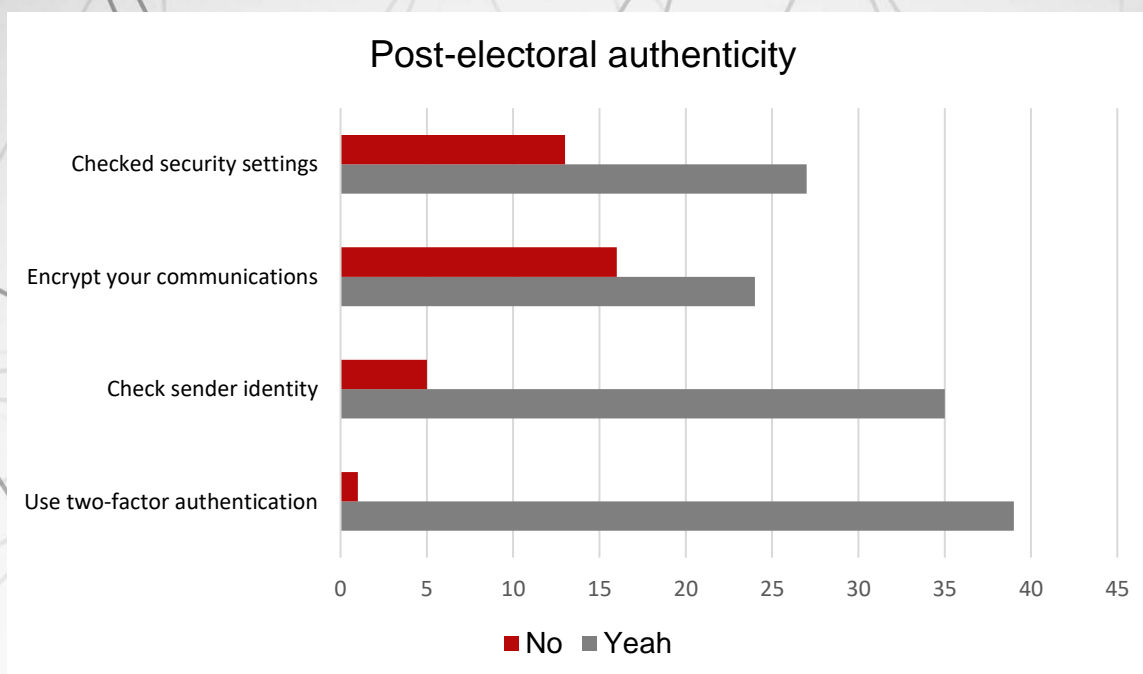


After the elections, 77.5% of those surveyed changed the passwords of their social networks due to the increase in surveillance of the digital activity of human rights defenders, especially electoral observers, however, it remains the high percentage (75%) of them that have not resorted to the use of password managers as a cybersecurity measure.

The Internet User Security Office (OSI) defines password managers as “Applications that serve to store all our credentials (users, passwords, websites to which they correspond, etc.) in a database encrypted using a master password.”

Table 10. Post-electoral authenticity

Ítem	After the presidential elections in Venezuela on July 28	Yeah		No	
		f	%	f	%
4	Have you enabled two-factor authentication to access your social networks?	39	97,5	1	2,5
5	Do you check the identity of the sender of the emails you receive?	35	87,5	5	12,5
6	Do you have your online communications settings encrypted?	24	60	16	40
7	Do you regularly review your social media privacy settings?	27	67,5	13	22,5

