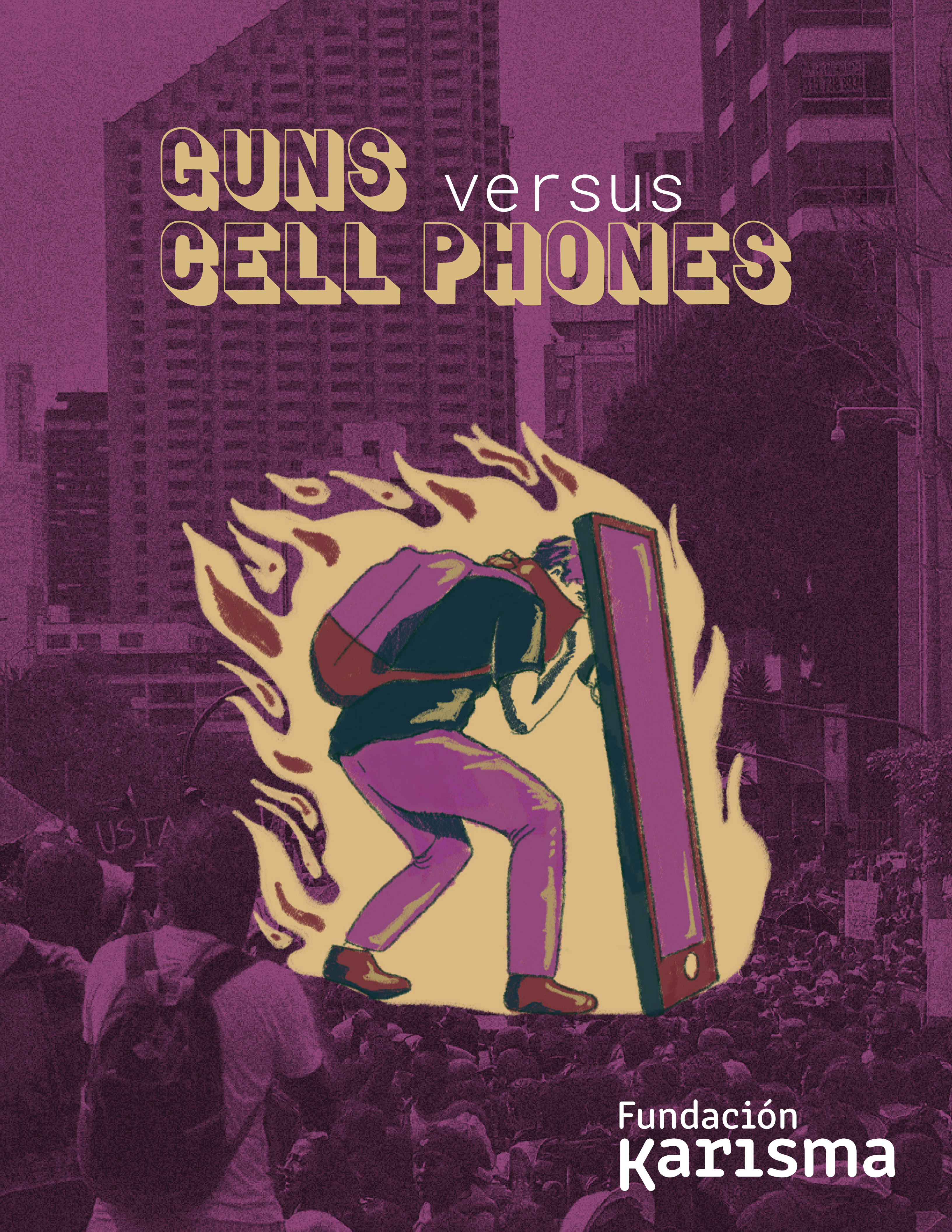
GUNS versus CELL PHONES



Fundación Karisma

GUNS versus CELL PHONES

Bogotá, Colombia
September 2021

Written by:
Juan Pablo Parra
Carolina Botero

Reviewed:
Pilar Saenz
Andrés Velásquez
Juan Diego Castañeda
Joan López
Lucia Camacho

Editorial design:
Hugo A. Vásquez

Illustration:
Don Repollo

In an effort so that all people have access to knowledge, Fundación Karisma is working to make its documents accessible. This means that its format includes metadata and other elements that make it compatible with tools such as screen readers. The purpose of accessible design is that all people, including those with some kind of disability or difficulty with reading and comprehension, can access the content. More information on the subject at http://www.documentoaccesible.com/#que-es

Fundación Karisma

CONTENTS

INTRODUCTION

On April 28, 2021, after President Iván Duque submitted the Tax Reform bill before the Congress of the Republic, a massive citizen protest movement—known as the National Strike—took off in Colombia. From then until June 15, marches and activities were officially called in different cities throughout the country.

Amid this panorama of social and democratic unrest, the rallies and marches were scenes of confrontations between protesters and law enforcement (note that the Police are a national organization part of the armed forces), including armed civilians supporting the Police. Simultaneously, on some social networks such as Facebook, Instagram, Twitter, and Tik Tok, people began to post claims and videos about alleged human rights violations against demonstrators. Publications documenting the excessive use of force by law enforcement against demonstrators or the attacks by citizens on law enforcement and local infrastructure went viral.

With the increase in the intensity of the confrontations in the streets and the people marching with their cell phones in their hands, as a mechanism to denounce and defend against abuses, reports also emerged about possible actions by State representatives that disproportionately limited fundamental rights exercised by citizens through technology, such as freedom of expression, access to information, assembly, and the right to privacy.

The lack of clear information about what happens to rights in the digital environment amid the protest; the absence of investigations by Colombian authorities, and the proliferation of cases in which publications or accounts were blocked, disappeared, or diminished their scope, generated a feeling of general censorship by the State against citizens and questions about the role of Internet service providers and internet intermediaries in the events. In this report, we will analyze the impact that the Colombian digital space suffered from the cases of possible violations of human rights exercised in digital spaces by citizens and that were collected by the Karisma Foundation during the first month of the strike, between April 28 and May 28, 2021.

Some of the risks that we explain here were reported, together with other civil society organizations, to the Inter-American Commission on Human Rights (IACHR) before its working visit to Colombia to consider them in its document of recommendations to the national government[1]. Said letter of observations and recommendations was published the first week of July and included a chapter dedicated to the Internet as a space for protest[2]. There, the IACHR drew the State's attention to issues such as cyber-patrolling by law enforcement, interruptions to internet service, orders to block I.P. addresses and included recommendations to adapt or limit said activities to the inter-American framework[3].

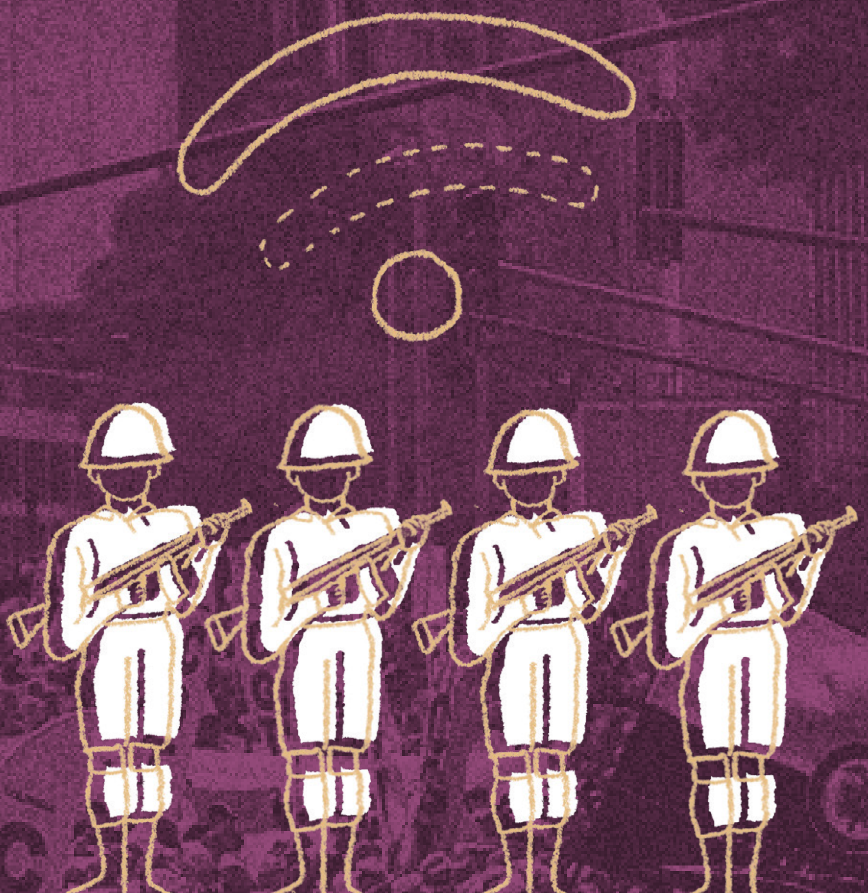
For greater clarity, this report is organized as follows: first, it will address the cases in which the State is accused of having interfered with the Internet through blockages or alleged cuts; then, the risks for citizens generated by campaigns to criminalize digital protest and fake news reports carried out by the Ministry of Defense will be explained; in a third stage, the use of technologies to control social protest and searches of cell phones will be discussed; to close, we will make brief comments on the role played by private online intermediaries during the strike and; finally, some conclusions and recommendations will be presented.

[1] Fundación Karisma. Pedimos incorporar y analizar las violencias digitales en la protesta durante su visita [We asked that digital violence in the protest during their visit be incorporated and analyzed] Available at: https://web.karisma.org.co/una-peticion-para-incorporar-y-analizar-las-violencias-digitales-en-la-protesta/

[2] Karisma Foundation official Twitter account. Thread from July 7, 2021: https://twitter.com/Karisma/status/1412839454595760130

[3] IACHR. IACHR Completes Working Visit to Colombia and Issues its Observations and Recommendations. Available at: https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/167.asp

ONE.
THE STATE MESSES WITH THE INTERNET: SELECTIVE SHUTDOWNS AND BLOCKAGES DURING THE NATIONAL STRIKE



Uno de los principales temores de la ciudadanía respecto de los derechos digitales durante el paro One of the main fears of citizens regarding digital rights during the national strike was the possibility that the State interfered with the Internet to limit protest messages or as a mechanism to prevent reporting on alleged abuses by law enforcement in the streets. This fear of censorship became apparent with the avalanche of publications on social networks that denounced internet cuts during the strike. Nevertheless, the problem goes further since, normatively, several state entities have powers to interfere with the Internet, without it being clear whether they have used those powers or who exercises control over them in this regard.

