In Focus: security and main digital threats in Latin America

DERECHOS DIGITALES
América Latina

IN FOCUS: SECURITY AND MAIN DIGITAL THREATS IN LATIN AMERICA

This publication was produced by Derechos Digitales, an independent non-profit organization founded in 2005, whose mission is the defense, promotion, and development of fundamental rights in digital environments in Latin America.

DERECHOS DIGITALES
América Latina

General Supervision: Rafael Bonifaz and Mayra Osorio

Author: Valentín Díaz

Revision and proofreading: Rafael Bonifaz, Mayra Osorio, Juan Carlos Lara

English and portuguese translation: English-Gonzalo Bernabó / Portuguese-Dafne Melo

Design: Alter Studio

This report is the result of a joint work within the Latin American Observatory on Digital Threats (OLAD), an alliance of Latin American organizations that include Código Sur (regional), Colnodo (Colombia), Conexión Segura (Venezuela), Derechos Digitales (regional), Escola de Ativismo (Brazil), Fundación Acceso (regional), Fundación InternetBolivia. org (Bolivia), Fundación Karisma (Colombia), Instituto Nupef (Brazil), LaLibre.net Tecnologías Comunitarias (Ecuador), MariaLab (Brazil), Social TIC (Mexico), Sursiendo (Mexico) and Taller de Comunicación Mujer (Ecuador).

December, 2024

INDEX

IN FOCUS: SECURITY AND MAIN DIGITAL THREATS IN LATIN AMERICA

REPORT - DECEMBER 2023-MAY 2024

1.INTRODUCTION

The defense of human rights in the digital spectrum is a task that has become fraught with obstacles in Latin America, with governments increasingly using technology as a weapon against political dissent, and a growing presence of criminal actors online. In this scenario, we have cyber attacks on public services, massive collection and misuse of personal data by public and private entities, state espionage, and harassment of various vulnerable communities such as human rights and diversity advocates, activists, and journalists. These are just some of the online threats and human rights violations to which civil society actors are exposed in the world's most dangerous region for social leaders (Tarazona, 2024).

Keeping the internet free, open, and secure has become an imperative to guarantee the exercise of rights, as it has become an essential space for activism and the defense of human rights. In the current hostile regional context, the defense of human rights in the digital space requires greater cross-border efforts. The monitoring and response to cases by different organizations in terms of security and analysis of digital threats with a critical social approach lacks compilation and systematization as a regional phenomenon.

This report is the result of joint work within the Latin American Observatory on Digital Threats (OLAD), an alliance of Latin American organizations working in defense of online human rights, committed to joining forces to enhance the understanding of the behavior of digital security incidents from a regional perspective.

OLAD began its formation in 2021 and has undergone several maturation processes leading up to the publication of this report. Today, the following organizations are part of this alliance: Código Sur (regional), Colnodo (Colombia), Conexión Segura (Venezuela), Derechos Digitales (regional), Escola de Ativismo (Brasil), Fundación Acceso (regional), Fundación InternetBolivia.org (Bolivia), Fundación Karisma (Colombia), Instituto Nupef (Brasil), LaLibre.net Tecnologías Comunitarias (Ecuador), MariaLab (Brasil), Social TIC (México), Sursiendo (México) y Taller de Comunicación Mujer (Ecuador).

Each OLAD organization fulfills different functions in their respective geographical areas and within each country's context. Some of them focus, for example, on investigating and monitoring cases of cyber espionage or censorship of activists and journalists, while others concentrate on the democratization of technology and the protection of historically vulnerable or marginalized groups from attacks in digital spaces, expressions of prejudice based on inequalities of gender, race, social class, sexual identity, age or disability.

In October 2023, several OLAD members held a meeting in Santiago, Chile, where they agreed to conduct the *In Focus* report, a collaborative follow-up on digital security incidents. This report presents a synthesis of these organizations' work spanning a period between December 2023 and May 2024. It also aims to provide insights into the Observatory's processes by identifying strengths and challenges for the future, considering the typical complexities of collaborative work.

2.METHODOLOGY

The *In Focus* report is developed using a mixed methodology, which combines the analysis of data collected in the organizations' daily work with the qualitative experience derived from the discussions held during the different phases of work with the Observatory.

Two data collection methods were developed to achieve this objective. The first is a joint effort to monitor the digital security context in Latin America, which will be referred to in this report as "context monitoring." The second method is a data schematization of cases handled by each OLAD organization, which will be referred to in this report as the “Own Cases report.” The data collection period for both processes was set from December 2023 to May 2024.

The OLAD team collected a series of documentary information inputs for context monitoring. They conducted a curation of press articles and civil society publications on relevant digital incidents and threats recorded in Latin America during the reported period and compiled monthly reports to facilitate a general analysis of what happened during these six months. Among the analyzed incidents are cyber-attacks affecting public infrastructure and state services in the countries studied, situations of cyber-bullying and censorship of activists, and serious human rights violations using surveillance technologies against civil society.

On the other hand, the own cases report consists of data collection based on the cases handled by each organization participating in OLAD, using their own mechanisms, care protocols, and data anonymization measures. Since the Observatory is a coalition of organizations of different types working in diverse contexts, the data collected for the Own Cases report are equally diverse and should not be seen as a comparative measurement between cases, countries, or organizations.

It should be noted that the report presents a limitation bias related to the thematic lines of each organization involved in the OLAD. Therefore, the figures and numbers given in the Own Cases report should be analyzed from different points of view, compared to the natural tendency of this type of report to generate rankings. Instead, such data should be seen as a representation of the work carried out by the organizations belonging to the Observatory.

Despite these disparities, the OLAD team identified four common issues addressed by the participating organizations. These are surveillance and espionage, digital gender-based violence, attacks on critical infrastructure, and violations of online freedom of expression in the countries where the organizations work.

The cases documented between 2023 and 2024 are divided into three periods. The first report collected data from December 2023 to January 2024 and included 163 cases; the second from February to March 2024, with 135 cases; and a final report from April to May 2024, with 113 cases. The organizations attended 411 cases from December 2023 to May 2024.

3. DIGITAL SECURITY CONTEXT IN LATIN AMERICA

This section provides an overview of the current situation of digital security breaches and incidents in the region during the period under review. As indicated in the Methodology section, this chapter is based on press articles and reports on cases of digital attacks and breaches of broad scale or social impact affecting various historically marginalized groups. It is worth mentioning that the incidents detailed in this section do not represent the total number of events recorded in the region during the specified period but rather a sample resulting from constant monitoring work.

3.1 BOLIVIA

Bolivia experienced one of the most intense times of political polarization in recent years during the period covered by this report. A clear split in the ruling party (Molina, 2023) separated those loyal to the government of Luis Arce from those who remained in line with former president Evo Morales. Meanwhile, in June 2024, a failed coup attempt (BBC News Mundo, 2024) further strained the already divided public opinion.

With 62% of the population self-identifying as indigenous (National Institute of Statistics of Bolivia, 2024), the social muscle of Bolivian party politics is built on the rural population. The national political situation also affects community organization, as the current ruling party emerged from grassroots organizations with a plurinational approach (Do Alto, 2007).

In May 2024, the LatAm Journalism Review published a compilation of local organizations' research on disinformation in rural communities in Bolivia, Peru, and El Salvador (Knoerr, 2024). According to an investigation by ChequeaBolivia, in three rural localities (Villa Tunari, Cochabamba; Yacapaní and Montero, Santa Cruz), online disinformation intensified during the political and electoral crisis of 2019, which ended with the departure of Evo Morales from power and massive protests, with significant participation of rural organizations, against the interim government of Jeanine Añez, leaving dozens of people dead (ChequeaBolivia, 2024). The report shows that the indigenous population was particularly exposed to disinformation during these events.

With a new government but still in a polarized context, rural communities could face new attempts to manipulate public discourse.

3.2 BRAZIL

In April 2024, the Brazilian judiciary opened an investigation against tycoon Elon Musk, the majority shareholder of X (formerly Twitter), and pointed him out as responsible for a “criminal instrumentalization” to obstruct justice (Folha de Sao Paulo, 2024), after the reactivation of several user accounts that had been ordered by the judiciary to be closed because they were considered to be amplifiers of disinformation. Musk then responded with a series of public disqualifications of the judge who made the decision (DW, 2024). The fact deepened the crisis of relations between the platform and the government, leading to the temporary suspension of the social network nationwide by order of a judge of the Supreme Federal Court (STF), under the requirement that the company appoint a legal representative in Brazil, the second largest market for X in the world (BBC News Mundo, 2024).

This scenario is compounded by the fact that Elon Musk also owns the satellite internet company Starlink, whose traffic volume tripled in Brazil that year, according to Cloudflare Radar’s 2023 annual report, especially in uncovered rural areas (Belson, 2023). Seeking alternatives to this dependence, the government signed a memorandum of understanding with China in November 2024 to use its constellation of commercial satellites to provide broadband connectivity to remote areas (Xinhua English, 2024).

The legal conflicts between the Brazilian government and X occurred after the platform’s ownership change following Musk’s complex hostile takeover process (BBC News Mundo, 2024). In 2022, the platform, then called Twitter, agreed to a set of restrictive rules ordered by the Brazilian Superior Electoral Court (TSE) to protect the presidential election from the impact of disinformation. The regulation left it up to the Court to decide what content should be removed from the platform, under threat of heavy fines for every hour of delay in moderation efforts (Chambers, 2022).