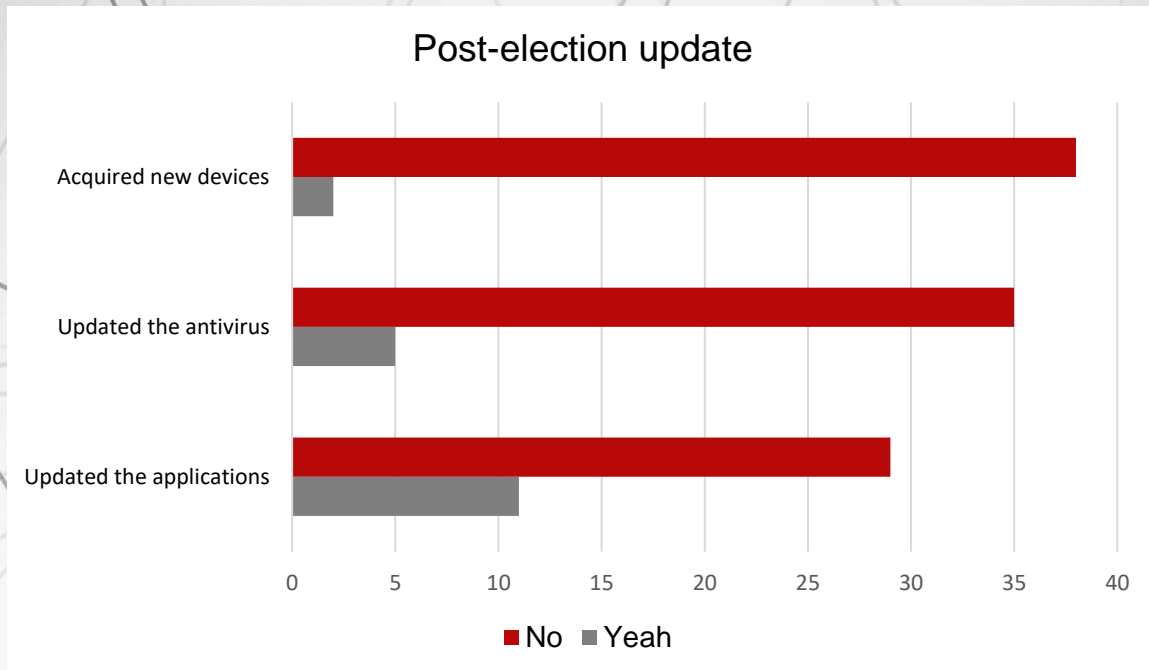


With the increase in threats, intimidating speeches and cases of arrests following the digital surveillance exercised by the Venezuelan State, almost all of those surveyed (97.5%) enabled authentication on their social media and email accounts. of two factors, which indicates that they were concerned about protecting themselves from attacks on their cybersecurity.

Two-step verification (sometimes called multi-factor authentication) helps protect you by making it harder for someone else to sign in to your account. It uses two different forms of identity: your password and a contact method (also known as security information).

Table 11. Post-election update

Ítem	After the presidential elections in Venezuela on July 28	Yeah		No	
		f	%	f	%
8	Did you update your social media applications?	11	27,5	29	72,5
9	Have you updated the virus protection software on your devices?	5	12,5	35	87,5
10	Did you acquire new electronic devices to manage your social networks?	2	5	38	95

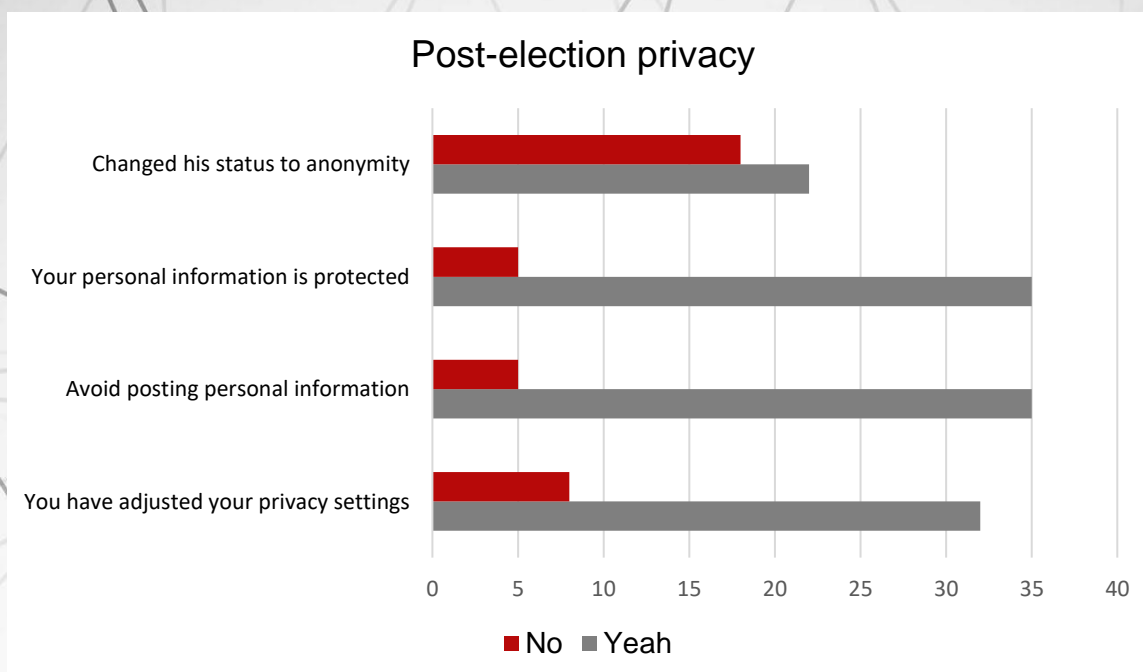


Whether it is a personal device or an organization's computer, having protection against threats is vital, and even though there is a wide variety of antivirus, each with its characteristics and strengths, there is a need to keep them updated to have access to improvements that can range from fixing bugs and failures to adding different tools and new features.

This allows the level of protection against a malware attack; however, the majority of respondents (87.5%) have not taken it as a cybersecurity measure, having in this regard a weakness in digital security.

Table 12. Post-election privacy

Ítem	After the presidential elections in Venezuela on July 28	Yeah		No	
		f	%	f	%
11	Have you made adjustments to your social media privacy settings?	32	80	8	20
12	Do you avoid posting personal information on your accounts?	35	87,5	5	12,5
13	Do you consider that your personal information is adequately protected?	35	87,5	5	12,5
14	Did you switch to anonymity to post on social media?	22	55	18	45