This chapter will address the cases in which the State messed with the Internet during the national strike. Specifically, we will refer to the alleged internet cuts in Cali, the discretionary powers of the security agencies to use devices that jam the cell phone signal, and the orders given by the Superintendency of Industry and Commerce to block some specific I.P. addresses. In sum, we will analyze how the Colombian State has installed technological capacity to restrict internet access or block online content and if the applicable legal framework establishes an institutional design that offers guarantees of human rights and/or avoids abuses by the authorities.

1.1 Initial clarifications. Internet cuts a complex issue

Before addressing the specific cases, it is necessary to make some clarifications. First, there has not been an internet blackout or shutdown in Colombia, neither before nor during the national strike. That is to say, there has not been a service delivery shutdown on State orders, as is the case of Myanmar[4] or Venezuela in the 2013 elections[5] —or at least there is no proof of it. However, since the strike began, citizen reports of internet outages have been constant.

These complaints are not minor issues. During the 2021 demonstrations, it became common for citizens to turn to the internet en masse to express their discontent and document live, or rebroadcasting, what was happening in the streets, especially irregularities related to law enforcement. This active use of the Internet and social networks to exercise rights of the scope of freedom of expression, access to information, and political participation, makes citizen reports of possible internet blockages of particular concern. State interference in internet service provision threatens the fundamental core of the rights mentioned above since it completely prevents citizens from expressing, participating, or informing themselves about the national context and obstructs denouncing or documenting

The importance of the Internet to exercise and enjoy human rights leads us to the second clarification: Colombia, as a State Party to the American Convention on Human Rights, is obliged to protect the Internet and is prohibited from blocking or turning it off. In this regard, the rapporteurs on freedom of expression from different international human rights organizations, including the Organization of American States (OAS) and the United Nations (U.N.), indicated in 2011 that: "Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds."[6] .

[4] Myanmar: End World's Longest Internet Shutdown, article available at: https://www.hrw.org/news/2020/06/19/myanmar-end-worlds-longest-internet-shutdown

[5] Venezuela: Internet blocked for "three minutes" on Election Day. Read more at: https://advox.globalvoices.org/2013/04/15/venezuela-internet-blocked-for-three-minutes-on-election-da/

[6] The Joint Declaration on Freedom of Expression and the Internet, 2011, can be found at https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849

Moreover, in the same vein, the Inter-American Commission on Human Rights (IACHR) ruled when referring to internet cuts in times of protest and pointing out that "limitations on internet access, including total or partial disconnections, internet throttling, temporary or permanent blockages of different sites and applications before, during, or after peaceful meetings constitute illegitimate restrictions on the rights of association and assembly."[7]

The third factor that must be taken into account in the Colombian case is the weak infrastructure that the country has to provide public services such as the Internet or electricity. According to data from September 2020, Colombia is one of the countries with the worst access to the web[8], with only 24.3 million reported internet accesses for more than 50 million people. In addition, there are different levels of access and quality of service, depending on the region, with the excluded areas being those with the most deficient services.[9] Something similar happens with electricity delivery since at least 1,710 towns in Colombia are still lit with candles[10]. Furthermore, although this outlook is not so drastic in cities, there are indeed populations and marginalized areas where access is lower in quality.

When we talk about internet outages or interruptions, we must not only account for possibly illegal actions by the State but also lack of access to quality connectivity, mass events that overload the network (such as marches or concerts), physical damage to infrastructure, maintenance of the service provider network, power outages, and platform or application-level issues. All these are factors that plausibly explain the failures in service delivery. Therefore, establishing the origin and nature of the interference is central to guaranteeing people's rights. The socio-political context or technical complexities do not justify interruptions to internet service, nor do they exempt the State from forcing an investigation and clarification of what happened.

1.2 Selective and illegal interruptions and cuts of the Internet. Cali, a night without Internet and with law enforcement in the streets

The first notorious and relevant case about internet outages in the country was that of Cali during the afternoon and night of May 4, 2021 (approximately from 4:30 pm) until the early morning of the next day. Problems with the internet service that Netblocks, an English organization dedicated to monitoring the Internet, confirmed in its statement *Internet disrupted in Colombia amid anti-government protests*[11] May 5. This denunciation had particular national relevance due to the strong military presence that engulfed the city and the brutality of the confrontations. Police violence allegedly left three young men shot dead

[7] Office of the Special Rapporteur for Freedom of Expression. Inter-American Commission on Human Rights. Protest and Human Rights: Standards on the rights involved in social protest and the obligations that should guide the state response. Paragraph 298. Available at https://www.oas.org/en/iachr/expression/publications/Protesta/ProtestHumanRights.pdf

[8] El Tiempo. Colombia, uno de los países con más dificultades en acceso a internet. Available at; https://www.eltiempo.com/tecnosfera/novedades-tecnologia/internet-calidad-de-conexion-en-colombia-con-mas-dificultades-en-el-mundo-529850#:~:text=Seg%C3 % Bn% 20the% 20Ministry% 20of% 20las, and% 20no% 20 have% 20this% 20benefit and MinTIC. ¿Cómo está el país en conexión de internet? [How is the country with internet connection?] Available at: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/MinTIC-en-los-medios/151654:Como-esta-el-pais-en-conexiones-de-internet

[9] MinTIC. Quarterly newsletter of the ICT sector - Figures fourth quarter of 2020. Available at: https://colombiatic.mintic.gov.co/679/w3-article-172261.html

[10] El Tiempo. The 1710 villages that are still lit with candles in the country. Available at: https://www.eltiempo.com/colombia/otras-ciudades/los-poblados-que-aun-no-tienen-energia-electrica-en-colombia-324980

[11] Network. Internet disrupted in Colombia amid anti-government protests. Accessed at: https://netblocks.org/reports/internet-disrupted-in-colombia-amid-anti-government-protests-YAEvMvB3

on the night of May 4 in the Siloé district, where internet outages were also reported.

From the start of the protests, on April 28, until the Internet outages complaints, Cali had been the epicenter of the national strike. In this, the country's third most important city, there were intense clashes between citizens and the Police, with complaints in social networks and the national press about deaths and fires in the city, especially in the districts of Agua Blanca and Siloé.[12] Given this scenario, a curfew was decreed from April 28 to May 2[13] , and the arrival of more soldiers to the city was announced[14].

In this context of high military presence and violence, the complaints of internet outages in Cali came to the fore between May 4 and 5. The first reports of problems were given through Twitter, noting that live broadcasts of the marches and the clashes were failing, people's data plans were not working correctly, and it was challenging to connect to social networks.[15],[16]

Some of the citizen complaints reported that there were also power cuts in Siloé. In addition, some witnesses point out that the internet outages or blockages prevented uploading content to networks or even accessing it in any way. "Let's say that right now it has calmed down because there is already a national and international outlook, but when it just started, it seemed that the entire network was lost. Siloé was off one day for five hours, five hours in which nothing entered or left. I mean, I was on a walkie-talkie with the human rights people, and we didn't know if they were alive or dead—there was simply no signal—I saw the mobile unit with big equipment with an antenna, I don't have a photo. Much of what I shared was timeless because there was no signal there," says Jahfrann, a Colombian freelance photographer in an unpublished testimony collected by the Foundation for Press Freedom (FLIP).

This type of problem due to alleged cuts to telecommunications was also experienced by members of Red Alterna Popayán, an alternative media outlet that covered the strike in another city, Popayán. In an unpublished interview conducted by FLIP, they stated that: "Here in the camp there was no signal, not even radio. For example, some colleagues were broadcasting, and we had to record because it didn't work, [the live broadcasts]

[12] El Tiempo. A siete sube cifra de muertos en el paro en Cali: https://www.eltiempo.com/colombia/cali/cali-tuvo-una-noche-de-terror-tras-orden-de-militarizacion-de-duque-592136

[13] Infobae Ministry of Defense confirmed the militarization in Cali: 450 soldiers arrive. Accessed at: https://www.infobae.com/america/colombia/2021/04/28/ministerio-de-defensa-confirmo-la-militarizacion-en-cali-llegan-450-soldados/

[14] Office of the Governor of Valle del Cauca. Extraordinary Security Council confirms the arrival of more Esmad and Army personnel to the department. Accessed at: https://www.valledelcauca.gov.co/publicaciones/70630/consejo-extraordinario-de-seguridad-confirma-la-llegada-de-mas-personal-del-esmad-y-el-ejercito-al-departamento/ and El Tiempo. Paro Nacional Cali: Toque de queda. Accessed at: https://www.eltiempo.com/colombia/cali/paro-nacional-cali-toque-de-queda-y-militarizacion-por-desordenes-584340

[15] Blue Radio. ¿Qué pasó con el internet en Cali durante las protestas del pasado martes?. Accessed at: https://www.bluradio.com/blu360/pacifico/que-paso-con-el-internet-en-cali-durante-las-protestas-del-pasado-martes

[16] Denunciations on Twitter about the night of the 4th and morning of the 5th of May:
https://twitter.com/DefenderLiberta/status/1392601992292405251?s=20,
https://twitter.com/julioclondono/status/1389941025775439876?s=20,
https://twitter.com/Mariaisa1990/status/1389841875830546434?s=20,
https://twitter.com/chef_alv/status/1389856559874912257?s=20,
https://twitter.com/MarceHolguinh/status/1389912481401868291?s=20
https://twitter.com/MULATACARAMELO1/status/1389826205294202880?s=20
https://twitter.com/juanmiguel94/status/1390498845839212544?s=20
https://twitter.com/juansitx/status/1389826124843266048?s=20
https://twitter.com/cranvodk/status/1389810050370318337?s=20
https://twitter.com/diegop4z/status/1390066216866357248?s=20
https://twitter.com/male_juri/status/1389814647868506113?s=20
https://twitter.com/JENNJGP/status/1389941927106260996?s=20

would drop off very easily. From what I have fixed, we have been able to work through VPN. Because in the beginning, it was an attack—more than anything—directed at the connection addresses. Nevertheless, when Minister Molano arrived to accompany, there was no signal or total [sic] way to connect to VPN. Mainly, when confrontations get louder is when poof!: the connection disappears".

The uproar over the possible outage materialized when on May 5, Netblocks claimed there were internet access problems and said it was the second incident during the national strike. According to the data published by the English observatory, two disruptions decreased connectivity by up to 25% in Cali.