Then-President Jair Bolsonaro and some of his supporters had long been speaking out about the alleged lack of transparency of the TSE and, on several occasions, sowed doubts about the reliability of the country’s electronic voting system (Diaz, 2022). Despite the restrictions the TSE imposed on the leading platforms and Bolsonaro’s silence after the announcement of the results declaring Lula the winner, on January 8, 2023, thousands of supporters of the defeated candidate invaded and vandalized the buildings of the

Congress, the Presidency and the Federal Supreme Court (STF) (BBC News Mundo, 2024). After Musk's acquisition, the Supreme Court opened an investigation against the tycoon for allegedly failing to contain disinformation directed at the TSE (Biller & Sá Pessoa, 2024).

Also in April, extensive research by The Influence Industry Project analyzed how electoral disinformation on Meta's platforms (Facebook, Whatsapp, and Instagram) played a role in the democratic destabilization attempts of 2023 (Maia, 2023). In May, the Brazilian judiciary signed a memorandum of understanding with several companies, including Meta, TikTok, Google, Kwai, and LinkedIn, to redouble efforts against disinformation (Abrão, 2024).

The co-responsibility of the platforms regarding electoral integrity, the defense of democracy, and trust in the country's democratic institutions are issues that have been widely discussed in Brazil. In this search, the different branches of government have been adopting regulations and holding debates for several years, both parliamentary and directed toward civil society (Global Freedom Of Expression Columbia University, 2020). On this path, Brazil has encountered not only Musk's frontal resistance but also the constant lobbying generated by a handful of big tech companies to slow down or torpedo regulatory projects (Colombo, 2024). In January 2024, for example, after an investigation, the Federal Police concluded that Google and Telegram had "abused their economic power" to oppose the passage of a bill to combat disinformation (Falcão, 2024). In the delicate balance between the health of Brazilian democracy and freedom of expression, disinformation remains one of the main challenges of a networked Brazil.

In December 2023, the government took a significant step forward regarding privacy by launching an application that allows theft victims to lock their devices remotely. This feature facilitates reporting and allows victims to secure sensitive information quickly (EFE, 2023).

On the legislative front, the Senate has been discussing a draft regulatory framework for artificial intelligence (Projeto de Lei n° 2338, 2023) since the end of 2023, which has been welcomed by local human rights and technology organizations (Coalizão Direitos Na Rede, 2024). In 2024, the Social Communication Council of the National Congress convened to discuss bills that would make journalistic content subject to remuneration by the platforms where it is shared (Câmara dos Deputados, 2024).

In January 2024, the Federal Police announced an investigation against former officials of the Brazilian Intelligence Agency (Abin) during the Bolsonaro administration, accused of having illegally surveilled some 30,000 people, including journalists and STF magistrates (Sadi, 2024). The accusations involve federal deputy Alexandre Ramagem, who was director of the unit in Bolsonaro's government, allegedly responsible for the illegal use of software of Israeli origin called FirstMile by the company Cognyte, which allows the interception of the geographic position of a mobile device through its GPS signals, through an alteration of the SS7 protocol handled by the country's telecommunications companies, information that is confidential by law (BBC News Brazil, 2024).

In March 2024, an investigation by Intercept Brazil uncovered the use of a tool that allows the collection of open-source intelligence (OSINT) in private profiles on Facebook by more than a dozen public agencies (Ameno, 2024). This revelation reopened the question of governments' roles and the limits of the collection of personal data for the security of citizens.

3.3 COLOMBIA

Colombia began 2024 with a missed opportunity to pass a bill on gender-sensitive technology. The bill was approved for debate in January and stemmed from an order from the country's Constitutional Court for the State to begin addressing gender-based violence in the digital space (Moreno, 2022). During the parliamentary debates (Castañeda, 2022), the original proposal was subject to amendments that completely redefined the original concept of the law, the protection of persons exposed to gender-based violence (Karisma, 2024). In May, with just a change in the order of three words, the legislature left the door open to a new range of definitions of digital violence (Moreno, 2024), which included mentions of the protection of public officials who raise suspicions of the human rights community in digital environments[1].

In February, with the presentation of the National Digital Strategy to 2026 (Ministry of ICT, 2024), the government of Gustavo Petro sought a direction towards digital transformation. The strategy conceives digital transformation as a holistic policy divided into four pillars: connectivity, data infrastructure, trust and digital security, and promotion of digital skills.

[1] Both the first version of the bill, proposed in the First Permanent Constitutional Commission of the Senate and the subsequent versions with the modifications mentioned in this report appear in the official gazette of the Colombian Congress. In its first version, it appears in gazette N 605 of 2023. The most recent version, which ended up archived, appears in gazette N 342 of 2024. Both can be found in the search engine of the Congressional Gazette (Congreso de la República de Colombia, n.d.).

At the beginning of 2024, a ransomware-type[2] cyberattack on the portals of the Salud Total health insurance company affected health services in a system with 4.8 million members (Rodríguez, 2024). In a country where private providers manage the public health system, the National Health Superintendence had no choice but to issue a statement.

In March 2024, Gur Meggido, an Israeli journalist for the Haaretz newspaper, stated in an investigation that Colombia paid 13 million dollars in cash for acquiring the spy software Pegasus from the Israeli NSO Group (Megiddo, 2024). Months later, President Gustavo Petro (Beltrán, 2024) denounced this same information, attribution the purchase to his predecessor Iván Duque in 2021, when Colombia was experiencing massive protests that lasted several months.

In April, Defense Minister Iván Velásquez confirmed (Revista Semana, 2024) the presence of profiles associated with the largest group of dissident fronts of the now-extinct FARC guerrillas, the Estado Mayor Central (EMC), on the social network TikTok following the publication of a journalistic investigation (AFP, 2024). The guerrillas send recruitment messages to Colombian youth on this Chinese-origin social network. General Helder Giraldo, then Commander-in-Chief of the Armed Forces, declared that the activities of the dissidents on this social network were “a flagrant violation of the ceasefire” that was in effect at the time due to the peace talks with the Colombian government.

3.4 ECUADOR

Recently, the security crisis in Ecuador has escalated to new levels, leaving behind a record homicide rate of 47 per 100,000 inhabitants in 2023 (Observatorio Ecuatoriano de Crimen Organizado, 2024), the highest in Latin America. Among the most significant violent events were the assassination of presidential candidate Fernando Villavicencio in August 2023 (BBC Mundo, 2023) and the national wave of armed violence that the country experienced in January 2024 (Cañizares et al., 2024), which gained worldwide notoriety for the hostage-taking of state television workers by an armed group during a live broadcast.

These events led President Daniel Noboa to declare a state of internal armed conflict, allowing the country’s militarization (BBC News Mundo, 2024). This situation resulted in a series of human rights violations, primarily perpetrated by the military, including cases of extrajudicial executions, forced disappearances, and numerous reports of torture in

[2] Ransomware: Malware that blocks a device by encrypting its contents. It is used for extortion, demanding a ransom to release the information (ESET, n/a).

the streets and prisons of the country (Human Rights Watch, 2024). Simultaneously, the government launched a smear campaign against human rights defenders who were exposed before the official narrative (Amnesty International, 2024), an apology for military abuses that was also widely disseminated by social media users during the first months of the conflict declaration (Curipoma, 2024).

In this context, the Permanent Committee for the Defense of Human Rights (CDH Guayaquil), which represents dozens of victims of human rights violations in Guayaquil, including families of persons deprived of their freedom, denounced in February a cyber attack that disabled their emails. The organization described this as “a deliberate act of intimidation resulting from the denunciations of the abuse exercised by the Armed Forces” (@cdh.gye, 2024). In the same month, the journalist protection NGO Fundamedios sent an alert about a series of cyberattacks, more than 300 since December 2023, against the journalistic portal Indómita Media, which constantly publishes about the deteriorating human rights situation in Ecuador (Fundamedios, 2024).

As a prelude to these events, in December 2023, a court case linked to a deceased drug trafficker rocked the investigation into the assassination of presidential candidate Fernando Villavicencio (Attorney General’s Office of Ecuador, 2024). Conversations extracted from the phone of Leandro Norero, a crime boss killed in a prison massacre in 2022 (BBC News Mundo, 2024), revealed links between the drug trafficker and employees of ECU-911, the state emergency response and coordination center that manages an extensive national network of surveillance cameras (ECU-911, s/f-a).

For the so-called Metastasis case, the Attorney General’s Office released a series of conversation records from Norero’s Threema application with several public figures, including journalists, police officers, prison guards and judicial officials. One of the released chats showed that Norero had used software from the national emergency response system, ECU-911, to monitor Villavicencio (Bonifaz, 2024), information that was later acknowledged by the director of the entity as a case of “misuse” of its technologies in January of this year (Primicias, 2024). The software used was Mobile Locator, a geolocation software that, according to ECU-911 itself, “provides an approximate location of a person’s call to the single 911 emergency line from a telephone” (ECU-911, n/d-b).

At the same time, the country’s National Assembly attempted to pass a Digital Security Law that would, for the first time, install a debate on the prevention and treatment of digital threats and cyber-attacks. Without being exempt from controversial articles

(Carrillo, 2024), the pioneering project at least meant an acceleration of the public debate on cybersecurity. However, the project was eventually shelved due to a lack of political support (National Assembly of Ecuador, 2024).

In December 2023, the Comptroller General's Office began an audit of the contracting process for installing an internet voting system designed for the Ecuadorian migrant community abroad for the first round of elections in August of that year (El Universo, 2023). Implementing this technology failed (La Barra Espaciadora, 2024), as the platform collapsed and users reported problems from early morning hours in exercising their right to vote. Later, Diana Atamaint, president of the organization, confirmed that the platform had been subject to a cyber-attack, and it was therefore decided to suspend the counting of votes and ignore the results for this population. It subsequently emerged that the hired company had no experience in the field.