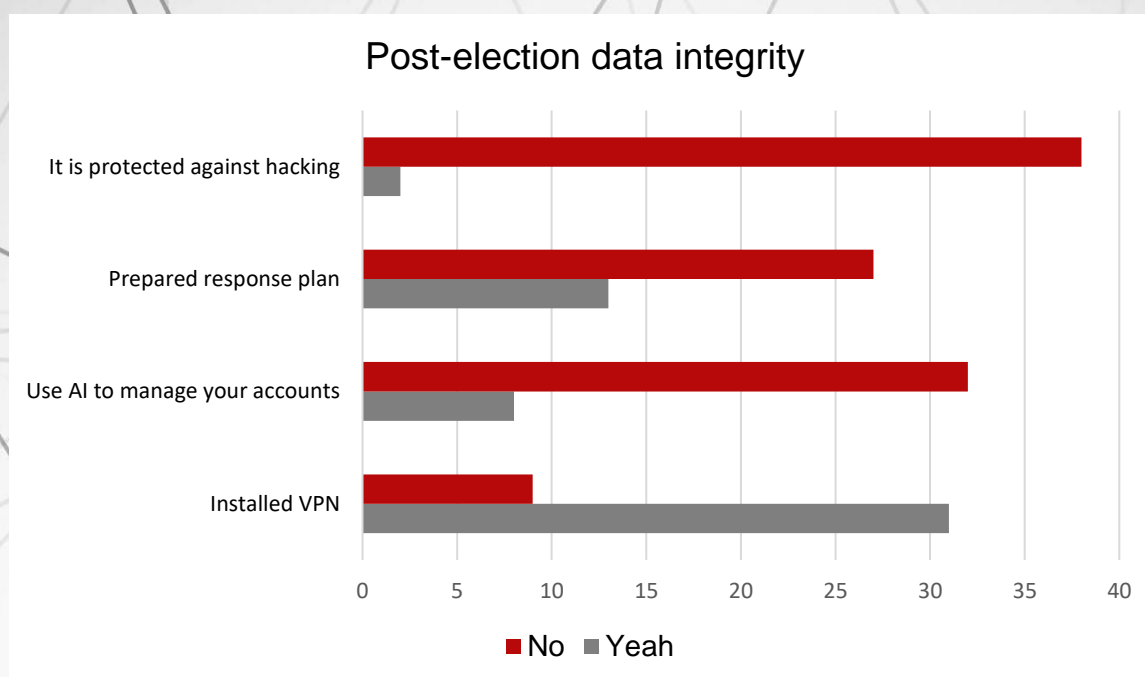


Online anonymity is the ability to use the Internet without providing any personally identifiable information. This means that you can do whatever you want on the Internet without anyone knowing who you are, and in the case of Venezuela, after July 28, 2024, 55% of those surveyed opted for this modality to be able to express themselves freely without revealing their identity, and thus avoid being victims of surveillance, threats or direct attacks by State actors.

Likewise, 87.5% of those interviewed consider that they made the corresponding adjustments to protect their personal information, which is a positive aspect to maintain their digital activism.

Table 13. Post-election data integrity

Ítem	After the presidential elections in Venezuela on July 28	Yeah		No	
		f	%	f	%
15	Have you installed a VPN to use your social networks?	31	77,5	9	22,5
16	Do you use artificial intelligence to manage your social media accounts?	8	20	32	80
17	Did you develop a response plan for possible attacks on the security of your social media accounts?	13	32,5	27	67,5
18	Do you consider that your electronic devices are protected from hacking?	2	5	38	95



After the blocking of the social network's opposition political leaders, but the importance of data protection was also given to those who needed to publish without putting their personal information at risk.

It is relevant to address the need for protection against account hacking expressed by 95% of those surveyed, because this is a weakness that can be exploited by those who seek to restrict people's digital rights, especially rights defenders. humans, and also help them create a response plan for possible attacks on the cybersecurity of their organizations and members, since only 32.5% expressed that they have adequate planning.

Table 14. Post-electoral knowledge in digital security

Ítem	After the presidential elections in Venezuela on July 28	Yeah		No	
		f	%	f	%
19	Have you sought to strengthen your cybersecurity knowledge on your own?	30	75	10	25
20	Have you participated in any cybersecurity training organized by your work organization?	16	40	24	60
21	Do you think you need digital security training?	22	55	18	45