The Netblocks report does not allow knowing the origin or nature of the interruptions it documented[17], and it should be taken as one more piece of information to inform us about possible internet interference. That said, concerning internet interruptions in the case of Cali, the report coincided with significant noise on social networks about possible internet interruptions in sectors of the city. Furthermore, Netblocks reported service provider issues with Colombia Telecomunicaciones S.A., better known as Movistar, who also said it had connectivity issues on the fixed internet network in Aguablanca district's early hours of May 5. The provider indicated that this was due to the theft of a fiber optic cable and problems reconnecting to service due to the public order situation. Movistar did not refer to the service failures in the Siloé sector or the problems with mobile devices reported on Twitter. For its part, Emcali, the other company mentioned in the Netblocks report on service interruptions as a benchmark for comparison with Movistar, indicated that it had provided the service as usual and that no type of voluntary service interruption had been carried out,[18] just as the NetBlocks report had said at the time.

In this regard, in an interview with the newspaper El Espectador, Sergio Martínez, director of the Communications Regulation Commission (CRC) - the highest authority on internet issues in Colombia - pointed out that the only report they had received on May 4 was for damages to the infrastructure. Moreover, he added that "at no time are we going to endorse or order or indicate that the internet should be blocked or closed [...] by the CRC, we are never going to issue a mandate of this type because that threatens freedom and democracy in Colombia"[19].

The Ministry of Information Technologies and Communications (known as MinTIC in Colombia), for its part, merely produced a report with companies' statements noting without proof that the damage was caused not by theft but "vandalism"; that this could not be repaired because of the demonstrations. Statements hinting dropping the neutral language used by private companies to speak about the events and pointing at protesters veiledly.

To date, it is still not known with certainty what happened in Cali between May 4 and 5. The State's explanations about the internet outages in Cali are insufficient, if not null. Furthermore, although well-intentioned, the statements of the service providers do not allow us to establish what happened either. For example, although

[17] There are questions about the methodology and data of the reports that Netblocks makes, since in different cases its reports on internet drop offs or outages have been refuted and considered unreliable. This problem has been aggravated by Netblocks refusal to be more transparent with the information and methodology it uses. This problem has been described in articles like *How the internet censorship world turned on NetBlocks* in Wired (Accessed at: https://www.wired.co.uk/article/netblocks-internet-shutdow). In any case, the questions to Netblocks reveal that the lack of reliable information on internet outages is a problem in itself.

[18] Emcali. We report normality in the fixed telephony service, internet, mobile telephony throughout the city. Accessed at: https://twitter.com/search?lang=es&q=(from%3AEMCALIoficial)%20until%3A2021-05-06%20since%3A2021-05-04&src=typed_query

[19] El Espectador. ¿Por qué se cayó internet en algunas partes de Cali durante el 4 de mayo?. Accessed at: https://www.elespectador.com/tecnologia/por-que-se-cayo-internet-en-algunas-partes-de-cali-durante-el-4-de-mayo/

the Netblocks report does not allow determining in which areas of Cali the interference to the internet service occurred, from the complaints in networks and media, it is clear that the epicenter was Silóe, primarily affecting mobile phone connections. Movistar's response, this being the case, is reasonable to understand the problem detected in the Netblocks report concerning the city of Cali, but it is insufficient to explain the problems with internet access from landlines and mobiles that occurred in Siloé.

In addition, it should not be forgotten that both in Cali, as in Barranquilla, in the municipality of Caldas (Antioquia), and the Portal of the Americas in Bogotá, internet cuts were also reported, and there was talk of simultaneous power cuts when the Demonstrations turned violent due to clashes with the Police. As with the Internet, power failures could be explained by infrastructure problems. The truth, however, is that there is no information to support the story about infrastructure problems located in places of protest, nor is there evidence of intentional cuts as having occurred, for example, in Venezuela[20]. This lack of information, the result of state opacity and the lack of transparency of the private parties involved, sets the trend regarding possible violations of rights in the digital environment during demonstrations. Subject to which, from now on, we draw attention.

Contrary to what happens in Colombia, the availability of information regarding internet or energy interruptions should be such as to allow public scrutiny on all aspects of connectivity involved. For example, this last was the case in Washington in June 2020 amid protests against President Donald Trump. In that case, thanks to a large amount of information available about what happened, the complaints about possible internet interruptions were refuted by journalists from the Reuters agency who managed to reconstruct what happened during the protests.[21]

In any case, as we explained in the previous section, it is the responsibility of the Colombian State, as a result of its international obligations to protect human rights in the digital environment, to carry out investigations to determine causes and those responsible for the internet outages that occurred in Cali. However, this has not been the case, and the State has refused to give answers or even to seek them, partly because of its institutional design, as we will explain later. This political and institutional phenomenon has left in the environment a feeling of censorship and doubts about whether law enforcement, which was present in the areas where Internet access problems were reported, is using devices that they have in their power to block the signal.[22]

1.3 Censorship at discretion. Law enforcement signal jammers

One of the factors generating more questions about events in Cali between May 4 and 5 is the military and Police's strong presence in the city and their possible interference in providing the internet service. It should be noted, to begin with, that there is no evidence that the army or the Police used devices to interrupt the signal during the national strike. However, it is a fact that security agencies are equipped with and regularly use these devices to block the signal. An example of this is the telecommunications blocking mechanisms used in prisons,[23] or the six "frequency inhibitors" purchased by the Directorate of Criminal Investigation and Interpol

[20] Derechos Digitales. Políticas Públicas de Acceso a Internet en Venezuela. Accessed at: https://www.derechosdigitales.org/wp-content/uploads/CPI_venezuela.pdf

[21] Reuters. Fact check: Washington, D.C. did not have a city-wide blackout at 1 am on June 1, 2020. Available at: https://www.reuters.com/article/uk-factcheck-dc-blackout-protests/factcheckwashington-dcdid-not-have-a-city-wide-blackoutat-1-amon-june-1-2020-idUSKBN2383OK

[22] El País. La interrupción de internet durante las protestas enardece a los manifestantes en Colombia. Accessed at: https://elpais.com/internacional/2021-05-06/la-interrupcion-de-internet-durante-las-protestas-agita-a-los-manifestantes-en-colombia.html

[23] Caracol Radio. Por demandas y multas apagamos bloqueadores de señal: Inpec. Accessed at: https://caracol.com.co/radio/2019/09/12/judicial/1568304853_201434.html and W Radio. Extorsiones carcelarias: ¿Están de adorno los bloqueadores de señal de celulares?. Accessed at: https://www.wradio.com.

(DIJIN) in 2016 from Robotec Colombia SAS and classified as military and intelligence equipment.[24]

In addition, law enforcement is legally empowered to employ signal-blocking devices, and most worryingly, to do so without control over their actions. This power was granted through Resolution 2774 of 2013[25] of the MinTIC. Regulation in which law enforcement is authorized to acquire and use jammers, blockers, and radio signal amplifiers for "reasons of security and general interest." The only requirements are to internally justify the use of the inhibitor and provide technical studies about it.

The situation became even more worrisome in 2018 when the MinTIC changed its original regulation through Resolution 1823[26] and established that there are "special authorizations" that empower "state security agencies" to install jammers in open sites in cases "related to public security," without the need for authorization from the MinTIC or judicial control.

There are several concerns in regard with this unchecked and discretionary power of law enforcement to use jammers and blockers. Firstly, because it involves the use of technologies that prevent access to the Internet, it implies a disproportionate restriction on rights such as freedom of expression and information, it is not included in a law and will never pass a legality, necessity, and proportionality test of the American Convention. As the IACHR's Office of the Special Rapporteur for Freedom of Expression has pointed out, it is not enough to make abstract references to national security to restrict rights[27].

Secondly, as Resolution 1823 of 2018 states, special permits to use signal or Internet blocking technology are exempt from oversight mechanisms. However, due to the authorization´s scope, it should only have been delivered through judicial authority, and despite the fact that the rest of the powers regulated by the resolution require prior permission from the MinTIC. Finally, the generic justification of "national security," which we reiterate has previously been classified as insufficient by the IACHR, increases opacity, since it makes it difficult to access information that confirms the use of these devices, probably when consulting the Ministry of Defense or law enforcement would refuse to release the information with this excuse.

It is also worrisome that there is no technical, state entity independent of the executive that exercises control over interference with the Internet. The Commission for Communications Regulation [Comisión de Regulación de Comunicaciones] (CRC), an entity created in 2019 to act as a convergent regulator, lacks the capacity to protect citizens from interference with their right of access to electronic communications, as it does not have oversight and sanction powers in Internet matters, functions that are at the head of the MinTIC. By legal design, it should be the CRC, the body that has the knowledge and technical capabilities to process data and investigate internet service providers, and even the actions of other State entities, but this is not the case. In addition, the CRC should also protect and inform users of telecommunications services about the origin and nature of internet outages and punish whoever is responsible, but, again, in practice, it does not have any of these powers.

co/noticias/actualidad/extorsiones-carcelarias-estan-de-adorno-los-bloqueadores-de-senal-de-celulares/20210212/nota/4109297.aspx

[24] National Police, Ministry of National Defense. Sale contract PN DIJIN No. 03-2-1005018. Approved on July 5, 2016.

[25] MinTIC. Resolution 2774 of 2013. Accessed at: https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_2774_2013.htm

[26] MinTIC. Resolution 1823 of 2018. Accessed at: https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_1823_2018.htm

[27] Office of the Special Rapporteur for Freedom of Expression. Freedom of Expression and the Internet. Paragraph 157.Available at: http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf

On the other hand, the National Spectrum Agency (ANE), the technical body that supports the MinTIC in its functions of surveillance and control of the electromagnetic spectrum, is called upon to investigate interference with cell phone signals, a matter under its control. However, it has not done so and, if it does, its affiliation to the MinTIC does not offer the confidence and sufficient independence to monitor the government of which it is a part.

Thus, the current legal design has left the surveillance and sanction of the sector and not only the definition of public policy, in the hands of the MinTIC—an executive branch entity. Thus, the Colombian government ends up watching over something for which it should be accountable. Its work, in effect, has been limited to giving reassuring reports regarding the provision of internet service by private companies, using language that disqualifies the protesters, despite the persistence of complaints on social networks that show other types of threats. It merits noting how in similar situations, regulators in Thailand[28] or United States[29] have carried out investigations given their autonomous powers and being in charge of protecting the rights of those who use telecommunications services.

The lack of an institutional framework that guarantees internet access rights and investigates interference with these rights, added to questions about law enforcement's use of its powers to inhibit signals and its repeated presence in areas where there have been blockages and interruptions, leaves a feeling in the air of a lack of protection and guarantees for human rights in digital environments amid the national strike. Faced with this situation, many civil organizations have asked the State to comply with its international obligations to investigate, punish and guarantee the non-repetition of human rights violations, such as blocking the Internet.[30] Just like mechanisms for periodic, technical, and independent information are created to allow public scrutiny of the health of infrastructure in Colombia, as recommended by the IACHR in its Observations and Recommendations document. However, so far, they have been ignored.