In the judicial sphere, the case of the Swedish computer scientist Ola Bini, who was indicted by the Ecuadorian prosecution on charges widely questioned by civil society organizations (Bonifaz & Silva, 2024), ended this year. However, the outcome did not align with the expectations of his defense and human rights organizations. In a surprising turn of events and based on an argument that lacked technical precision, an appeals court overturned a first-instance sentence that had found him not guilty of the crime of non-consensual access to a computer system (CNN Español, 2024b). With this conviction, the computer scientist was sentenced to one year in prison, but days later, the same court accepted a request for a conditional suspension of the sentence. In other words, Ola Bini is a free man, although convicted by justice. The Swede was arrested under questionable circumstances (Electronic Frontier Foundation, 2021), as his arrest coincided with the expulsion of Wikileaks founder Julian Assange from the Ecuadorian embassy in the United Kingdom, where the Australian had been in asylum since 2012. Ola Bini and Julian Assange were close friends, and then President Lenín Moreno, with the support of his Interior Minister María Paula Romo, linked the Swede to alleged destabilization attempts.

3.5 EL SALVADOR

El Salvador is experiencing a reported erosion of its democracy under the government of Nayib Bukele (Bernal, 2024). Despite an explicit constitutional prohibition, Bukele was reelected this year with the approval of the Supreme Electoral Tribunal (CNN

Español, 2024). As in the cases of Venezuela and Nicaragua, mentioned below, these social processes have repercussions in the digital spectrum.

Already in 2022, Human Rights Watch warned (Taraciuk, 2022) of the Legislative Assembly's approval of a series of legal reforms, including amendments to the Penal Code and the Law on Computer Crimes (Derechos Digitales, 2022), which, among other things, include conduct such as obtaining confidential material in the category of cybercrime, threatening the practice of journalism.

In 2023, the country ranked 115th out of 180 in the Reporters Without Borders (RSF) Press Freedom Index; in 2024, it fell 18 to 133rd (RSF, 2024). As background, in 2022, the University of Toronto's Citizen Lab published an extensive investigation revealing illegal violations using Pegasus spyware on the phones of CSO representatives and journalists, including 22 journalists from the investigative portal El Faro (Gavarrete et al., 2022).

Later that year, a group of media workers filed a lawsuit against the company in U.S. court. However, in March 2024, a California judge dismissed the case. In its appeal, the group of journalists won the support of the giants Microsoft and Google, two manufacturers whose products Pegasus breached to access the communications of El Faro's employees (Gressier, 2024).

3.6 MÉXICO

Over the past two years, Mexico has attempted to pass legislation related to digital human rights, cybersecurity, and digital harassment but has not succeeded in promoting and discussing these ideas. In fact, three federal bills proposed by legislators have stalled without progress (Reyes, 2024).

In January 2023, a database containing sensitive personal data of several reporters circulated in a leaks forum (Osorio, 2024). Subsequently, it became known that the database came from the presidential press accreditation system for entering the morning conferences of former President Andrés Manuel López Obrador. This occurred in a delicate context, as Mexico is the most dangerous country for the practice of journalism outside of active war zones (RSF, 2024).

In February, the country made headlines with a new situation of excessive surveillance when an R3D investigation revealed some of the activities of the Cyberspace

Operations Center (COC) (R3D, 2024a) attached to the Ministry of National Defense. The COC, operating under the pretext of "military operations in cyberspace," monitored the activity of users critical of the military on social media in an attempt to influence public opinion, including through the use of bot accounts.

In the same month, the State faced new scrutiny in the Pegasus case (Article 19, 2024) when the Supreme Court of Justice ordered the Secretariat of Finance to disclose the information collected by this entity in an investigation into the purchase and use of the Israeli spyware, which has been the subject of hundreds of complaints about governments using this tool to persecute activists, journalists, and political dissidents. With very slow progress, the Pegasus case in Mexico is far from closed.

A month earlier, the only person charged with the illegal wiretapping of journalist Carmen Aristegui's phone with Pegasus, operator Juan Carlos García, was acquitted by a federal judge, who considered that the Attorney General's Office had failed to prove his participation in the crime (Proceso, 2024). However, the judge acknowledged that the journalist had been illegally wiretapped and stated that the case should be reopened because the prosecution had not made sufficient efforts to ensure justice.

Meanwhile, in April 2024, civil society organizations widely questioned Coppel, the retail and consumer credit giant, for its silence in the face of a cyberattack that massively affected its services and whose technical characteristics were never made clear to consumers (R3D, 2024). Independent voices assured that it must have been a ransomware-type attack.

3.7 NICARAGUA

As a report in September 2023 indicated, the measurement balance of human rights in digital environments in Nicaragua is negative (Derechos Digitales, 2023). The document pointed out important precedents dating back to the massive and prolonged protests of 2018, which were brutally repressed by Daniel Ortega´s government (OAS, 2018).

A report by the Inter-American Commission on Human Rights (IACHR) that year cited grave human rights violations, including extrajudicial executions, cases of torture, and hundreds of arbitrary detentions, as well as acts of censorship against citizens, journalists, and media outlets (Inter-American Commission on Human Rights, 2018).

At the same time, repression was also present in the digital space. Actions such as the interruption of internet access, the criminalization of online expression, attempts to manipulate public opinion, and mass surveillance of telecommunications are just some of the many challenges facing Nicaraguan civil society, which must overcome increasingly complex obstacles.

In February 2023, the Ortega government implemented the unprecedented decision to strip more than 300 critics of his mandate of their Nicaraguan citizenship, an act widely condemned by human rights organizations (Yuhas, 2023). A legal framework for that figure was only established in January 2024, when the Nicaraguan National Assembly approved a constitutional reform that allows the withdrawal of nationality from citizens convicted of treason (EFE, 2024). In September, Ortega once again utilized this resource after releasing over a hundred political opponents from prison and expelling them to the border with Guatemala (EFE, 2024).

3.8 VENEZUELA

The first half of 2024, an election year for Venezuela, appeared to be a preamble to what finally happened in July and August (United Nations Human Rights Council, 2024). The Venezuela diagnosis in this report is limited by its own methodological factors, which establish a time window (December 2023 to May 2024) that prevents an in-depth analysis of the events that followed the widely questioned reelection of Nicolás Maduro (The Carter Center, 2024) and his subsequent process of political repression in response to social protest. Thus, in this report, the context report for Venezuela can be seen as an analysis of the policies and decisions that paved the way for the election.

The Report on the situation of digital human rights in Venezuela 2022+2023, by VE sin Filtro, warned of the existence of a “massive” state apparatus for interception of telecommunications and arbitrary practices by the authorities, such as the demand for access to personal data and conversations through the confiscation of devices (VE sin Filtro, 2023). The report mentions the abusive use of social media surveillance, often directed at journalists and activists, and its use to intimidate, threaten, and spread stigmatizing speech against political dissidence. The report also addresses the problem of scarce and precarious connectivity for the average Venezuelan, constantly decimated by recurrent power outages throughout the country.

The 2023 annual report on digital rights, Algorithms of Silence, found 128 human rights violations in cyberspace against journalists, citizens, and civil society organizations (Instituto Prensa y Sociedad, 2023). The document also states that 46 independent media outlets remained blocked by internet service providers operating in the country during the year. Some of these blockages were reported a few months before the elections, as with the portals El Político, Impacto, and La Gran Aldea (Espacio Público, 2024).

In February 2024, Digitel, one of the country's largest phone companies, suffered a ransomware attack that compromised the personal data of thousands of users and exposed the weak infrastructure used by several of the country's main companies (@ vesinfiltro, 2024).

In April, the government promoted a bill called the Law against Fascism, Neo-Fascism and Similar Expressions, which includes a very vague definition of what it considers "fascist" behavior and exposes people to prison sentences for it, which NGOs say could have a restrictive effect on freedom of expression in the country (Programa Venezolano de Educación Acción en Derechos Humanos, 2024).

In May, Venezuela's current Minister of Foreign Affairs, Diosdado Cabello, announced on his television program the introduction of a bill to limit foreign funding for civil society organizations (Con el Mazo Dando, 2024). The possibility of including legislation of this type in the Venezuelan legal system was already considered in 2022 and 2023 (Calderón, 2024). Finally, days after Maduro's reelection, the law was approved by a majority in the National Assembly (Amnesty International, 2024).

4. THEMATIC AREAS AND CASE STUDIES

This section categorizes a series of systematizations of information from different sources. Some of these systematizations are based on data, while others are derived from the discussion of shared experiences and the identification of patterns during the various meetings organized by the Observatory.

This chapter aims to provide a more in-depth and focused analysis of the four thematic axes that the Observatory was able to identify in its articulation with the different organizations: digital gender-based violence, attacks on critical infrastructure, surveillance and espionage, and violations of online freedom of expression.

As mentioned above, the data for this report was collected over three periods: 163 cases were collected from December 2023 to January 2024, 135 cases from February to March 2024, and 113 cases from April to May 2024. .

4.1 DIGITAL GENDER-BASED VIOLENCE

Various forms of online expressions of gender-based violence have become an almost transversal axis in the work of most of the organizations that are part of OLAD. For this reason, and due to the number of cases handled, the Observatory has been able to collect enough data to allow for a more in-depth analysis.

The organizations that are part of OLAD and that addressed cases of gender-based violence in the digital space during the respective periods covered by this report were Derechos Digitales (regional), Fundación Acceso (regional), Fundación Internet Bolivia (Bolivia), La Libre (Ecuador), MariaLab (Brazil), SocialTIC (Mexico), and Taller de Comunicación Mujer (Ecuador).