Post-electoral knowledge in digital security

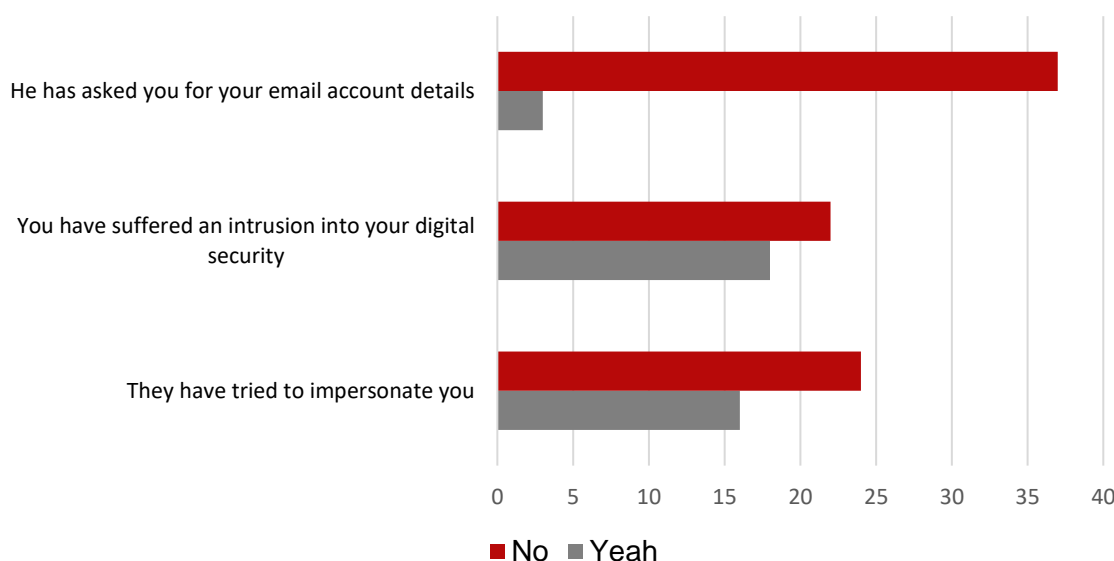


Even though the respondents have made efforts to strengthen their electronic defense mechanisms, it is necessary to strengthen knowledge in cybersecurity because after the elections this aspect became crucial to guarantee the integrity of people and organizations, especially those dedicated to the defense of human rights, because 55% of those surveyed stated that they require appropriate instruction in the face of the risks of surveillance, persecution or attack in the digital sphere.

Table 15. Post-election cybersecurity attack

Ítem	After the presidential elections in Venezuela on July 28	Yeah		No	
		f	%	f	%
22	Have they tried to impersonate you on social networks?	16	40	24	60
23	Have you been the victim of any intrusion into your security measures to access your social networks?	18	45	22	55
24	Have you been asked for personal information related to your email accounts?	3	7,5	37	92,5

Post-election cybersecurity attack

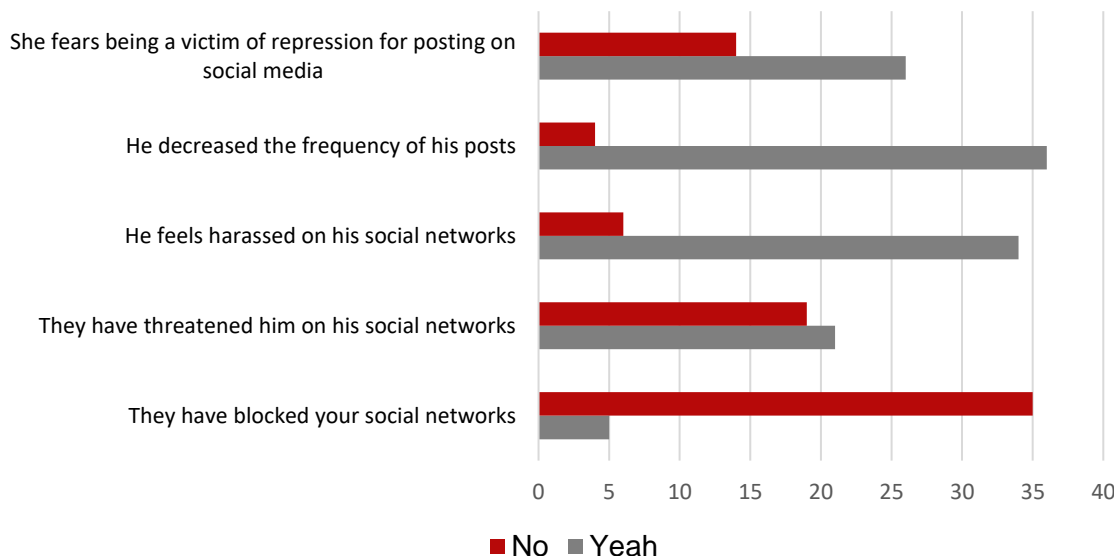


These responses reflect a complex environment where risk and surveillance are omnipresent, and security and freedom of expression are critical considerations for the practice of each of these groups following the July 28 electoral process. The differences in their responses underline the need to address threats in a contextualized manner and develop appropriate protection strategies for each sector.

Table 16. Post-electoral digital persecution

Ítem	After the presidential elections in Venezuela on July 28	Yeah		No	
		f	%	f	%
25	Have any of your social media accounts been blocked?	5	12,5	35	87,5
26	Have you been subjected to threats through messages on social networks for carrying out your work?	21	52,5	19	47,5
27	Do you feel harassed via social media for posting content about human rights?	34	85	6	15
28	Did you decrease the frequency of your social media posts to avoid bullying?	36	90	4	10
29	Are you afraid of being a victim of repression by the State if you publish on social networks?	26	65	14	35

Post-electoral digital persecution



The analysis of these responses can offer a clear vision about the climate of insecurity and fear that the population in Venezuela faces, especially in the context of the repression after the presidential elections, because 90% of those surveyed have decreased the amount of social media posts as a personal safety measure, however, it also means the loss of your ability to work freely without fear of retaliation.

Harassment and surveillance are common practices used to discourage the defense of rights in the country, because they have a paralyzing effect on the activity of those dedicated to promotion and denunciation through social networks.

It is noteworthy that 52.5% of those surveyed were subject to threats, with election observers being one of the groups most affected by the repressive wave unleashed with the so-called Operation Tun-Tun, where polling station witnesses were persecuted in some cases. after monitoring by security forces through the use of personal social media accounts.

In general, all groups experience some degree of risk, but journalists seem to be in the most critical situation with an almost unanimous perception of increased danger. This perception of risk and experiences of harassment have affected the willingness

of union members and human rights defenders to participate in online activism, and the constant threat can lead to self-censorship and limit their ability to act in defense of their rights or those of others.