1.4 Net neutrality at risk. An unbalanced internet

The Colombian State has recognized the principle of net neutrality[31] through the law[32] and in its internal regulations[33]. According to this principle, which is one of the foundations of the Internet as we know it today, "[t]he treatment of data and Internet traffic should not be subject to any discrimination based on factors such as devices, content, author, origin and/or destination of the material, service or application."[34] Moreover, according to

[28] Khaosod English. Cop admits signal jammers were deployed at protest. Accessed at: https://www.khaosodenglish.com/news/crimecourtscalamity/2020/08/24/cop-admits-signal-jammers-were-deployed-at-protest/

[29] CBSN. FCC Investigates BART Cell Service Shutdown. Accessed at: https://sanfrancisco.cbslocal.com/2011/08/16/fcc-investigates-bart-cell-service-shutdown/ and Wetmachine. Are Police Jamming Cell Phones At Standing Rock Protest? The FCC Should Investigate. Accessed at: https://wetmachine.com/tales-of-the-sausage-factory/are-police-jamming-cell-phones-at-standing-rock-protest-the-fcc-should-investigate/

[30] UN Human Rights Committee, General Comment No. 37 (2020), on the right to peaceful assembly (Article 21) *. Accessed at: https://www.hchr.org.co/files/observacion-general-37.pdf

[31] Fundación Karisma. ¿Qué es la neutralidad de la red? Accessed at: https://web.karisma.org.co/que-es-la-neutralidad-de-la-red/

[32] Law 1450 of 2011, article 56.

[33] Communications Regulation Commission, article 3 of Resolution 3502 of 2011: "By which the conditions relating to Internet neutrality are established, in compliance with the provisions of article 56 of Law 1450 of 2011." Available on the internet at: https://www.crcom.gov.co/resoluciones/00003502.pdf

[34] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information. 1 June 2011, Declaration on Freedom of Expression and the Internet, http://www.oas.org/en/iachr/expression/showarticle.asp?artID=849&lID=1. Point 5 (a).

IACHR[35] and Constitutional Court[36] interpretations, the States, parties to the American Convention, are obliged to protect the network's neutrality since its basic idea is directly linked to the rights to freedom of expression and information access, pillars of democratic societies.

Thus, in Colombia, service providers, as well as the State, are obliged to refrain from using their power to discriminate, restrict, block or interfere "in the transmission of Internet traffic, unless it is strictly necessary and proportional, to preserve the integrity and security of the network; to prevent the transmission of unwanted content at the express request—free and not incentivized—by the user; and, to temporarily and exceptionally manage network congestion."[37] For all these cases, the inter-American parameters on freedom of expression and access to information are applied, the exception to the rule being that regulated in Law 1336 of 2009, according to which the MinTIC can block pages with content related to sexual abuse of minors (so-called child pornography) or, more recently, to prevent illegal online gambling.

According to the IACHR, the "mandatory blocking or suspension of entire or generalized websites, platforms, conduits, I.P. addresses, domain name extensions, ports, network protocols or any application, as well as measures aimed at eliminating links (links), data and websites of the server where they are hosted," constitute a restriction that is only admissible for openly illegal speeches and not protected by the right to freedom of expression per Article 13 of the American Convention.[38]

The Colombian State faced the National Strike under this regulatory framework. On May 4, 2021, Anonymous allegedly published the name, identity document number, and email address of a few members of law enforcement and other government officials after they attacked the army's official website at dawn on the same day in response to the murders that had occurred in the course of the protests and in which the military and Police were supposedly involved.[39]

To counter the action of Anonymous, the Vice Minister of Connectivity of the MinTIC sent on May 21 to internet providers in Colombia an order to block two specific URLs in the application of a resolution of the Superintendency of Industry and Commerce (SIC).[40] The statement by which MinTIC notified the decision did not include a copy of the SIC resolution.

The legitimacy of the decision can be disputed, but from its context, it is undeniable that it was disproportionate, and there may have been some irregularities. The SIC resolution, to begin with, is not public, which prevents qualifying the legality, proportionality, and necessity of the administrative act.[41] At the time of the events, the

[35] Office of the Special Rapporteur for Freedom of Expression IACHR. Freedom of Expression and the Internet. Paragraph 25. Available at: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

[36] Constitutional Court. Judgment T-179 of 2019.Available at: https://www.corteconstitucional.gov.co/relatoria/2019/T-179-19.htm and Judgment SU-420 of 2019.Available at: https://www.corteconstitucional.gov.co/relatoria/2019/SU420-19.htm

[37] Office of the Special Rapporteur for Freedom of Expression IACHR. Freedom of Expression and the Internet. Paragraph 30. Available at: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

[38] Office of the Special Rapporteur for Freedom of Expression. Inter-American Commission on Human Rights. Protest and Human Rights. Paragraph 157. Available at: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

[39] Publimetro. Anonymous publica números de tarjetas de crédito de altos mandos militares colombianos. Accessed at: https://www.publimetro.co/co/noticias/2021/05/04/anonymous-publica-numeros-de-tardamientos-de-credito-de-altos-mandos-militares-colombianos.html

[40] Fundación Karisma. Tweet from May 21, 2021: https://twitter.com/Karisma/status/1412839454595760130

[41] Letter from Karisma, El veinte, the FLIP and ISUR to the Inter-American Commission. We asked that digital violence in the protest during their visit be incorporated and analyzed. Accessed at: https://

last decision published on the entity's page was from April 2021 and did not correspond to the blocking order.[42] On the other hand, according to what Karisma was informed, the resolution that contains the order was not made available in a timely fashion to the Internet service providers when it was made known to them through the notice from the Vice Minister of ICT. In other words, neither the service providers could assess the legality, necessity, and proportionality of the measure or whether it had been issued as required by law. Nor were they allowed to defend themselves efficiently against it.

We are then talking about a decision limiting fundamental rights of a confidential nature, which goes against the legal system and violates fundamental rights such as defense, due process, and access to information. Whether the SIC exercised its administrative or judicial powers, it should have applied the principle of publicity or contradiction, as the case may be.

The second problem is that based on what is known about the resolution[43] and assuming that the reason for "monitoring the measure" is the technical knowledge of the MinTIC, it seems that the Vice Minister of Connectivity, who signed the communication delivered to the internet providers, does not know how the web works. It is impossible to comply with the order to block a specific URL within the archive.org or ghostbin.co domain without completely blocking those websites. In other words, neither the SIC nor MinTIC considered that this order would block all the websites' content, regardless of whether what was hosted on the two web pages was related to the resolution's content. This last fact is even more severe considering that archive.org also hosts evidentiary content amid social protests.

The director of the Karisma Foundation, Carolina Botero, explained it like this: "When we access a page on the Internet or when an application tries to connect with its servers that use the HTTPS protocol, Internet providers can only know to which domain or I.P. (for example archive.org) we are connecting, from then on the connection is encrypted, the company cannot see what resource or path within the server is being accessed. For this reason, an order to block a specific URL would have to be addressed not to the Internet provider but to whoever manages the page in question (for example, archive.org). If the internet service provider tries to comply with the order, what it will do is block the entire site and therefore prevent access to all its resources."[44]

The third problem is that the order—clearly excessive since it blocked other content not related to the SIC resolution—was performed by some of the service providers without considering the impact on the human rights of the users of their services. That seems to be the case of Emcali and Avantel regarding reports from several people who say they were unable to access the archive.org and ghostbin.co sites while using their services. These problems were confirmed by the Open Observatory of Network Interference (OONI), regarding which we recommend reading the column in El Espectador, *La peligrosa y torpe orden de bloquear páginas web* [The dangerous and clumsy order to block webpages] where the subject is explained in detail. It is worth noting that this does not seem to have happened with the rest of the service providers, which could indicate that the problem was not more significant thanks to the fact that some of the providers did not comply with an order issued by the SIC that was disproportionately restrictive with the fundamental rights of citizens.

web.karisma.org.co/wp-content/uploads/2021/06/Carta_visita_CIDH.pdf

[42] El Espectador. La peligrosa y torpe orden de bloquear páginas web. Accessed at: https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/la-peligrosa-y-torpe-orden-de-bloquear-paginas-web/

[43] Fundación Karisma. Tweet from May 21, 2021: https://twitter.com/Karisma/status/1412839454595760130

[44] El Espectador. La peligrosa y torpe orden de bloquear páginas web. Accessed at: https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/la-peligrosa-y-torpe-orden-de-bloquear-paginas-web/

Reviewing this action from the point of view of neutrality, it is clear that this rule protects legitimate content. In other words, one cannot speak of a violation of neutrality if abusive material against children and adolescents is blocked, nor if one acts to prevent the circulation of content that violates data protection regulations, for example. However, when the order of the authority is illegal or does not conform to the standards —because it is disproportionate, for example—then there is a relationship between those blockages and neutrality. The bad implementation has the effect of preventing access to legitimate content, which happens if an entire page is blocked trying to prevent people from accessing a specific URL.

Finally, it is worth noting that the SIC decided to modify its decision to block specific URLs after receiving a letter from some of the internet service providers explaining why compliance with this order was not technically feasible and how it put fundamental rights at risk. The former changed the recipient of the blocking order from service providers to the administrators of the domains archive.org and ghostbin.co.[45] Furthermore, one must not forget that the IACHR, in its observations and recommendations document following the working visit to Colombia, reaffirmed that blocking content or services is the last resort. That, precisely, is not justified except in extreme cases (such as the protection of minors from sexual exploitation); therefore, like any restriction on the exercise of freedom of expression, this must be legally enshrined, be necessary, and proportional.

[45] Superintendency of Industry and Commerce. Resolution Number 37070 of 2021. Available at: https://www.sic.gov.co/sites/default/files/documentos/062021/Resolucion37070del17deJunioDe2021_PorLaCualSeModificaElResuelvDeLaResolucion29323del14DeMayoDe2021.pdf

TWO. THEY ARE WITH ME OR AGAINST ME. THE STATE NARRATIVE THAT CRIMINALIZES DIGITAL PROTEST

The criminalization of social protest has been a constant in Colombia during the past decades[46]. However, with the irruption of telecommunications technologies, digital protest arose, and the picture changed. Political and social movements and civil society defense organizations had at their disposal a tool with the power to directly communicate their contents and make them viral. Faced with this new expression of digital political participation, the Colombian State has continued with its textbook response, that is, to stigmatize, criminalize and persecute.