Three of these organizations operate direct help lines and offer accompaniment and response in cases of digital gender-based violence. They assist women, children, activists, human rights groups and people who are part of the LGTBQA+ community. These projects are the S.O.S Digital Center of InternetBolivia.org Foundation (Bolivia), Maria d'Ajuda of Marialab (Brazil) and Navegando Libres of the Women's Communication Workshop Network (Ecuador). In this regard, it is available the report Helplines to address online gender-based violence: *Monitoring and trends in Bolivia, Brazil, and Ecuador,* which delves into common patterns regarding digital gender-based violence in the region (Araújo et al., 2024).

During the first period defined by the Observatory, from December 2023 to January 2024, the organizations reported 28 cases. In the second period, from February to March 2024, the number of cases analyzed increased significantly to 50, representing almost a third of all cases reported in the different work lines. Finally, in the third period, from April to May 2024, 40 cases were counted.

The workflow allowed us to identify common patterns in the nature of cases addressed mainly by organizations that fight against gender-based violence. Therefore, we have divided them into thematic areas approached broadly, given that the characterization of each phenomenon may vary according to the criteria of each organization. The first one corresponds to cases of digital harassment[3], which totaled 39 incidents during the three time periods studied. The second category encompasses the dissemination of intimate or sexual content without the consent of the person concerned[4]. This category had a total of 33 cases during the three periods studied. The third group comprises records of violations against social platform accounts belonging to women or women's groups dedicated to activism in its various forms. Feminist activism has a strong presence in these groups, although not exclusively. The total number of cases in this group during the three periods analyzed is 24.

In all of these forms of online gender-based violence, the data reported by the organizations show that the vast majority of these types of attacks are directed at private individuals and that, in most cases, the aggressors are also usually private individuals. However, there is also a significant percentage of cases where the perpetrator could not be identified.

4.2 ATTACKS ON CRITICAL INFRASTRUCTURE

Another area of interest for the Observatory is attacks on critical websites and infrastructure of organizations defending human rights in the broadest sense. During the period set for preparing this report, OLAD´s organizations addressed more than fifty cases.

Most of the cases considered for this report were reported by La Libre, a small organization based in Ecuador that seeks to provide "solid and accessible" technological infrastructure to organizations, individuals, and social movements working in defense of human rights, nature, justice, and equality. Between December

[3] In the report Helplines to address online gender-based violence cases: Monitoring and trends in Bolivia, Brazil, and Ecuador, which used a different time period, two of the organizations that are part of OLAD (InternetBolivia.org and the Taller Comunicación Mujer network) reported that digital harassment was the second most common type of digital violence reported by their helplines.

[4] This type of case is included in the categorization of digital sexual violence by the helpline Navegando Libres por la Red of Taller Comunicación Mujer, which is identified in the report Helplines to address online gender-based violence cases: Monitoring and trends in Bolivia, Brazil, and Ecuador as the most attended type of digital violence by the organization. In the case of Maria d'Ajuda of Marialab, this behavior is typified as exposure of intimate images and is the third most attended type of violence. In the same report, the S.O.S. Digital Center of InternetBolivia.org Foundation includes this problem in the category of sexual abuse through information technology (ICT), which involves various forms of violence, such as threats and extortion of victims related to the possible publication of intimate content.

2023 and May 2024, La Libre handled at least 34 cases related to attacks on social organizations' and activists' websites. It also handled 22 cases of ransomware or data hijacking.

The disparity in the data reported in this section is mainly due to the fact that a central part of La Libre's work is helping build and maintain infrastructure and providing technical assistance to organizations.

La Libre is present in several countries, although it works mainly in Ecuador. Its co-founder, Jonathan Finlay, assures In Focus that the organization has been working for 10 years to "develop autonomous infrastructures, implement services, and provide technology solutions for human rights and environmental defenders."

La Libre's approach is "oriented to accompaniment," weaving networks with other social organizations "to strengthen the struggle." "In some cases (the organizations) look for us because they are suffering or have suffered an attack because they have lost information, applications, websites, or networks and want to recover them. Sometimes, their organization simply needs to improve the physical infrastructure of their telecommunications or redesign their website," says Finlay.

In other words, La Libre offers a wide range of digital services specially devised for the needs of organizations and people defending rights. The main difference with regular commercial services is that "people who work in human rights are usually in conditions that are not the same as those of a company or a bank," he explains. For this reason, organizations "want to work with someone who understands what they are doing." The idea is to provide "close support," which does not necessarily involve technical aspects.

Not every approach to digital threats refers only to technical issues. In the case of ransomware, for example, once a system's encryption has been completed, the focus is more on "accompaniment and recommendations, firstly to prevent it from happening again, and secondly to recover as much information as possible in the shortest possible time."

At the end of 2023, "devices in several organizations were infected by different means and with different malware programs" in nearly simultaneous ransomware attacks. Laptops and desktops were primarily affected, but the organization also recorded two cases of server infections. Finlay notes that the attacks occurred as part of "threat group campaigns" that sent phishing[5] emails that targeted the administrative areas of the organizations and ended up infecting computers.

Other cases, such as website attacks, can be reactively dealt with. These are typically "denial of service attacks[6], brute-force password guessing, malware infection of websites, or cases where phishing techniques have been used "to take over website credentials and temporarily take control."

In such cases, La Libre evaluates the case on a "scenario by scenario" basis. Depending on the nature of the attack, technical solutions can be simple, or, in more complex cases, regaining control of a site or network can be a long and tedious process.

4.3 SURVEILLANCE AND ESPIONAGE

The cases of Mexico and El Salvador, described in the chapter on regional context, illustrate the seriousness of cases in which espionage technologies supposedly designed to enforce the rule of law have been used for political or personal purposes by those in a position to use the State's monopoly on the use of force.

El Salvador's case with Pegasus is somewhat more recent than that of Mexico, where the first reports of its use date back to 2017 (BBC Mundo, 2017). However, its use was not revealed until the publication of a transnational journalism project in 2021. It exposed a series of wiretaps of hundreds of personalities among journalists, activists, and government officials worldwide (Forbidden Stories, 2021).

In Mexico, the government of Enrique Peña Nieto used the spyware[7] against 15,000 people, including family members of the victims of the 2014 Ayotzinapa massacre (Romero, 2021). A member of OLAD has been working on issues of state espionage in this country for years: SocialTIC. In April 2023, the organization published a joint report

[5] Phishing: A malicious social engineering technique that consists of sending fraudulent emails, text messages, calls, or websites to trick users into sharing their personal data, access credentials to a platform, or forcing them to download some type of malware onto their device (Kosinski, 2024).

[6] Denial-of-service attack: A type of malicious cyberattack that consists of an interruption of a service. It usually works by overloading requests on a website, for example, causing an interruption of service when the server receives more requests than it can process simultaneously (Cloudflare, n/d).

[7] Spyware: Software designed to collect confidential data from a device without the owner's consent. Spyware is usually installed on a device through deception (Kaspersky, n/d).

with Centro Prodh, R3D, and Article-19, revealing evidence of new cases of Pegasus spying by the military against human rights defenders from Centro Prodh (Centro PRODH et al., 2023). A month later, the New York Times reported another major case of wiretapping of the undersecretary for human rights, Alejandro Encinas (Kitroeff & Bergman, 2024).

In Mexico, organizations follow a coordinated workflow to handle cases of illegal surveillance using Pegasus. Through an alliance called the Digital Rights Coalition, which includes SocialTIC, R3D, the Prodh Center, and Article 19, "each organization has a very precise role" when a case arises, says Paúl Aguilar, digital security coordinator at SocialTIC.

R3D is responsible for providing legal representation to victims. Article 19 documents freedom of expression violations, while Centro Prodh documents human rights violations that may occur in each case. SocialTIC, on the other hand, is responsible for the technical aspects of the investigation, including analyzing devices and other actions. This task is often conducted in collaboration with the CitizenLab of the University of Toronto.

SocialTIC's work is not limited to spyware detection. The organization also conducts a series of training with the victims "to help them configure their devices" and take the necessary measures so that a similar situation "cannot be repeated" or at least "make it more difficult for the attacker."

SocialTIC offers "permanent attention to people who could be or have been monitored by any kind of media." This is done on an individual basis, "especially for journalists who have been spied on before" and of whom there are new suspicions of intervention. "This shows that we are witnessing a recurrence of cases," says Aguilar. In some cases, it is Pegasus, but in others, "there are indications that other technologies are being used" in Mexico. It is not limited to spyware but also includes communications interception, invasive social media monitoring, physical tracking, and network harassment campaigns. Aguilar explains that "it is a broader surveillance and espionage operation, not just focused on spyware.

SocialTIC also works with organizations that accompany groups of people under surveillance. These accompaniments are "much more extensive because they involve working with the entire organization," he says. Mexico is organized politically under a decentralized federal system, which grants its constituent states a range of powers, including their security systems at the municipal and State levels. Although Pegasus is sold only to the central government and its defense agencies, the use of other surveillance and spying technologies in the states is on the rise.

“There are other technologies that the states are purchasing, maybe of a lower range. So, it seems that they have access to other types of spyware, less sophisticated, to other technologies of communications intervention and tracking, less sophisticated. It is in proportion to their economic capacity”, Aguilar points out, adding that “there is evidence that almost all 32 states have purchased this type of technology (...) We are working on demonstrating that they have used them against civil society”.

4.3 VIOLATIONS OF ONLINE FREEDOM OF EXPRESSION

The fourth area of OLAD’s observations focuses on violations of online freedom of expression. In this domain, the organizations that make up the Observatory addressed 92 cases of attacks on freedom of expression within their respective countries.