Dismissal of public sector workers for the use of networks after July 28

After July 28, the day of the presidential elections, the massive dismissal of public sector workers was evident due to the use of social networks, with only in the state of Apure a total of 5,000 workers receiving summonses to appear before the Educational Zone, by Mary Orasma, to notify them of their dismissal for alleged ideological reasons, since they expressed their support for Edmundo González Urrutia in the elections.

In said plains entity, the Internal Management Secretariat of the Educational Quality Development Center was instructed to notify the citizens mentioned in a list, who were required to appear at the Internal Management coordination, in order to verify the employment status of the employees, who had to appear between August 15, 2024 and September 15, 2024, the list issued included educators, administrative staff and workers.

Again, August 15 stands out, because the National Union of Press Workers of Venezuela disclosed through its "X" account that on August 1 and 2 more than 40 employees of the state television channel VTV were fired only for having "liked" publications by María Corina Machado.

These dismissals are considered illegitimate and affect the job stability of workers. "We reject the State's retaliation against those who think differently and express themselves on the matter. We demand that the inspectorates and the International Labor Organization (ILO) intervene to restore the rights of those affected," the message concludes.

"They have been fired from VTV and also from RNV. There is terror in reporting and we have collected some testimonies in the midst of tears and fear. They have been fired for liking any publication by María Corina Machado or for writing "fraud" in their

WhatsApp statuses," the account of the National Union of Press Workers describes in X.

In addition to these cases, there have been documented cases of workers being forced to resign. Through mass layoffs, threats and guidelines that force the WhatsApp application to be removed from cell phones, the national government has implemented retaliatory measures against hundreds of workers from the National Civil Aviation Institute (INAC) and the Conviasa and Aeropostal airlines, who did not support President Nicolás Maduro in the presidential elections.

At Conviasa, layoffs exceeded 190, while at INAC more than 100 employees have been laid off. So far, Aeropostal has recorded five layoffs. It is important to note that these actions not only affect workers and employees, but also impact administrative and managerial staff, pilots and flight attendants, who have been identified for expressing their rejection of the electoral fraud that occurred on July 28.

The general manager of Aeronautical Safety is responsible for preparing the "black list" at the INAC, and he ordered that, as of July 29, employees have the obligation to publish photos on their mobile phones or on social networks expressing their support for Maduro. Those who refused to comply with said order received serious threats from their superiors, including the aforementioned Aeronautical Security manager. In addition to coercing staff to work during the days when the "opposition" called for rallies, employees are also being forced to delete the WhatsApp application and install the Wechat application instead.

Patterns of persecution associated with the exercise of digital rights

Layoffs: Throughout the 25 years that they have been in power, Chavismo's coercion of public employees as a mechanism of social control has been present, fundamentally since 2004 with the birth of the list you are with until modern times.

Prior to the presidential elections, there were threats and actions to prevent public sector workers from publicly expressing their sympathy for opposition candidates. However, this action of arbitrary termination of the employment relationship between

the individual and the State that has been seen over time, on this occasion could be observed in public institutions and state companies. Once again, the state oil company of Venezuela in the days after July 28 carried out this practice against those workers who, for publishing statuses and opinions on social networks such as Instagram WhatsApp Facebook and even in “X”, were fired from their jobs in states like Falcón, but also in Anzoátegui and Monagas.

Harassment and threats: This being a practice also connected within the patterns of violation of labor rights, the same retaliation is observed on this occasion for publishing on social networks against public sector workers, although the measure taken by the executive translated into different practices, the majority change based on messages of possible undisclosed transfers or dismissals, verbal abuse in the workplace, orders to delete workers' social networks and even threats to call the security forces.

Unconsulted transfers: There are reports that in the state of Apure some workers in the education sector were transferred to different areas than where they had already been working, without the prior request of the employee as established by law.

Prohibition of entry to the workplace: Both in the state of Apure and in other regions of the Venezuelan plain, there are reports of workers who, after July 28, due to their opinions on social networks, were not notified of dismissals against them, but neither were they allowed them to enter their workplace.

Social media account hacking: During the second week of September, several hacks and piracy attempts were reported using suspicious links or phishing, directed at the accounts of Venezuelan journalists and citizens. One of those affected was Andrés Rojas Jiménez, host of Unión Radio and editor of the Petroguía portal. On the morning of September 14, he received a message from a user supposedly identified as Meta, the current name of the parent company of Facebook and Instagram. The message misleadingly warned about possible inactivation of accounts on Instagram for alleged violations of the social network's rules, such as sharing copyrighted

content or spam messages. Users were then instructed to complete an appeal form, through which hackers could gain access to their data.

Institutional violence towards women who exercise digital rights

On September 12, Venezuelan actress Prakriti Maduro's X account was hacked. This actress, who has been denouncing the repressive patterns that the regime has imposed on the population since the elections, revealed that in the previous days she had been the victim of an attack on her personal account on the same platform. This occurred after he published testimonies that had reached him through his private messaging about arbitrary arrests in the context of the protests after the elections. In a publication on hack me, they won't be able to find traces of my informants."

Using the online tool Brand 24, an analysis was carried out on the stigmatization of two very active figures on social networks and highly popular personalities in Venezuela, such as the political leader María Corina Machado and the Human Rights defender Rocío San Miguel.