The Internet is a space that encourages and spurs the exercise of protest. Whether through chain letters, online petitions, demonstrations, or campaigns on social networks, the network allows the full and democratic exercise of freedom of expression and information, the right to associate and participate in political life. For this reason, the State must guarantee access to the Internet for citizens and conditions that do not intimidate, stigmatize, or violate people who protest on the web.[47] As we explain below, the Colombian government seems not to have fulfilled this obligation during the national strike.

2.1 What are we talking about when we talk about cyber patrol?

When we talk about cyber patrol, it seems that we mean many things. What comprises the active digital patrolling performed by law enforcement during the national strike is unknown, which is already problematic. So, to understand this issue, before addressing what happened during the national strike, we will make some semantic clarifications about what cyber-patrol in Colombia is or seems to comprise.

In 2015 with the issuance of Resolution 5839 of the National Police,[48] cyber patrol makes its appearance within the legal system. Said regulation enabled the Police Cybernetic Center to "carry out cyber patrols 24/7 on the web" to identify threats against "citizen cybersecurity" of national or international origin. As well as to "develop the ability to identify and detect common factors in the incidents of their knowledge."[49] However, the resolution does not specify what cyber patrol comprises but rather directly enables the Police to do it without establishing procedures, permitted or prohibited tools, or limits. It is worth noting that a resolution does not have the status of a statutory law and, therefore, does not comply with the legal requirement of Article 13.2 of the American Convention, according to which any limitation on rights such as freedom of expression, association, and information must be clearly expressed in a legal norm, which has been the result of a democratic debate.

In the absence of a normative definition, it is necessary to look for other sources that allow us to understand what Colombian security organizations understand by cyber patrol. *The Defense Sector Report. Guarantees to peaceful demonstrations and control of violent actions, period from April 28 to June 4, 2021,*[50] of the Ministry of Defense (MinDefensa), sheds some light on what cyber patrol can be and does so in at least three dimensions: investigating and preventing cyber threats, misinformation, and profiling.

[46] 070 Magazine. La criminalización de la protesta en Colombia es histórica. Accessed at: https://cerosetenta.uniandes.edu.co/la-criminalizacion-de-la-protesta-social-en-colombia-es-historica1/#:~:text=La%20Corte%20Suprema%20de%20Justicia,frente% 20a% 20la% 20protest% 20social.

[47] Office of the Special Rapporteur for Freedom of Expression. Inter-American Commission on Human Rights. Protest and Human Rights. Accessed at: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

[48] National Police. Resolution 5829 of 2015. Available at: https://www.policia.gov.co/file/32305/download?token=OA0OIAOJ

[49] National Police. Resolution 5829 of 2015. Article 15, numeral 12.

[50] MinDefensa. The Defense Sector Report. Garantías a la manifestación pacífica y control de acciones violentas, período 28 de abril al 4 de junio de 2021. Available at: https://www.mindefensa.gov.co/irj/go/km/docs/pccshrcontent/Recursos%20MDN/Plantillas%20Documentos/Ministerio/CentroDocumentos/Generales/Recursos/INFORME_DEFENSA_GarantiasManifestacion.pdf

2.1.1. Patrolling the web to investigate and prevent cyber threats

In line with international examples, such as Spain,[51] in Colombia, it seems that, under the name of cyber patrolling, judicial investigation activities are being carried out on the possible commission, or for the prevention, of cybercrimes or crimes committed on or through the Internet.

The MinDefensa report mentioned indicates that thanks to cyber patrolling, "104 cyber events were detected, thusly; 41% (43 events), corresponds to defacements (modifications of web code), 32% (33 events), corresponds to information leak attacks, 20% (21 events) denial of service, 7% violation of websites (7 events)"[52]. According to the report, cyber patrol in Colombia involves searches and judicial inquiries about crimes committed through the Internet and the blocking of websites where these crimes are allegedly carried out. For example, in the latest report from the Ministry of Defense on the national strike, published on July 2, it is noted that during cyber patrol activities, the following have been recorded: 2,295,194 IP addresses with malicious behavior, 147,281 general preventive alerts, 1986 malicious campaigns and four domains identified in malicious campaigns[53].

However, MinDefensa has made public very little information about its monitoring activities on the Internet in the framework of activities to combat cybercrime. For example, it does not indicate which websites have been classified as malicious, what type of attacks have been registered, against whom, what actions were taken against I.P. addresses, what happens with the alerts they generate or with the domains they identify, how they relate to the protest or what "malicious campaign" means.

While the Police must have the ability to protect people from being victims of cybercrime, the tools they use must be regulated by a proportionate and reasonable legal framework that empowers them to do so. Within a democracy, no power must be absolute or arbitrary but must have adequate checks and balances, and this applies equally on and off the web. In these cases, the Colombian police actions are not clear or transparent, which prevents public scrutiny and therefore does not build trust in the authority, a central element of a cybersecurity policy.

We know very little about how this dimension of cyber patrolling was carried out during the strike or whether it is undergoing. However, if a cyber threat alert results in a domain name or URL being blocked, we need to guarantee it is done correctly, as mentioned in the net neutrality section.

2.1.2. Patrolling the web to combat misinformation

As inferred from the *General record of the national strike [Balances generales del paro nacional]*, published during May and June on the official Twitter account of the Ministry of Defense,[54] Another way of understanding or possibly sizing cyber patrolling is the monitoring of pages, profiles, and social networks in order to track fake news; as has also been the case in Argentina.[55]

The Police carried out the immediate Colombian precedent of a cyber patrol to identify online content that allegedly generated disinformation in 2020. Within the framework of the Covid-19 pandemic, the Police created

[51] RTVE Spain. ¿Qué es el ciberpatrullaje? Accessed at: https://www.rtve.es/play/audios/cooperacion-publica-en-el-mundo-fiapp/cooperacion-publica-mundo-fiiapp-ciberpatrullaje-01-07-20/5614376/

[52] MinDefensa. The Defense Sector Report. Garantías a la manifestación pacífica y control de acciones violentas, período 28 de abril al 4 de junio de 2021. Available at: https://www.mindefensa.gov.co/irj/go/km/docs/pccshrcontent/Recursos%20MDN/Plantillas%20Documentos/Ministerio/CentroDocumentos/Generales/Recursos/INFORME_DEFENSA_GarantiasManifestacion.pdf

[53] MinDefensa. Tweet, July 2: https://twitter.com/mindefensa/status/1410958233058037761

[54] MinDefensa official Twitter account. Publication July 2, 2021. Available at: https://twitter.com/mindefensa/status/1410958233058037761

[55] https://observatoriolegislativocele.com/ciberpatrullaje-o-inteligencia/

a periodic report of the fake news detected by the Virtual Immediate Response Police Unit.[56] Activity that at the time, was identified by the IACHR as a risk to the fundamental freedoms of the citizenry because "it could bring the region back to a logic of criminalizing expressions about officials or matters of public interest and establishing a tool with a strong inhibitory effect of the dissemination of ideas, criticism, and information."[57]

Despite what the IACHR has said, cyber patrolling, understood as tracking alleged "false news" seems to have gained currency in law enforcement. The Defense Sector Report already mentioned made this clear. This document indicates that during the national strike, 21,675 hours of cyber-patrolling were carried out until June 9, in which "disinformation campaigns were identified in order to generate chaos and hate content towards State institutions. 154 pieces of fake news have been identified and corroborated. Of these, 91 focused on misdirection with untruths that have affected the image of the National Police."[58]

The Police are devoting a considerable percentage of resources and time tracking and labeling posts on social networks as fake, in a self-appointed fashion, without legal support, of the power to act as "truth police." This denotes a generalized perception that citizens are guilty and the ignorance and stigmatization of political dissent and reports of human rights violations. Furthermore, it contradicts inter-American human rights standards since the government's attitude discourages denunciation and generates self-censorship.

2.1.3. Patrol the web to profile suspicious people and activities

In Colombia, there are disastrous and unpunished precedents of surveillance and profiling carried out by law enforcement, such as the cases of the DAS wiretaps[59] and the army files in early 2020.[60] In the latter case, the Colombian army engaged in massive and indiscriminate information collection, through computer tools, on different people they considered dangerous. An activity that is by all accounts a violation of human rights.[61]

Again, the *Defense Sector Report* shows that cyber patrolling also served to control protests in the physical world, in what we understand as a third form or dimension of cyber patrolling. The report notes that 3,420 preventive alerts were made in anticipation of acts of vandalism, 3,723 videos were analyzed to identify and distinguish those accountable, and that, thanks to this, 9 investigation proceedings were opened. These figures confirm that the monitoring of the network is extensive and that it includes "open-source intelligence" actions that lead to singling out people; that is, there is active surveillance of people's communications to criminalize them. How do human rights guarantees operate in these cases? Public information available does not provide data on this. Another aspect of the cyber patrol that we know little about is of concern, considering the history of wiretapping and profiling in Colombia.[62]

[56] Coronavirus and digital rights index. Cyberpatrol of the National Police to identify disinformation. Accessed at: https://cv19.karisma.org.co/docs/CiberpatrullajeDesinformacion/ y Policía Nacional. Reporte de noticias falsas detectadas por CAI Virtual. Accessed at: https://www.policia.gov.co/reporte-fakenews

[57] CIDH y su RELE expresan preocupación por las restricciones a la libertad de expresión y el acceso a la información en la respuesta de Estados a la pandemia del COVID-19. Available at: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1173&lID=2

[58] Ibid.

[59] Revista Semana. Así fueron las Chuzadas del DAS a la Corte Suprema de Justicia. Available at: https://www.semana.com/nacion/articulo/asi-fue-la-conspiracion/121785-3/

[60] Revista Semana. Las carpeta Secretas. Accessed at: https://especiales.semana.com/espionage-desde-el-ejercito-nacional-las-folders-secretas-investigacion/index.html

[61] Revista Semana. Así fueron las Chuzadas del DAS a la Corte Suprema de Justicia. Available at: https://www.semana.com/nacion/articulo/asi-fue-la-conspiracion/121785-3/

[62] Fundación Karisma. El ciberbolillo que nos espera. Accessed at: https://web.karisma.org.co/el-ciberbolillo-que-nos-espera/

Proof of this is the "cyber intelligence system based on artificial intelligence" that the Police tried to acquire in 2020 and finally acquired in July 2021[63] to monitor websites, social networks, TOR, I2p, Freenet, and instant messaging systems such as Telegram.[64] Although the contracting proceedings were declared void on two occasions, it is very telling that the Police would acquire an automated system that allows them to perform profiling from the social network publications of citizens. The breadth of the criteria for "dangerous" that the Police may use puts citizens' freedom of expression and information at risk since it is possible that retaliation will take place based on profiles from behavior in networks or that citizens self-censor, stop participating in debates, or following groups or celebrities to avoid being singled out.