Derechos Digitales, Marialab, SocialTIC, La Libre, Fundación Internet Bolivia, and Sursiendo reported cases under this category. Among all the organizations, 34 social media accounts were recovered. Nineteen were from December 2023 to January 2024, nine from February to March 2024, and six from April to May 2024. The account recoveries–which may have been taken away due to cyber-attacks or massive complaint efforts–were carried out on Facebook, Instagram, X (formerly Twitter), and WhatsApp. In general terms, the profiles whose cases are prioritized tend to be those of people involved in the defense of rights, social and environmental activism, and the search for justice and equality.

Another side of this phenomenon can be observed in the registration of smear and defamation campaigns, which are sometimes coordinated. From December 2023 to January 2024, the organizations reported 20 cases under this subcategory; between February and March 2024, 14; and from April to May 2024, there were 24.

In this subcategory, La Libre’s numbers once again stand out. The total number of cases handled by all organizations in the three time periods is 58, of which La Libre handled 51 in Ecuador.

As mentioned in the chapter on the regional context, there has been a hostile situation against human rights defenders in Ecuador since the declaration of an internal armed conflict in January 2024. It is crucial to consider this situation of stigmatization of human rights defenders when referring to the cases handled by La Libre. When it comes to smear campaigns, La Libre works mainly with counseling for the victims.

At the beginning of the year, when the President of Ecuador declared a state of internal war, “there were campaigns, apparently organized by large teams of people very close to the government, attempting to affect organizations demanding respect for human rights.” Several human rights organizations, such as the Permanent Committee for the Defense of Human Rights, which provides free advice to victims of state crimes, were simultaneously targeted by hundreds of accounts.

A search on X, formerly Twitter (X, 2024), filtered between January 9 and 15 with the keywords “defenders” and “criminals” shows hundreds of results like this: “Excellent work @ffaa (the Armed Forces account), and these criminal defenders must be given the same attention,” says a user commenting on a citizen video showing acts of torture by the military. The keyword “Rulay” also leads to this trend. It is the name of a song attributed to a criminal group that turned out to be the soundtrack, as a meme, of dozens of videos of military men exercising torture.

In the first weeks of the declaration of armed conflict, “it was obvious that there were state agencies that were focusing their efforts, especially communications teams and consultants, on carrying out these attacks,” he says. “It was super violent. And it was constant and permanent,” he denounces.

Finlay recalls the case of an organization that works with people deprived of their liberty, which was initially subjected to stigmatizing and violent comments on social media. Soon after, the comments became threats via email and persistent phone calls.

“In this particular case, a process of accompaniment was implemented, proposing strategies to block this interaction for mental health reasons. The actions taken in this scenario included advice on configurations to block and isolate social media content, the design of protocols in the event of threats, and training on call blocking, among others. Finlay defines all of this as “digital security support.

Along with their work in these areas, Karisma (Colombia) and Conexión Segura (Venezuela) have worked closely and have vast experience in documenting and analyzing content censorship, network blocking, and internet failures in social unrest and repression contexts.

In Colombia, Karisma accompanied a case before the Constitutional Court to access public information about a widespread internet shutdown in Cali on one of the most intense days of the 2021 national strike. The government of then President Iván Duque never investigated these facts (Karisma, 2023). Karisma and other organizations defending freedom of expression petitioned the Court to try to clarify the situation (Botero & Parra, 2022). The Court did not determine whether or not the widespread suspension of services was related to the protests. However, it pointed out that the State had failed in its role by not initiating an investigation to clarify the facts at the time.

In contexts where censorship is more direct, as in Venezuela, initiatives in favor of online freedom of navigation and expression must include other approaches. Conexión Segura seeks to promote and disseminate basic security tools by distributing user-friendly materials to teach people, for example, how to use a VPN to access sites that may be blocked in Venezuela, such as news sites. For this purpose, they launched an application for Android devices this year: Noticias sin Filtro (Conexión Segura, 2024).

5. LESSONS LEARNED

CREATION OF A REGIONAL OBSERVATORY

In more than three years of work, with an enormous effort to articulate the member organizations under changing conditions and with an overwhelming burden in their daily work, OLAD has managed to put some common features around the state of human rights in the digital environment in Latin America on the table. Working together has made it possible to strengthen bonds of trust between very different organizations and with different fronts of struggle.

The result is a collective intersectional effort to understand, from a regional perspective, the key aspects of online advocacy: threats to democracy or freedom of press and expression, state abuse, and gender-based violence are just some of the ways in which technology can be used as a coercive element by malicious actors.

The articulation of a group with these characteristics was itself an enormous challenge, as was the discussion process that led to the identification of common patterns in the region and, ultimately, to the drafting of this report.

The greatest challenge has been implementing a system to measure or quantify the results of the joint work of the different organizations, referred to in this report as the

"Own Cases report." This process, as in OLAD's creation in previous years, requires real-time adaptation to the needs of the member organizations.

Creating a regional observatory of digital threats is a complex task, and coordinating common work while developing each organization's agendas in parallel is a major challenge that will need to be analyzed in the next period of the Observatory's work. The wide range of characteristics of the member organizations makes quantitative measurement more complex, so this report recommends the adoption of methodological modifications and adaptations to overcome these obstacles.

At the same time, some methodology aspects should be replicated and even expanded to collect more segmented information to help characterize types of aggression, victims, the profile of the aggressors, and the type of technologies used to violate rights. This is the case, for example, of the data produced by organizations dealing with digital gender-based violence.

Therefore, for the next OLAD cycles, it is necessary to identify which areas of study are appropriate for adopting qualitative processes and which areas need to deepen quantitative measurement.

REFLECTIONS ON THE ANALYZED PERIOD

This report shows that some of the main actors threatening human rights defenders are governments, anti-rights groups that endanger online freedom of expression, criminal actors present in cyberspace, and individuals who, through expressions of sexism and structural racism, affect mainly women and LGBTIQ+ people. The absence of State responses is an almost constant and cross-cutting factor in the region. There is also an upward trend in several regional governments adopting authoritarian policies and strategies, which adds another layer of vulnerability to the affected populations.

Amid an unprecedented crime wave in the region (Crisis Group, 2023), there is a growing presence of criminal actors involved in digital rights violations. An example of this dynamic is the use of a state agency's geolocation system by a criminal leader in Ecuador to monitor the assassinated presidential candidate Fernando Villavicencio. The fact that an organized criminal group can access, in real-time, sensitive personal data of citizens sets off a regional alarm, as what is happening in Ecuador could already be happening in other countries.

In terms of surveillance and espionage, there is a growing trend towards the adoption of such technologies. These technologies are becoming increasingly accessible, especially for local governments. In the case of more sophisticated spyware such as Pegasus, a regional pattern can also be seen as Colombian President Gustavo Petro, at the time of this report, was reviewing an alleged irregular purchase of the spyware during the administration of his predecessor, Iván Duque (El Espectador, 2024).

This makes Colombia the fifth Latin American country reported to have used the software, along with Mexico, El Salvador, Panama, and the Dominican Republic. This report recommends updating the methodology of work in this area, perhaps in a qualitative direction, to find mechanisms for measuring organizations' work from a regional perspective.

Meanwhile, several countries in the region are facing significant challenges with electoral and political disinformation. Brazil, for example, is trying to initiate discussions on the role of social platforms in democracy, with disinformation as a priority. In doing so, the Brazilian State has been confronted with the powerful lobby of large technology companies. In Bolivia, the rupture of the ruling party has resulted in significant polarization, with disinformation gaining ground most strongly in rural indigenous populations. In Colombia, the fight against disinformation has generated numerous legislative proposals, none of which have yet been approved, that contain dangerous censorship mechanisms and endanger the digital ecosystem.

In the same way they affect critical infrastructure, such as an oil pipeline or a bank, the IT threats faced by individuals, communities, and organizations that defend human rights and nature represent a serious violation of their rights. This type of aggression affects individuals and the whole community since it is an attack on the root of the democratic order of their countries. This is the starting point of OLAD's vision, which seeks to provide a Latin American resilience response to the violent digital threats that affect its population, coming from several fronts.

6. REFERENCES

Abrão, C. (2024, junio 6). Corte Suprema de Brasil firma acuerdo con principales plataformas de redes sociales para combatir la desinforma. Gazeta do Povo. https://agenciabrasil.ebc.com.br/justica/noticia/2024-06/stf-assina-acordo-com-redes-sociais-para-combater-desinformacao

AFP. (2024, marzo 4). TikTok, nueva herramienta de reclutamiento guerrillero en Colombia. RFI. https://www.rfi.fr/es/m%C3%A1s-noticias/20240403-tiktok-nueva-herramienta-de-reclutamiento-guerrillero-en-colombia

Ameno, F. (2024, diciembre 3). Farra com dados: Uso de ferramenta que cruza conexões do Facebook e dados da polícia explode no país. Intercept Brasil. https://www.intercept.com.br/2024/03/12/uso-de-ferramenta-que-cruza-conexoes-do-facebook-e-dados-da-policia-explode-no-pais/

Amnistía Internacional. (2024a, agosto 16). Venezuela: Aprobación de Ley anti-ONG castiga la asistencia a víctimas y la defensa de los derechos humanos. Amnistía Internacional. https://www.amnesty.org/es/latest/news/2024/08/venezuela-aprobacion-ley-anti-ong-castiga-asistencia-victimas-defensa-derechos-humanos/

Amnistía Internacional. (2024b, septiembre 24). Colectivos y movimientos al frente de la defensa de derechos humanos en Guayaquil y la costa de Ecuador. Amnistía Internacional. https://www.amnesty.org/es/latest/campaigns/2024/09/colectivos-y-movimientos-al-frente-de-la-defensa-de-derechos-humanos-en-guayaquil-y-la-costa-de-ecuador/