The report generated for the hashtag #CarcelParaLaSayona that the national government accounts promoted against the political leader María Corina Machado, was established between July 19 and September 19, 2024 in a period of 92 days.

The volume of impressions exceeded 28, also the reach on social networks of this label reached over 375,000, the reach outside of social networks was 4,434, the number of interactions was 38,789, and the number of "likes" was 19,355; It should be noted that the amount of 25,634 dollars was invested in this activity to reach that number of people.

The same happened with the case of human rights defender Rocío San Miguel, in an analysis carried out by the Obsevatorio Venezolano de Cazadores de Fake News, at the time of her arrest on February 9, 2024 at the Simón Bolívar International Airport in Maiquetía, being re-victimized by the Venezuelan State with a discredit campaign by troll accounts related to the ruling party. From the platform we hunt

Fake News explained in a Twitter thread on 02/11/24, they explain that the account #AsiSeDifamaEnVenezuela Rocío San Miguel @rociosanmiguel was a victim of the stigmatization campaign #RocíoNoEsSanta, which means that it is not treated from just an isolated label; It is part of a government information operation. This disqualification tactic is not new, but part of a broader pattern that seeks to discredit those who criticize or oppose the current administration.

The campaign against her sought to link her with alleged assassination plans, accusations that were promoted by Tarek William Saab and that played a crucial role in the dissemination of messages on social networks. Phrases such as "conspiracy plot" (with 52 mentions), "bracelet plot" (with 37 mentions) and "attempted assassination" (with 22 mentions) were used to refer to Rocío San Miguel, focusing the search on these mentioned keywords.

Legal provisions violated

The Venezuelan State, by exercising blocking practices on information portals and social networks, is violating several international agreements and treaties on human rights and digital rights, signed and ratified by the Bolivarian Republic of Venezuela.

These digital blockades hinder people's ability to communicate effectively and access critical information, which is vital in any functioning democracy. Likewise, they affect the ability of civil society organizations to operate, monitor human rights violations, and educate the population.

Below are some of the main international instruments that Venezuela violates by executing blockades:

1. International Covenant on Civil and Political Rights (ICCPR)

Article 19: Establishes the right to freedom of expression, which includes the freedom to seek, receive and disseminate information and ideas of all kinds. Blockages to information portals or social networks restrict this fundamental right and the right to information.

2. American Convention on Human Rights

Article 13: Recognizes the right to freedom of thought and expression. This includes the State's obligation to guarantee access to information and the prohibition of censorship.

3. Universal Declaration of Human Rights

Article 19: Similar to the ICCPR, it establishes that everyone has the right to freedom of opinion and expression, as well as to seek, receive and disseminate information and ideas by any means.

4. United Nations Principles on the Application of Human Rights on the Internet: These principles establish that human rights must be protected and promoted in the digital environment, which includes the prohibition of censorship and the guarantee of access to information.

5. Convention on the Rights of the Child: Although it focuses on the rights of minors, this convention also highlights the importance of access to information and free expression, which would be compromised by blocks on digital media.

Censorship and blocking practices in Venezuela not only contravene national norms, but also challenge widely accepted international standards regarding freedom of expression and access to information. This highlights the need for greater international surveillance and pressure to ensure respect for digital rights.

6. Constitution of the Bolivarian Republic of Venezuela: Promulgated in 1999, it establishes various fundamental rights that the State must guarantee to all people, but by exercising censorship practices on digital media, the Venezuelan State is violating several aspects and articles of this Constitution.

Article 49 - Right to Defense: Although it refers mainly to rights in judicial proceedings, censorship can affect the right to defense and the possibility of receiving truthful and timely information.

Article 57 - Right to Freedom of Expression: This article establishes that everyone has the right to freely express their thoughts, ideas and opinions. It also guarantees the right to seek, receive and disseminate information and ideas of all kinds, which is directly affected by digital media censorship.

Article 58 - Right to Information: This article guarantees the right of every person to receive truthful and timely information. The censorship of information portals and social networks prevents the population from having access to the information necessary for informed decision-making.

Article 59 - Prohibition of Censorship: Expressly establishes that censorship cannot be imposed on the media. This implies that any attempt to block web pages or restrict access to social networks can be considered a form of prohibited censorship.

Article 70 - Protection of Freedom of Communication: This article protects communication and information as fundamental rights of the people. Limiting access to digital media and social networks has a direct impact on this right.

Article 108 - Right to Freedom of Thought and Expression: Reiterates that freedom of thought and expression in any form of communication is guaranteed, this being essential for the exercise of the right to freedom of expression and access to information.

Article 126 - Role of the State in Communication: This article establishes that the State must promote and guarantee the right to communication and information. Censorship practices go against this obligation of the State.

Article 337- States of Exception: The President of the Republic, in the Council of Ministers, may decree states of exception. Circumstances of a social, economic, political, natural or ecological nature that seriously affect the security of the Nation, the institutions and the citizens, in which regard the powers available to them are insufficient, are expressly classified as such. to deal with such events. In such case, the guarantees enshrined in this Constitution may be temporarily restricted, except for those referring to the rights to life, prohibition of incommunicado detention or

torture, the right to due process, the right to information and other intangible human rights.