Concerning cyber patrol, the IACHR, in its "*Observations and Recommendations. Working visit to Colombia*" document, did not speak to the first dimension, it dealt for the most part with the second dimension and said something about the third. The Commission pointed out that cyber patrolling targeted "the proactive monitoring of allegedly false content regarding the evolution of the protests, discrediting the image of law enforcement, as well as the instigation of public hatred."[65] They further noted that said action by the Colombian State, where the security forces abrogate the power to check and classify complaints on the Internet as true or false, is "especially worrying" since information on the security forces' actions is categorized. Moreover, it said that such behavior promotes censorship.

2.2 The law enforcement offensive to take over the narrative in the digital public space

During the national strike, law enforcement was left in a bad light at the national and international level when, in the first weeks of protests, the Internet was flooded with denunciations and videos about the alleged excessive use of force or possible human rights violations. Faced with this barrage of complaints and outrage, the Ministry of Defense did not react with sanctions to those involved in alleged excesses or crimes, but by launching, what seems to be, a strategy to take over the narrative on the national strike and the actions of the security organizations in the digital public space. This dimension of cyber patrolling was discussed the most and was what we saw during the national strike.

There are some clear indications that cyber patrol was used as a tool to control the narrative in the digital public space. To begin with, as explained, the implementation of the truth police that catalogs its actions as true or false denotes the Defense Ministry's interest in managing its image and not so much caring about the security of citizens. The power of law enforcement to verify with its confidential sources that what is published on the Internet by citizens is false, in addition to not having legal support and that the IACHR has cataloged it on several occasions as a threat to freedom of expression and information, arises from the interest in countering complaints against law enforcement.

On May 5, 2021, this was exemplified when the #ColombiaEsMiVerdad campaign was launched through the

[63] Fundación Karisma. Nuevo Contrato de la DIPOL para perfilar y rastrear a las personas en internet. Accessed at: https://web.karisma.org.co/nuevo-contrato-de-la-dipol-para-perfilar-y-rastrear-a-las-personas-en-internet/

[64] Karisma Foundation in collaboration with NGO Temblores. Dime a quién sigues y te diré qué tan peligrosos eres. Accessed at: https://web.karisma.org.co/dime-a-quien-sigues-y-te-dire-que-tan-peligroso-eres/

[65] Inter-American Commission on Human Rights. Observations and Recommendations. Working visit to Colombia. Accessed at: https://www.oas.org/en/iachr/reports/pdfs/ObservacionesVisita_CIDH_Colombia_ENG.pdf

official social networks of all branches of the armed forces and the Ministry of Defense, which attempted to end "misinformation" framing publications that did not benefit the image of the army or the Police as fake news or digital terrorism.[66]

The Fake News Bulletin of the National Police[67] or the publications made on May 13 by the Police[68] and on May 19 by the army[69] on their networks are a part of this image campaign, under the hashtags: #ColomabiaEsMiVerdad, #RompaLaCadena, #MeInformoMejor, making appeals not to share what they call false with the aim of "breaking the chain of disinformation."

However, as the strike has advanced and the intensity of the confrontations has decreased, at least during June, the hashtag #ColombiaEsMiVerdad began to be used by members of law enforcement and from their official networks to disseminate information that legitimizes the military or helps spread a positive image of the military.[70] Meanwhile, #RompaLaCadena continues to be used actively to fight against "misinformation" and making a call "not to play the game of fake news through social networks."[71] Finally, #MeInformoMejor has been used from official accounts of the Presidency and Vice Presidency to signal public complaints as false and request that they not be shared[72].

The campaign against the supposed disinformation carried out by law enforcement shows the intention to control what is said in the digital public space about what was happening in Colombia. First, complaints about possible human rights violations and the content unrelated to the security organizations were cataloged, without legal support, as true or false. Furthermore, the Office of the President promoted not sharing previously cataloged publications and, instead, from the accounts belonging to entities attached to the Ministry of Defense, news favorable to their image was published and shared. All these behaviors show an intention to control when, how, and what was said about unemployment and law enforcement on social networks, the most important and far-reaching debate space today.

Additionally, there were many cases in which local or national government officials have referred in a stigmatizing way to citizens who, in one way or another, are an active part of the national strike. On the same day the demonstrations began, April 28, 2021, the Presidential Advisor for Human Rights, Nancy Patricia Gutierrez, pointed out that there were "vandals who camouflage themselves among the protesters" and that they deserved "harsher criminal sanction."[73] As the strike intensified and social media began to flood with content about clashes between protesters and law enforcement or allegations of abuse in the use of force by the Police, the campaign to criminalize the protest was also digitized.

On May 3, the defense minister, Diego Molano, said in a tweet that "the terrorists are operating with sum-

[66] El Tiempo. Ministerio de Defensa Lanza Campaña contra Noticias Falsas en el Paro. Accessed at: https://www.eltiempo.com/justicia/servicios/ministerio-de-defensa-lanza-campana-contra-noticias-falsas-en-el-paro-586659?utm_medium=Social&utm_source=Twitter#Echobox=1620400394

[67] National Police. Fake News en el marco del Paro Nacional 28a, 29a y 30a. Accessed at: https://oas.policia.gov.co/sites/default/files/documento_10_fake_news_manifestaciones.pdf

[68] Special Operations Unit in Emergencies. May 13 Tweet: https://twitter.com/GrupoPONALSAR/status/1392910787904147457?s=20

[69] Directorate for the Expansion of Transparency Standards of the Army, Tweet from May 19: https://twitter.com/YoSoyDanteEJC/status/1395116046860836867?s=20

[70] Hashtags #ColomabiaEsMiVerdad on Twitter: https://twitter.com/search?q=%23ColombiaesMIvERDAD&src=typed_query

[71] Hashtags # RompaLaCadena on twitter: https://twitter.com/search?q=%23RompaLaCadena&src=typed_query

[72] #MeInformoMejor hashtags on twitter: https://twitter.com/search?q=%23MeInformoMejor&src=typed_query

[73] Presidency of the Republic of Colombia. "Vándalos son criminales que merecen la sanción penal más dura": Counselor Nancy Patricia Gutiérrez. Accessed at: http://www.derechoshumanos.gov.co/Prensa/2021/Paginas/280421-Vandalos-son-criminales-que-merecen-la-sancion-penal-mas-dura-Consejera-Nancy-Patricia-Gutierrez.aspx

mons through WhatsApp and Telegram, and their actions have been systematic in major cities."[74] Similarly, the Ministry of Defense launched the #ColombiaEsMiVerdad campaign mentioned before through its social networks. The intent was to dismiss the accusations against the law enforcement as false and in response to the activism of K-pop fans—mostly young women—who had seized hashtags like #SupportAMiFuerzaPublica, #NoMasParo #ParoDestructorSOS, #UribeTieneLaRazon, and #YoApoyoAlEsmad, to disseminate information about their favorite bands and songs, countering the trend started by Colombian politician, Alvaro Uribe Velez, in defense of law enforcement using arms against the people who were demonstrating.[75]

Another example of the campaign to delegitimize the protest by the Ministry of Defense is the video published on May 6, 2021, on the official Facebook and Twitter accounts of Minister Molano[76]. The publication in which he literally dismissed complaints about law enforcement as false and referred to these as "digital terrorism."[77]

On May 7, the Commander General of the Armed Forces referred to the protests of K-pop fans as fake news in a statement.[78] Additionally, that same day, the director of the Police spoke through a video denying the accusations of abuse by ESMAD and the Police and pointing out that these complaints were part of a campaign of disinformation and digital terrorism.[79]

President Duque has also participated in the campaign to criminalize network activism during the strike. On May 28, 2021, when the first month of demonstrations was completed, and after a day marked by violence in the streets and by complaints on networks about armed civilians working together with the Police, the president referred to what happened in a speech in Cali pointing out the existence of "islands of anarchy" and a "low intensity urban digital terrorism" campaign.[80]

The IACHR made pronouncements regarding the allegations of falsehood and digital terrorism in its *Observations and recommendations. Working visit to Colombia*. The Commission called for law enforcement to stop rating the contents, avoiding incurring censorship and recommended that the State provide more information on the subject to the public debate. In addition, he pointed out that it had "received complaints from the authorities regarding people who publish information that contains, in his opinion, messages of "hatred" or "incitement to violence."[81] In other words, content was being published outside the limits of the right to freedom of expression and that it may be intervened by a judicial authority, respecting due process. Regarding this issue, the IACHR urged the Colombian government to make the respective complaints, but again to refrain, as is its duty, from qualifying or censoring.

Thus, the strategy of the Colombian State to capture the narrative about the strike and law enforcement on the Internet—the contemporary space for public debate with the most significant scope and importance—has four steps: 1) point out as false the complaints about excesses by the security forces, invite not to share and

[74] MinDefensa. Tweet, May 3: https://twitter.com/mindefensa/status/1410958233058037761

[75] Semana. Fans del K-pop "spamean" hashtags uribistas. Accessed at: https://www.semana.com/cultura/articulo/fans-del-k-pop-spamean-hashtags-uribistas/202132/

[76] Defense Minister, Diego Molano. Tweet May 6, 2021: https://twitter.com/Diego_Molano/status/1390311574800375809?s=20

[77] Defense Minister, Diego Molano. Facebook post on May 6, 2021: https://www.facebook.com/DiegoMolanoAponte/videos/2861421874131466/

[78] https://www.cgfm.mil.co/es/blog/colombia-es-mi-verdad-campana-que-busca-terminar-con-las-noticias-falsas

[79] Semana. "Es falso que la policía ataca la manifestación pública y pacífica": general Jorge Vargas, director de la institución. Accessed at: https://www.semana.com/nacion/articulo/es-falso-que-la-policia-ataca-la-manifestacion-publica-y-pacifica-general-jorge-vargas-director-de-la-institucion/ 202144 /

[80] Presidency of the Republic of Colombia. Statement by the President of the Republic, Iván Duque Márquez - May 28, 2021. Available at: https://www.youtube.com/watch?v=uAZj0kKxejA

[81] Accessed at: https://www.oas.org/en/iachr/reports/pdfs/ObservacionesVisita_CIDH_Colombia_ENG.pdf

promote content that benefits their image, 2) point out as vandalism and, therefore, terrorists, the organized actions of citizens in favor of the strike, 3) make use of the categories of the American Convention, which place limits on freedom of expression—incitement to hatred and violence—to indicate the content of citizens and thus encourage them to be blocked by the platforms and 4) bring the stigmatization of the protest and of those who protest towards criminalization using the exceptional framework of terrorism in order to discourage participation in demonstrations. All this, presumably, to mutate the online narrative of a legitimate protest movement with complaints of excesses in the use of force by the State to episodes of vandalism and terrorism, physical and digital, where false or hate-inciting narratives were promoted.