Araújo, D., Mendez, L. A., Osorio, M., Diego, M., Priscilla, P., Venturini, J., & Lobato, C. (2024, noviembre). Líneas de ayuda para atender casos de violencia de género en entornos digitales: Monitoreo y tendencias en Bolivia, Brasil y Ecuador. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/LineasAyuda-ESP.pdf

Artículo 19. (2024, junio 2). SCJN confirma que Hacienda deberá entregar información relativa al caso Pegasus. Article 19 MX-CA. https://articulo19.org/scjn-confirma-que-hacienda-debera-entregar-informacion-relativa-al-caso-pegasus/

Asamblea Nacional del Ecuador. (2024, junio 6). Asamblea Nacional archivó el proyecto de Ley de Seguridad Digital. https://www.asambleanacional.gob.ec/es/noticia/96846-asamblea-nacional-archivo-el-proyecto-de-ley-de

BBC Mundo. (2017, junio 20). Cómo protegerte de Pegasus, el sistema de vigilancia en el centro de las acusaciones de espionaje a periodistas en México. BBC Mundo. https://www.bbc.com/mundo/noticias-40341302

BBC Mundo. (2023, julio 10). Matan en una cárcel de Ecuador a 7 ciudadanos colombianos acusados por el asesinato del candidato presidencial Fernando Villavicencio. BBC Mundo. https://www.bbc.com/mundo/articles/c3gx53lezgjo

BBC News Brasil. (2024, noviembre 25). O que é o FirstMile, software que teria sido usado pela Abin para monitorar jornalistas e ministros do STF. BBC News Brasil. https://www.bbc.com/portuguese/articles/c3g32mz1dzdo

BBC News Mundo. (2024a, abril 16). Twitter vs Elon Musk: Qué es la píldora venenosa con la que la red social quiere evitar la compra hostil del empresario. BBC News Mundo. https://www.bbc.com/mundo/noticias-61124066

BBC News Mundo. (2024b, mayo 10). Quién era Leandro Norero, el patrón, uno de los principales narcos de Ecuador que murió asesinado en la última matanza carcelaria en el país. BBC News Mundo. https://www.bbc.com/mundo/noticias-america-latina-63139767

BBC News Mundo. (2024c, junio 26). Cómo fue el intento de golpe de Estado que denunció el presidente de Bolivia después de que militares tomaran el centro de La Paz y entraran en la antigua sede de gobierno. BBC News Mundo. https://www.bbc.com/mundo/articles/c2jj33v45m7o

BBC News Mundo. (2024d, agosto 1). Cómo ocurrió el asalto de miles de seguidores de Bolsonaro a las sedes de los tres poderes en Brasil. BBC News Mundo. https://www.bbc.com/mundo/noticias-america-latina-64205936

BBC News Mundo. (2024e, agosto 30). 5 preguntas para entender por qué un juez en Brasil ordenó el bloqueo de la red social X en todo el país. BBC News Mundo. https://www.bbc.com/mundo/articles/c0rwjll15yqo

BBC News Mundo. (2024f, septiembre 1). El presidente Daniel Noboa declara la existencia de un conflicto armado interno en Ecuador y ordena al Ejército restablecer el orden tras varios atentados y la toma de un canal de TV. BBC News Mundo. https://www.bbc.com/mundo/articles/c3gy2zz03dpo

Belson, D. (2023, diciembre 12). Cloudflare 2023 Year in Review. The Cloudfare Blog. https://blog.cloudflare.com/radar-2023-year-in-review/

Beltrán, D. (2024, octubre 24). Gustavo Petro insistió en señalar al Gobierno Duque por la compra de Pegasus: Engañaron al estado de Israel, a la justicia y a Colombia. Infobae. https://www.infobae.com/colombia/2024/10/24/gustavo-petro-insistio-en-sus-criticas-por-la-compra-de-pegasus-enganaron-al-estado-de-israel-enganaron-la-justicia-colombiana-y-enganaron-a-colombia/

Bernal, A. (2024, agosto 3). Las políticas de Bukele: Una amenaza directa a la democracia. Open Democracy. https://www.opendemocracy.net/es/politicas-bukele-amenaza-democracia/

Biller, D., & Sá Pessoa, G. (2024, agosto 4). Elon Musk will be investigated over fake news and obstruction in Brazil after a Supreme Court order. AP. https://apnews.com/article/brazil-musk-x-supreme-court-investigation-a645757b95a66ee658832802908466ab

Bonifaz, R. (2024, febrero 25). Las fisuras de los sistemas de vigilancia en Ecuador. La Barra Espaciadora. https://www.labarraespaciadora.com/editorial/las-fisuras-sistemas-vigilancia-ecuador/

Bonifaz, R., & Silva, I. (2024, abril 26). Ola Bini y la criminalización del conocimiento. Derechos Digitales. https://www.derechosdigitales.org/23597/ola-bini-y-la-criminalizacion-del-conocimiento/

Botero, C., & Parra, J. (2022, octubre 24). El misterio detrás de los cortes de internet en cali durante el paro de 2021. Karisma. https://web.karisma.org.co/el-misterio-detras-de-los-cortes-de-internet-en-cali-durante-el-paro-de-2021/

Calderón, D. (2024, mayo 31). Una propuesta de ley contra el activismo. Derechos Digitales. https://www.derechosdigitales.org/23810/una-propuesta-de-ley-contra-el-activismo/

Câmara dos Deputados. (2024, abril 3). Conselho debate remuneração de conteúdo jornalístico nas plataformas digitais. Câmara dos Deputados. https://www.camara.leg.br/noticias/1039447-conselho-debate-remuneracao-de-conteudo-jornalistico-nas-plataformas-digitais/

Cañizares, A., Alvarado, A., John, T., Rios, M., & AnneClaire, S. (2024, octubre 1). Qué está pasando en Ecuador tras los hechos de violencia que sacuden el país. CNN en Español. https://cnnespanol.cnn.com/2024/01/10/ecuador-violencia-conflicto-armado-estado-excepcion-recap-trax

Carrillo, P. (2024, junio 20). La seguridad digital se hunde en el pantano político. La Barra Espaciadora. https://www.labarraespaciadora.com/ciberespacio/la-seguridad-digital-se-hunde-en-el-pantano-politico/

Castañeda, A. (2022, noviembre 8). Por medio del cual se adoptan medidas de prevención, protección, reparación y penalización de la violencia de género digital y se dictan otras disposiciones. Congreso de la República de Colombia. https://www.camara.gov.co/violencia-digital-de-genero

@cdh.gye. (2024, septiembre 2). CDH Bajo ataque [Post]. Instagram. https://www.instagram.com/p/C3JCcRrOagO/?igsh=dDRod3RkMXNoYjUz

Centro PRODH, R3D, SocialTIC, & ARTICLE 19. (2023, abril). Centro PRODH nuevamente atacado con Pegasus: Cómo la impunidad y la militarización proporcionaron la repetición del espionaje. https://socialtic.org/wp-content/uploads/2023/04/EE_Colibri_final.pdf

Chambers, B. (2022, octubre 21). Tribunal Superior Electoral de Brasil toma medidas contra la desinformación previo a la segunda vuelta presidencial. Agencia Anadolu. https://www.aa.com.tr/es/mundo/tribunal-superior-electoral-de-brasil-toma-medidas-contra-la-desinformaci%C3%B3n-previo-a-la-segunda-vuelta-presidencial/2717000

ChequeaBolivia. (2024, mayo 30). El impacto de la desinformación y los desafíos del periodismo en regiones clave de Bolivia. ChequeaBolivia. https://chequeabolivia.bo/el-impacto-de-la-desinformacion-y-los-desafios-del-periodismo-en-regiones-clave-de-bolivia

Cloudfare. (s/f). ¿Qué es un ataque de denegación de servicio (DoS)? Cloudfare. https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/

CNN Español. (2024a, enero 29). ¿Por qué puede Bukele ser candidato en las elecciones presidenciales de El Salvador en 2024? CNN en Español. https://cnnespanol.cnn.com/2024/01/29/bukele-reeleccion-el-salvador-orix

CNN Español. (2024b, mayo 4). Revocan sentencia de inocencia a Ola Bini, amigo de Julian Assange, y lo declaran culpable de acceso ilegal a sistema informático. CNN en Español. https://cnnespanol.cnn.com/2024/04/05/ola-bini-assange-culpable-ecuador-orix

Coalizão Direitos Na Rede. (2024, agosto 7). Defendiendo la legislación brasileña sobre IA que protege los derechos. Coalizão Direitos Na Rede. https://direitosnarede.org.br/2024/07/08/defendiendo-la-legislacion-brasilena-sobre-ia-que-protege-los-derechos/

Colombo, G. (2024, marzo 23). Lobby de big techs trava enfrentamento às fake news, dizem advogados. Poder 360. https://www.poder360.com.br/brasil/big-techs-sao-desafio-para-tse-conter-fake-news-nas-eleicoes/?ref=nucleo.jor.br

Comisión Interamericana de Derechos Humanos. (2018, junio 21). Graves violaciones a los derechos humanos en el marco de las protestas sociales en Nicaragua. Comisión Interamericana de Derechos Humanos. https://www.oas.org/es/cidh/informes/pdfs/Nicaragua2018-es.pdf

Con el Mazo Dando. (2024, mayo 20). Cabello sobre Ley de Fiscalización de las ONG: Van a tener que explicar de dónde vienen los fondos. Con el Mazo Dando. https://mazo4f.com/cabello-sobre-ley-de-fiscalizacion-de-las-ong-van-a-tener-que-explicar-de-donde-vienen-los-fondos