Let us remember that both the Constitution of the Bolivarian Republic of Venezuela and the Organic Law on States of Exception (article 7, paragraph 14), establish that the right to information cannot be restricted.

Censorship in Venezuela not only affects individual rights, but also has an impact on the collective rights of Ibero-American society since it generates a bad precedent, given the abuses and restrictions imposed by other countries in the world and the region, adapted with their own strategies.

Furthermore, the surveillance and restriction of digital media occurs in the midst of a climate of general fear, where Venezuelans are inhibited from exercising freedom of expression and citizen participation, or at least that is what the State tries to impose.

Conclusions

The analysis of the situation of digital rights in Venezuela in 2024 reveals an alarming reality that reflects the complexity of the country's sociopolitical environment. The conclusions of this report focus on several key findings that not only document the current state of digital rights, but also emphasize the urgent need to address and mitigate the observed issues.

It was evident that freedom of expression in the digital sphere faces significant challenges, censorship of the media and repression of critical voices have led to an atmosphere of fear and uncertainty among citizens. Many people have opted for self-censorship, avoiding expressing their opinions and participating in public debates for fear of reprisals, with 55% of those surveyed (22 people) changing their online status to anonymity and 90% of these decreasing the amount of his publications after the presidential elections.

The protection of personal data has been another of the axes analyzed in the investigation, because the lack of clear legislation on privacy and the implementation of mass surveillance practices have exposed citizens to constant risks. Many Venezuelans are unaware of how their information is collected, used and stored online, leaving them vulnerable to abuse of their data by state and non-state actors.

This situation requires an urgent debate on the need to establish legal frameworks that adequately regulate data protection and guarantee the rights of citizens in the digital environment. In this regard, it is striking that the encryption of the respondents' communications went from 47.5% before the July 28 elections to 60% after the elections, in a personal attempt to increase their cybersecurity.

A worrying aspect that has emerged strongly in this research is digitalized institutional violence, a phenomenon that manifests itself through technological tools used by the State to exercise control and repression. This form of violence translates into mechanisms for monitoring and tracking citizens' digital activities, creating an environment of constant surveillance that inhibits freedom of assembly and association. In this regard, after July 28, 65% of those surveyed stated that they fear being subject to some type of retaliation by the national executive linked to their activity on social networks as part of their role as a human rights defender.

Furthermore, threats to digital security, such as cyber attacks on opponents and civil society organizations, reflect a systematic strategy by the State to silence all criticism. The coexistence of sophisticated technological tools together with the lack of adequate infrastructure to protect citizens has contributed to an environment in which digital violence becomes a mechanism of control and repression.

The report also highlights the need to promote digital literacy among the population, in order to strengthen citizens' abilities to navigate the digital environment safely and effectively, which is crucial to empowering them to defend their rights. In reference to this aspect, 100% of those interviewed expressed their desire to strengthen their knowledge in cybersecurity, either through training programs or educational

resources, which serve to teach them to use digital tools as instruments of defense and promotion of their freedoms.

Furthermore, it is imperative that the international community pay attention to the situation of digital rights in Venezuela, which is why cooperation between countries and non-governmental organizations is essential to create support networks that can help citizens face the challenges posed by the Censorship and digitalized institutional violence.

In conclusion, the results on the monitoring of digital rights in Venezuela in 2024 is a call to action, which shows the urgent need to address digitalized institutional violence and its implications. It is essential to adopt a comprehensive approach that promotes digital rights as an essential part of the fight for democracy and respect for human rights in the country, as well as promoting a constructive and collaborative dialogue that involves all actors in society.

Recommendations

This environment has created a society where communication and the exchange of ideas are severely restricted, affecting not only democratic dynamics, but also the population's ability to inform themselves and organize around common causes, which is why the following recommendations are made to the International Community:

- Establish monitoring and documentation mechanisms for cases of digitalized institutional violence in Venezuela, ensuring that human rights violations are recorded and reported.
- Provide legal assistance to victims of digital rights violations, supporting local organizations working to defend human rights and protecting activists.
- Use diplomatic channels to urge the Venezuelan State to cease practices of digital surveillance and repression, promoting freedom of expression and respect for digital rights.

- Financially support projects that promote digital literacy and education on digital rights in Venezuela, providing resources to train citizens.
- Create international coalitions of human rights organizations that work together to address digitalized institutional violence in different contexts, including Venezuela.

Digital platforms have become risk spaces, where dissent is persecuted and where citizens fear being subject to reprisals, such as arbitrary arrests or harassment, which is why the Venezuelan State is urged to:

- Reform and repeal laws such as the Law against Hate, in order to establish a solid legal framework that protects the digital rights of citizens, incorporating specific measures against institutional violence and abuse of power in the digital environment.
- Promote transparency in the management of personal data and establish clear privacy policies that respect the rights of citizens, avoiding the misuse of information.
- Implement training programs for government officials on digital rights and ethical requirements related to privacy and data protection.
- The immediate cessation of harassment through digital platforms towards political and different types of civil society organizations that are not aligned with the party and government so that violence on social networks translates into physical violence towards political dissidents.

The recommendations made in this report seek to guide policy makers, as well as human rights organizations, towards actions that strengthen the protection of digital rights in the country, but also encourage citizens to:

- Promote workshops and awareness campaigns on digital security, teaching citizens tools and practices to protect their personal information and prevent online manipulation.