THREE. TECHNOLOGY AT THE SERVICE OF SURVEILLANCE OR HOW TO ABUSE THE TOOL TO CONTROL PROTESTS AND THREATEN PEOPLE'S RIGHTS

The lack of regulation on the use of non-lethal weapons was recognized by the former U.N. Special Rapporteur on Extrajudicial Executions, Christof Heyns, as a risk to human rights since 2014.[82] Despite this, the variety of non-lethal or less-lethal weapons at present has only increased due to technological advances. In many cases, the line that differentiates lethal from non-lethal has been lost.[83]

Something similar happens with digital technology. Technological advances have also incorporated various types of technology to control and monitor social demonstrations or crowds by the State. Furthermore, although it is to be assumed that with the appearance of new technologies, the State's regulation of them would be increased so that they are not abused and can become a threat, that does not seem to be the case in Colombia.

In this section, we will address the case of facial recognition devices and access to people's cell phones by the State in the context of the national strike, exposing the risks that these imply for the fundamental rights of citizens.

3.1. Use of surveillance technology in the framework of citizen protests

In 2020, the United Nations High Commissioner for Human Rights, Michelle Bachelet, published a report on technologies that violate the right to peaceful protest. The report pointed out that "surveillance by technological means has been an important factor in the reduction of civic space that has occurred in many countries" since "the authorities use these means to monitor those who participate in protests directly."[84] This, in turn, causes people to lose interest in publicly expressing their ideas "for fear of being identified and later suffer adverse consequences."[85]

Consequently, the high commissioner recommended that the States "refrain from using facial recognition technology to identify those who participate in peaceful meetings and not make recordings of the protesters."[86] A recommendation that the Colombian State ignores.

3.1.1 What is facial recognition

A brief introduction is necessary before addressing the Colombian State's possible uses of facial recognition technology. Facial recognition is "a method through which to identify or verify the identity of a person using captures of their face, through the use of photographs, stored videos or cameras that capture images in real-time."[87] This technology aims to authenticate a person's identity, that is, to verify if the person is who they say they are or to identify an individual, in other words, to establish who they are or what their identity is.[88]

Now, identifying and authenticating a person's identity requires 1) capturing a face from different sensors, such as cameras, videos, or images, and 2) a database containing the records of the faces of various people to compare with the previously captured image.

[82] UN, Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Note from the Secretary General, A / 69/265, August 6, 2014 para. 73.
[83] Office of the Special Rapporteur for Freedom of Expression. Protest and Human Rights. Paragraphs 119 and 120.. Available at: https://www.oas.org/en/iachr/expression/publications/Protesta/ProtestHumanRights.pdf"
[84] Office of the United Nations High Commissioner for Human Rights. Las nuevas tecnologías deben reforzar el derecho a la protesta pacífica, no impedirlo. Accessed at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=E
[85] Ibid.
[86] Ibid.
[87] Fundación Karisma. What is and how does facial recognition work? Accessed at: https://digitalid.karisma.org.co/2021/07/01/que-es-reconocimiento-facial/
[88] Ibid.

In summary, the facial recognition process is as follows: first, a query image is captured, that is, the image of a person's face; then, the system detects and determines the position of the eyes and, from there, the query image is converted into a "facial print," that is, into a numerical and digital representation of this face. Once the facial print is created, it is compared with all the facial prints stored in the database. For a detailed explanation about this procedure, we recommend I.D. Colombia, *What is and how does facial recognition work?*[89]

3.1.2 Facial recognition system in the hands of the Colombian State

It is known with certainty that at least three entities of the Colombian State have systems capable of massively identifying faces in any video or image format: Migration Colombia, the National Police, and the National Registry.[90] Here we will briefly refer to the last two entities since their actions may be related to what happened during the national strike.

The Registrar's Office manages the National Identity System (SNI), which has facial recognition technology and contains the data of all people over seven years of age who have processed identity documents. This system aims to legally identify people based on unique characteristics, in this case through algorithms that identify facial biometrics. Specifically, since 2018, the Registry has included facial recognition in the SNI and offers it as a service to third parties, including law enforcement, without it being clear what legal framework or guarantees with the right to privacy it is applying.[91]

On the side of the National Police, it has been established that in 2019 they contracted a facial, palm, and finger biometric system to "individualize crime" by identifying people in videos and images[92]. In addition, as reported by the Directorate of Criminal Investigation and Interpol of the National Police to the Karisma Foundation in 2021, the ABIS system of the Police would be using the Registrar's databases to compare query images. As in the case of the Registrar, this technology is being used without a controlling legal framework, and possibly, even in political contexts, such as demonstrations and protests. This system is run by the DIJIN, the Judicial Police, so ideally, it should be used in criminal investigations and with prior judicial authorization. However, we cannot rule out that the system can be used in protest contexts because the ABIS system is in the hands of law enforcement authorities and could be used outside the context of criminal investigations.

3.1.3 Inappropriate use of technology to control social protest during the national strike

In 2019, the National Police launched, in Bogotá and Medellín, a camera to monitor the demonstrations during November.[93] As reported in several national media, the high-quality cameras incorporated into the police hawk helicopter had software that compared the physical features captured with those of the databases of the security agency such as the Directorate of Criminal Investigation and Interpol. (Dijin) and with the databases of the National Registry.[94] The Police said that these cameras would be used in areas where there were disturbances to

[89] Ibid.

[90] Fundación Karisma. Facial Recognition Guide in Colombia. Accessed at: https://digitalid.karisma.org.co/2021/07/01/guia-reconocimiento-facial/

[91] Fundación Karisma. The recognition system of the General Registry. Accessed at: https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/

[92] Fundación Karisma. El sistema multibiométrico ABIS de la Policía Nacional. Accessed at: https://digitalid.karisma.org.co/2021/07/01/ABIS-reconocimiento-facial/

[93] Revista Semana. This is the hawk, the helicopter that will monitor the stroke in Bogotá using facial recognition. Accessed at:https://www.semana.com/nacion/articulo/paro-21-de-noviembre-el-helicopio-que-vigilara-en-bogota-usando-reconocimiento-facial/641014/

[94] El Tiempo. Helicóptero halcón de la Policía estrenando identificación facial. Accessed at : https://

public order as a guide for those in uniform on the ground and, it was said, had a range of more than 15 meters.

However, in January 2021, the NGO, Dejusticia, questioned whether the Police were indeed using facial recognition tools to monitor demonstrations, stating *"that communication was an attempt by the authorities to dissuade Colombians from going out to protest."*[95] This conclusion follow on queries, through rights to petition with the Prosecutor's Office and Police, on investigations or prosecutions "as a result of the effective use of that tool."

There is no doubt about the presence of helicopters that have flown over protests during the National Strike in 2021 and during the marches associated with the 21N movement in previous years. In Bogota,[96] Cali,[97] Buga, [98]there are reports or videos of military helicopters flying over marches. We insist that what is not certain is whether they have processed images captured from helicopters to identify people with the help of the Registrar's databases or any other. Once again, the extreme opacity of the Colombian State, at least concerning the defense sector, makes it difficult to know what the security organs are doing or not doing. We insist this last is not compatible with the guarantees required of the State regarding a citizens' protest.

The other type of technology on which there are doubts regarding Police use in social protest is drones. The first thing to say is that the Police are equipped with this type of technology[99] and use it frequently[100] in different parts of the country.[101] In 2020, the Supreme Court of Justice protected the right to protest of several people and ordered a series of changes to the protocols and elements that the police riot squad can use.[102] However, technology was the significant issue absent from the sentence, which is why today, these devices could be used to monitor the strike marches. The Ombudsman's Office actually recommended that the Police use drones in the framework of the protest[103].

As things stand, it is not unreasonable to think that the drones that sometimes fly over the marches and crowds that occurred within the national strike were from law enforcement. Using these devices without proper regulation and control puts the right to privacy at risk and affects citizens' legitimate right to protest. As with internet hacks and facial recognition technology, however, there is no certainty. Given that there is no precise regulation on technology and the State does not periodically report on these matters, everything remains open to speculation.

www.eltiempo.com/bogota/estrenan-helicocopio-halcon-con-reconocimiento-facial-en-paro-del-21-de-nov Diciembre-435766

[95] Dejusticia. Día de la protección de datos: helicópteros, reconocimiento facial y protesta. Accessed at: https://www.dejusticia.org/dia-de-la-proteccion-de-datos-helicopteros-reconocimiento-facial-y-protesta/

[96] Revista Semana. ¿Por qué aterrizó un helicóptero de guerra Black Hawk anoche en Bogotá?. Accessed at: https://www.youtube.com/watch?v=fEMTX2vAz1g&ab_channel=RevistaSemana

[97] Vice. Colombia Is Rising Up. Accessed at: https://www.youtube.com/watch?v=WB2isJA1JdU&ab_channel=VICENews

[98] Infobae. Momentos de pánico en Buga por un helicóptero en medio de disturbios tras el paro nacional Accessed at: https://www.infobae.com/america/colombia/2021/05/06/video-momentos-de-panico-en-buga-por-un-helicoptero-en-medio-de-disturbios-tras-el-paro-nacional/

[99] Bogota City Hall. Five state-of-the-art drones will help take care of life in Bogotá. Accessed at: https://bogota.gov.co/asi-vamos/drones-de-ultima-tecnologia-refuerzan-seguridad-de-bogota

[100] El Tiempo. Patrulla con drones logró captura de 47 delincuentes en Barranquilla. Accessed at: https://www.eltiempo.com/colombia/barranquilla/patrulla-con-drones-ha-logrado-decenas-de-capturas-en-barranquilla-384854

[101] Blue Radio. Con drones pretenden vigilar la ciudad de Medellín para evitar las construcciones ilegales. Accessed at:https://www.bluradio.com/tecnologia/con-drones-pretenden-vigilar-la-ciudad-de-medellin-para-avitar-las-legales-construcciones-

[102] Dejusticia. Corte Suprema de Justicia protege el derecho a la protesta frente a la violencia policial. Accessed at:https://www.dejusticia.org/corte-suprema-protege-el-derecho-a-la-protesta/

[103] El Tiempo. Vigilar Protesta con drones y otras recomendaciones de la Defensoría. Accessed at: https://www.eltiempo.com/justicia/servicios/marchas-y-protestas-las-33-recomendaciones-de-defensoria-del-pueblo-para-evitar-violencia-556308

In this case, the state entity called upon to regulate and investigate the drones that fly over the marches is Civil Aeronautics, an administrative unit that issued the Colombian Aeronautical Regulations, the norm that by analogy applies to drones.[104] However, Aeronautics has not ruled on the matter, which again creates a legal vacuum that leaves the rights of citizens unprotected. At a minimum, the drones that fly over a demonstration would be expected to be identified so who controls them, and the number of the device is known, as in the case of police officers themselves. This provision would allow citizens to exercise some of their rights or to hold law enforcement accountable.