Conexión Segura. (2024). Noticias Sin Filtro. https://noticiassinfiltro.com/

Congreso de la República de Colombia. (s/f). Gacetas del Congreso de la República de Colombia [Dataset]. Gacetas del Congreso. Recuperado el 12 de abril de 2024, de http://svrpubindc.imprenta.gov.co/senado/index.xhtml

Consejo de Derechos Humanos de las Naciones Unidas. (2024, octubre 15). La Misión Internacional de la ONU revela graves violaciones de derechos humanos en Venezuela durante el período electoral 2024. Consejo de Derechos Humanos de las Naciones Unidas. https://www.ohchr.org/es/press-releases/2024/10/un-international-mission-reveals-gross-human-rights-violations-venezuela

Crisis Group. (2023, diciembre 5). América Latina lucha contra una nueva ola de criminalidad. Crisis Group. https://www.crisisgroup.org/es/latin-america-caribbean/latin-america-wrestles-new-crime-wave

Curipoma, L. (2024, noviembre 4). El perverso goce ante la violación de derechos humanos en detenciones militares. INREDH. https://inredh.org/el-perverso-goce-ante-la-violacion-de-derechos-humanos-en-detenciones-militares/

Derechos Digitales. (2022, noviembre 2). Las reformas legales en El Salvador: Un gran retroceso en los derechos humanos y el Estado democrático. Derechos Digitales. https://www.derechosdigitales.org/17840/las-reformas-legales-en-el-salvador-un-gran-retroceso-en-los-derechos-humanos-y-el-estado-democratico/

Derechos Digitales. (2023, septiembre). Derechos humanos en entornos digitales en Nicaragua. Derechos Digitales. https://www.derechosdigitales.org/publicaciones/derechos-humanos-en-entornos-digitales-en-nicaragua/.

Díaz, V. (2022, enero 4). Voto electrónico y consideraciones de política pública en América Latina. Derechos Digitales América Latina. https://www.derechosdigitales.org/wp-content/uploads/VotoElectronico-mapalatino.pdf

Do Alto, H. (2007). El MAS-IPSP boliviano, entre movimiento social y partido político. Análisis Político, 62, 26. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-47052008000100002

DW. (2024, agosto 4). Brasil: Elon Musk exige la renuncia de Alexandre de Moraes. DW. https://www.dw.com/es/brasil-elon-musk-exige-la-renuncia-de-alexandre-de-moraes/a-68763337

ECU-911. (s/f-a). Cámaras de Videovigilancia. ECU-911. Recuperado el 29 de noviembre de 2024, de https://www.ecu911.gob.ec/camaras-de-videovigilancia/

ECU-911. (s/f-b). Localizador Móvil. ECU-911. Recuperado el 29 de noviembre de 2024, de https://www.ecu911.gob.ec/localizador-mobil/

EFE. (2023, diciembre 19). El Gobierno brasileño lanza una aplicación para bloquear teléfonos celulares robados. Swissinfo. https://www.swissinfo.ch/spa/el-gobierno-brasile%C3%B1o-lanza-una-aplicaci%C3%B3n-para-bloquear-tel%C3%A9fonos-celulares-robados/49073140

EFE. (2024a, enero 19). El régimen de Nicaragua ratificó una reforma que despoja de la nacionalidad a los condenados por traición a la patria. Infobae. https://www.infobae.com/america/america-latina/2024/01/20/el-regimen-de-nicaragua-ratifico-una-reforma-que-despoja-de-la-nacionalidad-a-los-condenados-por-traicion-a-la-patria/

EFE. (2024b, octubre 9). Nicaragua despoja de su nacionalidad a 135 exdetenidos que expulsó hacia Guatemala. France24. https://www.france24.com/es/am%C3%A9rica-latina/20240910-o-nicaragua-despoja-de-su-nacionalidad-a-135-presos-pol%C3%ADticos-que-expuls%C3%B3-hacia-guatemala

El Espectador. (2024, octubre 22). El dueño de Pegasus ha lavado activos en Colombia: Presidente Petro. El Espectador.https://www.elespectador.com/politica/pegasus-petro-dijo-que-el-dueno-del-software-gerente-de-nso-group-lavo-activos-en-colombia-vuelos-noticias-hoy/

El Universo. (2023, diciembre 12). Contraloría empieza auditorías a los contratos del Consejo Nacional Electoral para hacer las elecciones presidenciales anticipadas. El Universo. https://www.eluniverso.com/noticias/politica/contraloria-general-del-estado-consejo-nacional-electoral-voto-telematico-contratos-fallas-auditorias-elecciones-presidenciales-2023-nota/

Electronic Frontier Foundation. (2021, junio 28). Carta de la EFF a la Secretaría de Derechos Humanos de la República de Ecuador (caso Ola Bini). Electronic Frontier Foundation. https://www.eff.org/document/carta-de-la-eff-la-secretaria-de-derechos-humanos-de-la-republica-de-ecuador-caso-ola-bini

ESET. (s/f). Ransomware. ESET. Recuperado el 29 de noviembre de 2024, de https://www.eset.com/es/caracteristicas/ransomware/

Espacio Público. (2024a, mayo 20). Operadoras bloquean portal web del medio digital La Gran Aldea. Espacio Público. https://espaciopublico.ong/operadoras-bloquean-portal-web-del-medio-digital-la-gran-aldea/

Espacio Público. (2024b, junio 3). Operadoras de internet bloquean portal informativo El Político. Espacio Público. https://espaciopublico.ong/operadoras-de-internet-bloquean-portal-informativo-el-politico/

Espacio Público. (2024c, septiembre 3). Bloquean portal web del medio Impacto Venezuela. Espacio Público. https://espaciopublico.ong/bloquean-portal-web-del-medio-impacto-venezuela/

Falcão, M. (2024, enero 31). PF vê abuso de poder econômico e manipulação de dados em campanha de Google e Telegram contra PL das Fake News. Globo. https://g1.globo.com/politica/noticia/2024/01/31/pf-ve-abuso-de-poder-economico-e-manipulacao-de-dados-em-campanha-do-google-e-telegram-contra-pl-das-fake-news.ghtml

Fiscalía General del Estado Ecuador. (2024). Caso Metástasis. Fiscalía General del Estado Ecuador. https://www.fiscalia.gob.ec/caso-metastasis/

Folha de Sao Paulo. (2024, noviembre 29). Moraes inclui Musk em inquérito das milícias digitais e abre nova investigação sobre obstrução. Folha de Sao Paulo. https://www1.folha.uol.com.br/poder/2024/04/moraes-inclui-musk-como-investigado-no-inquerito-das-milicias-digitais.shtml

Forbidden Stories. (2021). Pegasus Project. Forbidden Stories. https://forbiddenstories.org/projects_posts/pegasus-project/

Fundamedios. (2024, febrero 21). Indómita recibe un nuevo ataque cibernético, van 300 desde diciembre [Post]. https://www.fundamedios.org.ec/alertas/indomita-recibe-un-nuevo-ataque-cibernetico-van-300-desde-diciembre/

Gavarrete, J., Reyes, D., & Martínez, Ó. (2022, diciembre 1). Veintidós miembros de El Faro fueron intervenidos con Pegasus 226 veces entre 2020 y 2021. El Faro. https://elfaro.net/es/202201/el_salvador/25935/Veintid%C3%B3s-miembros-de-El-Faro-fueron-intervenidos-con-Pegasus-226-veces-entre-2020-y-2021.htm

Global Freedoom Of Expression Columbia University. (2020, mayo 26). El caso de la investigación sobre las noticias falsas en Brasil. Columbia University. https://globalfreedomofexpression.columbia.edu/es/cases/the-case-of-the-brazil-fake-news-inquiry/

Gressier, R. (2024, julio 24). Gigantes de tecnología y prensa dan espaldarazo a la apelación de El Faro en caso Pegasus. El Faro. https://elfaro.net/es/202407/el_salvador/27511/Gigantes-de-tecnolog%C3%ADa-y-prensa-dan-espaldarazo-a-la-apelaci%C3%B3n-de-El-Faro-en-caso-Pegasus.htm

Human Rights Watch. (2024, mayo 22). Ecuador: Abusos luego del anuncio de un ‘conflicto armado’. Human Rights Watch. https://www.hrw.org/es/news/2024/05/22/ecuador-abusos-luego-del-anuncio-de-un-conflicto-armado

Instituto Nacional de Estadística de Bolivia. (2024, marzo 23). Censo Bolivia 2024. Instituto Nacional de Estadística de Bolivia. https://censo.ine.gob.bo/

Instituto Prensa y Sociedad. (2023). Algoritmos del silencio: Reporte anual de Derechos Digitales 2023. Instituto Prensa y Sociedad. https://ipysvenezuela.org/wp-content/uploads/2024/05/IPYS_ReporteDerechosDigitales-2023.pdf

Karisma. (2023, octubre 14). ¿Cortaron o no cortaron el internet durante el Paro Nacional del 2021? Karisma. https://www.instagram.com/karismacol/reel/CyYv1rWOSf6/

Karisma. (2024, julio 6). Proyecto de ley ofrece nuevas formas de censura impuestas por funcionarios públicos mientras desprotege a víctimas de violencia de género. Karisma. https://web.karisma.org.co/proyecto-de-ley-ofrece-nuevas-formas-de-censura-impuestas-por-funcionarios-publicos-mientras-desprotege-a-victimas-de-violencia-de-genero/

Kaspersky. (s/f). Spyware: ¿Qué es y cómo protegerse? Kaspersky. Recuperado el 29 de noviembre de 2024, de https://latam.kaspersky.com/resource-center/threats/spyware?srsltid=AfmBOoqc5IIKjYFs65cr97NVgoZeJoGiZhFn-ovKTzhJlSDlM8IsuU-h

Kitroeff, N., & Bergman, R. (2024, mayo 22). El espionaje en México cobra una nueva víctima: Un aliado del presidente. The New York Times. https://www.nytimes.com/es/2023/05/22/espanol/alejandro-encinas-pegasus-espionaje.html

Knoerr, J. (2024, mayo 22). Investigadores observan un aumento de la desinformación a medida que los conflictos sociopolíticos afectan a las comunidades locales de Bolivia, El Salvador y Perú. LatAm Journalism Review. https://latamjournalismreview.org/es/articles/investigadores-observan-un-aumento-de-la-desinformacion-a-medida-que-los-conflictos-sociopoliticos-afectan-a-las-comunidades-locales-de-bolivia-el-salvador-y-peru/

Kosinski, M. (2024, mayo 17). ¿Qué es el phishing? IBM. https://www.ibm.com/es-es/topics/phishing#:~:text=El%20phishing%20es%20un%20tipo,otro%20modo%20a%20la%20ciberdelincuencia.