- Inform the population about the risks of self-censorship, encouraging citizens to freely express their opinions and share information, while empowering them to do so safely.
- Establish support networks between citizens and activists that share information and strategies on how to confront digitalized institutional violence, strengthening solidarity and collaboration in the defense of rights.

Bibliographic references

- Argos Hub LLC. (2020). *¿Qué es Ciberseguridad? Objetivos, elementos e impacto en 2020*. Texas, EEUU. Artículo en línea. Disponible en: <https://www.argoshub.com/que-es-ciberseguridad/>
- Asamblea Nacional de Venezuela. (2009). Constitución de la República Bolivariana de Venezuela. Disponible en: <https://www.cgr.gob.ve/assets/pdf/leyes/Constitucion.pdf>
- Asamblea Nacional de Venezuela. (2018). Ley Orgánica de Seguridad de la Nación. Disponible en: <https://www.observatoriodeconflictos.org.ve/oc/wp-content/uploads/2018/09/Ley-Organica-de-Seguridad-de-la-NAci%C3%B2n.pdf>
- Asamblea Nacional de Venezuela. (2019). Anteproyecto de Ley Constitucional del Ciberespacio de la República Bolivariana de Venezuela. Disponible en: <https://www.accessnow.org/wp-content/uploads/2019/01/ley-del-ciberespacio-venezuela.pdf>
- Asamblea Nacional de Venezuela. (2020). Ley Orgánica de Telecomunicaciones. Disponible en: https://www.oas.org/juridico/spanish/cyb_ven_ley_telecomunicaciones.pdf
- Asamblea Nacional de Venezuela. (2024). Ley contra el Fascismo, Neofascismo y Expresiones Similares. Disponible en: <https://www.observatoriodeconflictos.org.ve/oc/wp-content/uploads/2024/05/Ley-antifascismo-Venezuela.pdf>
- Asamblea Nacional de Venezuela. Ley Contra El Odio la Intolerancia y por la Convivencia Pacífica. Disponible en: <https://espaciopublico.org/wp-content/uploads/2017/10/Borrador-Ley-contra-el-odio-la-intolerancia-y-por-la-convivencia-pac%C3%ADfica.pdf>

Asamblea Nacional de Venezuela. Ley de responsabilidad social en radio, televisión y medios electrónicos. Disponible en: <http://mippci.gob.ve/wp-content/uploads/2023/03/1-Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electr%C3%B3nicos.pdf>

Cyberzaintza. (s/f). *Integridad*. Gobierno Vasco. Artículo en línea. Disponible en: <https://www.ciberseguridad.eus/ciberglosario/integridad#:~:text=En%20ciberseguridad%2C%20la%20integridad%20hace,datos%20en%20tr%C3%A1nsito%20o%20reposo.>

Gobierno Bolivariano de Venezuela. (2024). Decreto N° 4.975, mediante el cual se crea el Consejo Nacional de Ciberseguridad. Disponible en: <https://pandectasdigital.blogspot.com/2024/08/decreto-n-4975-mediante-el-cual-se-crea.html>

IBM (s/f). *¿Qué es un ataque cibernético?*. México. Artículo en línea. Disponible en: <https://www.ibm.com/mx-es/topics/cyber-attack#:~:text=el%20siguiente%20paso-,%2BFQu%C3%A9%20es%20un%20ataque%20cibern%C3%A9tico%3F,sistema%20inform%C3%A1tico%20o%20dispositivo%20digital.>

Instituto Nacional de Ciberseguridad. (s/f). *La importancia de las actualizaciones de seguridad*. España. Artículo en línea. Disponible en: <https://www.incibe.es/ciudadania/tematicas/configuraciones-dispositivos/actualizaciones-de-seguridad>

Organización de Estados Americanos. (1978). Convención Americana sobre Derechos Humanos. Disponible en: https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Organización de las Naciones Unidas (ONU). (1976). Pacto Internacional de Derechos Civiles y Políticos (PIDCP). Disponible en:

https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ccpr_SP.pdf

Organización de las Naciones Unidas. (1948). Declaración Universal de Derechos Humanos. Disponible en: https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf

Organización de las Naciones Unidas. (2006). Convención sobre los Derechos del Niño. Disponible en: <https://www.un.org/es/events/childrenday/pdf/derechos.pdf>

Organización de las Naciones Unidas. Principios de Naciones Unidas sobre la Aplicación de los Derechos Humanos en la Internet. Disponible en: https://www.un.org/sites/un2.un.org/files/principios_globales_onu_integridad_informacion.pdf

Serra, J. (2023). *¿Por qué es tan importante la actualización de antivirus? Te enseñamos cómo hacerla.* Artículo en línea para Ciberseguridadtips. Disponible en: <https://ciberseguridadtips.com/actualizacion-de-antivirus/>

WeLiveSecurity. (2022). *Autenticación en dos pasos: qué es y por qué es clave para evitar el robo de cuentas.* ESET Latinoamérica. Artículo en línea. Disponible en: <https://www.welivesecurity.com/la-es/2022/12/22/doble-factor-autenticacion-que-es-porque-lo-necesito/>

Zendesk. (2024). *¿Qué es la ciberseguridad y cuál es su relación con la IA?.* Artículo en línea. Disponible en: <https://www.zendesk.com.mx/blog/ciberseguridad/>