La Barra Espaciadora. (2024, octubre 13). Voto telemático y seguridad informática: Lo que nadie tomó en cuenta. La Barra Espaciadora. https://www.labarraespaciadora.com/ciberespacio/voto-telematico-seguridad-informatica/

Maia, P. (2023, agosto 1). A Cautionary Tale: Brazilian democracy, anti-democratic riots, and Meta's platforms. The Influence Industry Project. https://influenceindustry.org/en/explorer/case-studies/brazil-elections-meta-platforms/

Megiddo, G. (2024, mayo 26). $13m Cash on a Private Jet: How Colombia Paid for Israeli Spyware. Haaretz. https://www.haaretz.com/israel-news/2024-03-26/ty-article-magazine/.premium/13m-cash-on-a-private-jet-from-colombia-a-nonissue-for-israeli-head-of-defense-export/0000018e-7689-d706-a39f-f7f93fa10000

Ministerio TIC. (2024). Estrategia Nacional Digital de Colombia 2023 — 2026. Ministerio TIC. https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf

Molina, F. (2023, septiembre 28). Evo Morales y Luis Arce llevan al MAS al divorcio tras una larga pelea. El País. https://elpais.com/internacional/2023-09-28/evo-morales-y-luis-arce-llevan-al-mas-al-divorcio-tras-una-larga-pelea.html

Moreno, C. (2022, septiembre 27). Es tiempo de una ley sobre violencia digital de género. Karisma. https://web.karisma.org.co/es-tiempo-de-una-ley-sobre-violencia-digital-de-genero%EF%BF%BC/

Moreno, C. (2024, mayo 24). Un proyecto para proteger mujeres que protege es a políticos. La Silla Vacía. https://www.lasillavacia.com/red-de-expertos/red-de-las-mujeres/un-proyecto-para-proteger-mujeres-que-protege-es-a-politicos/

Observatorio Ecuatoriano de Crimen Organizado. (2024). Boletín anual de homicidios intencionales en Ecuador: Análisis de las estadísticas finales del año 2023. Observatorio Ecuatoriano de Crimen Organizado. https://oeco.padf.org/boletin-semestral-de-homicidios-intencionales-en-ecuador/

OEA. (2018, diciembre 19). CIDH denuncia agravamiento de la represión y el cierre de espacios democráticos en Nicaragua. OEA. https://www.oas.org/es/cidh/prensa/Comunicados/2018/273.asp

Osorio, M. (2024, septiembre 2). El riesgo constante de ser periodista en México: Un caso de filtración de datos personales. Derechos Digitales. https://www.derechosdigitales.org/23158/el-riesgo-constante-de-ser-periodista-en-mexico-un-caso-de-filtracion-de-datos-personales/

Primicias. (2024, noviembre 29). Caso Villavicencio: ECU-911 confirma el mal uso de la plataforma de rastreo de celulares. Primicias. https://www.primicias.ec/noticias/sucesos/ecu911-rastreo-celulares-caso-villavicencio/

Proceso. (2024, diciembre 1). Caso Pegasus: Absuelven al único acusado por el espionaje a Carmen Aristegui. Proceso. https://www.proceso.com.mx/nacional/2024/1/12/caso-pegasus-absuelven-al-unico-acusado-por-el-espionaje-carmen-aristegui-321992.html

Programa Venezolano de Educación Acción en Derechos Humanos. (2024, abril 4). Venezuela frente al espejo del fascismo: Perspectivas de derechos humanos sobre el proyecto Ley contra el fascismo, neofascismo y expresiones similares. Programa Venezolano de Educación Acción en Derechos Humanos. https://provea.org/actualidad/venezuela-frente-al-espejo-del-fascismo-perspectivas-de-derechos-humanos-sobre-el-proyecto-ley-contra-el-fascismo-neofascismo-y-expresiones-similares-laboratorio-de-paz/

Projeto de Lei n° 2338. (2023). Senado Federal. https://www25.senado.leg.br/web/atividade/materias/-/materia/157233

R3D. (2024a, febrero 27). Ejército de Bots: Las operaciones militares para monitorear las críticas en redes sociales y manipular la conversación digital. R3D. https://r3d.mx/2024/02/27/ejercito-de-bots-las-operaciones-militares-para-monitorear-las-criticas-en-redes-sociales-y-manipular-la-conversacion-digital/

R3D. (2024b, abril 24). Coppel guarda silencio sobre el incidente de ciberseguridad que afectó a sus sistemas. R3D. https://r3d.mx/2024/04/24/coppel-guarda-silencio-sobre-el-incidente-de-ciberseguridad-que-afecto-a-sus-sistemas/

Revista Semana. (2024, mayo 4). FF.MM. reaccionan a actuar de las disidencias al reclutar a menores a través de TikTok: Es una flagrante violación al mismo cese al fuego. Revista Semana. https://www.semana.com/nacion/articulo/ffmm-reaccionan-a-actuar-de-las-disidencias-al-reclutar-a-menores-a-traves-de-tiktok-es-una-flagrante-violacion-al-mismo-cese-al-fuego/202446/

Reyes, E. (2024, agosto 21). Ley de Ciberseguridad en México; una propuesta sin sustento técnico. Expansión. https://expansion.mx/tecnologia/2024/08/21/es-posible-una-ley-de-ciberseguridad-en-mexico

Rodríguez, M. (2024, enero 29). Salud Total EPS denunció ser víctima de ataque cibernético: Confirmó a sus usuarios si sus servicios se vieron afectados. Infobae. https://www.infobae.com/colombia/2024/01/30/salud-total-denuncio-ser-victima-de-ataque-cibernetico-eps-confirmo-a-sus-usuarios-si-sus-servicios-se-vieron-afectados/

Romero, M. (2021, julio 20). México: El Gobierno de Peña Nieto investigó a 15.000 personas con Pegasus. France24. https://www.france24.com/es/am%C3%A9rica-latina/20210720-pegasus-espionaje-mexico-pena-nieto

RSF. (2024a). Clasificación mundial de la libertad de prensa 2024: El periodismo, bajo las presiones políticas. RSF. https://rsf.org/es/clasificaci%C3%B3n-mundial-de-la-libertad-de-prensa-2024-el-periodismo-bajo-las-presiones-pol%C3%ADticas#:~:text=En%20la%20regi%C3%B3n%20Asia-Pac%C3%ADfico,)%20y%20Afganist%C3%A1n%20(178%C2%BA)

RSF. (2024b). El Salvador. RSF. https://rsf.org/en/country/el-salvador

Sadi, A. (2024, enero 25). Espionagem ilegal da Abin atingiu 30 mil pessoas e dados foram guardados em Israel, diz chefe da PF. Globo. https://g1.globo.com/politica/blog/andreia-sadi/post/2024/01/25/espionagem-ilegal-da-abin-atingiu-30-mil-pessoas-e-dados-foram-guardados-dados-em-israel-diz-chefe-da-pf.ghtml

Taraciuk, T. (2022, febrero 24). En El Salvador, leyes amplias sobre delitos informáticos amenazan derechos fundamentales. Human Rights Watch. https://www.hrw.org/es/news/2022/02/24/en-el-salvador-leyes-amplias-sobre-delitos-informaticos-amenazan-derechos

Tarazona, D. (2024, junio 6). Violencia en Latinoamérica: El 80% de los asesinatos contra defensores de derechos humanos ocurrió en la región. Mongabay. https://es.mongabay.com/2024/06/violencia-latinoamerica-asesinatos-contra-defensores-informe/

The Carter Center. (2024, julio 30). Declaración del Centro Carter Sobre la Elección en Venezuela. The Carter Center. https://www.cartercenter.org/news/pr/2024/venezuela-073024-spanish.pdf

VE sin Filtro. (2023). Reporte sobre la situación de los derechos humanos digitales en Venezuela. VE sin Filtro. https://vesinfiltro.com/res/files/reporte-2022-2023.pdf

@vesinfiltro. (2024, febrero 2). X [Post]. X. https://x.com/vesinfiltro/status/1753542563280093687

X. (2024). [Software]. https://x.com/search?q="defensores" AND "delincuentes" until%3A2024-01-15 since%3A2024-01-09&src=typed_query&f=live

Xinhua Español. (2024, noviembre 21). Constelación de satélites comerciales de China proporcionará servicios de internet a Brasil. Xinhua Español. https://spanish.news.cn/20241121/bb9137066179416283f657a00b868259/c.html

Yuhas, A. (2023, febrero 17). Seré nicaragüense hasta el día que me muera: El gobierno de Ortega retira la ciudadanía a cientos de personas. The New York Times. https://www.nytimes.com/es/2023/02/17/espanol/nicaragua-quita-ciudadania-disidentes.html

derechosdigitales.org