3.2 Searches of cell phones. A common practice that violates the fundamental right to privacy

Article 159 of the Colombian Police Code, and recently the Constitutional Court,[105] grant Police a high level of discretion to search or question people. However, the Police's power is not the permission to search people's cell phones at their discretion. The contents of a cell phone, such as chats, videos, images, records, keys, documents, among others, are directly related to the right to privacy of people, as it is information that only concerns the owner of the device and that it can also be connected with other constitutional guarantees such as professional secrecy or confidentiality of the source.

For this reason, as with a search of a house, the Police can only seize a cell phone with a court order. Otherwise, the fundamental rights to privacy, due process, and the presumption of innocence are violated. Now, complaints about cell phone searches are a constant in Colombia in the context of social protest.[106] There have even been reported cases in which the Police search to check people's social networks.[107] These actions imply an interference by the State security forces in the people's most personal and intimate sphere.

To understand what happens with searches of cell phones in Colombia, we must talk about the policy of the MinTIC of IMEI registration, the unique code that identifies cell phones, to combat the theft of devices. This policy is inefficient since it has not solved the problem of cell phone theft, while also putting the fundamental rights of citizens at risk,[108] as it serves so that the Police, who cannot check cell phones, can force people to show them the IMEI of their cell phone to verify that the device is not stolen; it has also lent itself to some irregularities.

Within the framework of demonstrations, there have been complaints that with the excuse of checking the IMEI, some police officers ask people for the password and unlock the cell phone, then they can review social networks or delete images and videos evidence of possible human rights abuses or violations.[109],[110] During the protest, Fundación Karisma also received some reports of direct intimidation by police officers against citizens to unlock their cell phones or in which they took advantage of the moment to place or remove the

[104] Externado University Magazine. Del campo de batalla a las calles: el derecho a la intimidad en la era de los drones. Accessed at: https://revistas.uexternado.edu.co/index.php/derest/article/view/4339/5066

[105] Infobae. Qué hacer si, en una requisa, la Policía le pide su celular. Accessed at: https://www.infobae.com/america/colombia/2021/03/04/que-hacer-si-en-una-requisa-la-policia-le-pide-su-celular/

[106] Legal milieu. ¿Las requisas policivas pueden incluir la revisión de redes sociales?. Accessed at: https://www.ambitojuridico.com/noticias/general/constitucional-y-derechos-humanos/las-requisas-policivas-pueden-incluir-la

[107] Fundación Karisma. Tweet from December 4, 2020: https://twitter.com/karisma/status/1202298426601463809?lang=es

[108] Fundación Karisma. Revisar IMEI, excusa para el abuso policial. Accessed at: https://web.karisma.org.co/revisar-imei-excusa-para-el-abuso-policial/

[109] Ibid.

[110] NGO tremors. Bolillo, Dios y Patria. Accessed at: https://issuu.com/temblores/docs/bolillo-dios-patria-digital

handcuffs to put citizens´ fingerprints on the cell phone reader without consent and thus unlock it.

The issue is complex: the Police cannot review the content of cell phones without a court order, but they can verify the IMEI in the databases of stolen cell phones, for which they can require the person to show them the IMEI of the device. In this way, when the regulation is harmonized, the stipulated procedure is that the person himself dials *#06# to show the IMEI of the device without having to hand over the cell phone or unlock it.

However, the line between checking the cell phone and verifying the IMEI in the middle of a search is too thin in practice and puts the fundamental rights of citizens at risk. In the context of a search, it is difficult to explain to a police officer the technical and legal details of the case, and many people may agree to hand over their cell phones when they feel intimidated. Therefore, the existence of the IMEI policy is a risk for the fundamental rights of citizens since it is an excuse for the Police to access cell phones. Even more in the context of protest, where searches increase and abuses by law enforcement are registered.

Thus, it is necessary to rethink the policies of the MinTIC on stolen cell phones and to issue protocols that make it clear that cell phone searches are equivalent to breaking into a house and, therefore, must meet the most demanding standards for the protection of privacy of people.

Colombia will need to develop a judicial framework for the protection of protests, and when it does so, it will need to make sure that surveillance technologies used during these do not limit fundamental rights and, therefore, they must respond to human rights standards, be outlined in law, justify their need, their use must be proportional, and respect due process.

It is essential to analyze the specific case of facial recognition technology used by law enforcement in these environments, given that in some countries, it has been deemed disproportionate and, therefore, has been prohibited. At the same time, we deploy it here without even having a legal framework. We ask that the technology used in protests be regulated, that protocols and procedures be developed to guarantee the exercise of the rights of people.

FOUR. SERVICE PROVIDERS. KEY ACTORS FOR THE GUARANTEE AND PROTECTION OF HUMAN RIGHTS DURING THE PROTESTS

The Internet has been recognized by the Colombian State and the IACHR as a tool that democratized and expanded the possibilities of exercising fundamental citizenship rights[111]. Now, it is a fact that the Internet is governed in a multi stakeholder manner; although governments have vital interests in regulating this network, its deployment and operation depend primarily on the private sector. In addition, it is recognized that due to its nature as a global communication medium, the Internet is subject to public law rules, and its regulation is not limited solely to what is established in private contracts.[112] All this without forgetting that civil society also plays an essential role in their discussions.

Given the role that the Internet and social networks have acquired in people's daily lives, it was only a matter of time before their relevance in society's public and political life became evident. The preceding has happened during elections and made evident during the recent social mobilizations in Latin America and during the social and political demonstrations against the Colombian government in 2021.

During the national strike, especially in the middle of the days with greater citizen participation or in which there have been clashes between protesters and law enforcement, social networks became the primary mechanism for reporting abuses of authority or violations of human rights. However, with the growing national outrage, reports also appeared on social networks of people who could not upload videos to their social networks, make live broadcasts, share other people's content, or the information they were uploading to their social networks was restricted in reach. All this, added to the complaints of internet blocks, already explained, generated a feeling of online censorship.

Although censorship is usually felt directed by the State, communication is mediated by private companies that suddenly seem not to allow citizens to express themselves at a crucial and urgent moment. Therefore, in times of growing social tension and considering the complexity of connectivity and use of services on the Internet, establishing the origin and nature of the problems people face in communicating can prevent the feeling of state censorship from increasing.

In the 2016 report on the role of the private sector and the State in the exercise of freedom of expression on the Internet,[113] the U.N. rapporteur for the promotion and protection of the right to freedom of expression recognized the important role of the private sector in respecting freedom of expression in the digital age. The report recognizes that companies are subject to state pressure that can lead to limitations on people's rights but reminds them that they also perform independent functions that can promote or restrict rights. The measure that is particularly highlighted in this report is transparency in the procedures applied by the private sector. It must consider impact assessments on people's rights and the possibility of providing information and data on their actions that allow for public scrutiny.

Here we explain three possible causes of the problems to communicate through the Internet that occurred during the 2021 national strike.

[111] Office of the Special Rapporteur for Freedom of Expression IACHR. Standards for a free, open and inclusive internet. http://www.oas.org/en/iachr/expression/docs/publications/internet_2016_eng.pdf

[112] United Nations. General Assembly. Resolution 70/125. Final document of the high-level meeting of the General Assembly on the general review of the implementation of the results of the World Summit on the Information Society, UN Doc. A/RES/70/125. February 1, 2016. Para. 9.

[113] See: https://www.undocs.org/A/HRC/32/38

4.1. Problems with the infrastructure for the provision of internet service

As previously explained, a proximate cause of the connection problems experienced by citizens may originate in failures in the internet infrastructure (such as damage, maintenance, or power outages) or overloaded networks (which can happen when there are concentrations of people who demand robust bandwidth). These types of events are frequent, and the information that companies provide about their performance and the current health of their networks is essential to clarify what is happening.

Regarding the case of the night of May 4 in Cali, we reiterate that the uproar in social networks led Movistar to inform the media and the ICT Ministry that there was damage in its network as a result of the theft of cables and the impossibility of repairing them due to the public order problems that shook Cali that day. This made it possible to understand the failure reported by Netblocks and also establish that the failures that occurred in sites like Siloé did not respond to problems in the infrastructure of the Internet operating companies in the country.

4.2. Content moderation

The second cause of problems in disseminating publications on networks is content moderation policies. Several factors help explain account cancellation, or scope restrictions, and content blocking on social media. As we explained in the chapter on connectivity, many factors must converge for a livestream to work during a protest. Not only does connectivity have to be activated through the physical infrastructure, but we must also be able to use the services that allow sharing content that we want to communicate and that is materialized in different formats (text, audio, video, or images) where social networks are the most obvious layer for people who use the Internet.

The content circulating on social networks is subject to the community rules, that is, to the rules that the people who use them must follow to prevent their accounts from being canceled or their contents from being blocked, or their reach diminished. Applying these rules and sanctions is known as content moderation and is carried out following the latest version of the terms of use that we accept when registering on the corresponding platform.

Thus, for the "livestream" to be successful, at least the Internet and electrical infrastructures must be active, the platform service working appropriately—we will talk about this in the following case—and the transmitted content must pass the content moderation filter. Content moderation happens all the time; however, the volume of information that is produced in a protest, the concentration of content production that can occur in the head of a few people at certain times, and the nature of the same—content that denounces police abuse can be classified, for example, as violent content that is prohibited by community rules— make content moderation the protagonist of protests and many people linked to that moment resent it in particular.

The social networks are thought to be a "family environment in daily use," suddenly, during protests that turn violent and confront different actors, they become scenarios for denouncing human rights violations, creating tensions and significant frustrations. Something similar to the right to enter a bar, club, or store, being a private place, we accept the rules, or otherwise, we are left out. However, this does not authorize the club to have discriminatory actions. In social networks—which belong to private multinationals—everyday content that does not comply with the terms of use that we accept when registering is blocked and taken down. However, when there is a social event, and people are counting on their accounts to report, these companies must protect communications and act to prevent their community norms from hindering denouncing severe human rights abuses.

To cite some cases in the context of the national strike, we find what happened on Twitter with the official account of Noís Radio, an alternative medium in Cali. On May 6, the media outlet reported that its Twitter account @noisradio had been "repeatedly restricted and tagged with the notice" Caution: This account is temporarily restricted, "after posting a note about police abuse. Although Twitter argued before the media that it is about "authenticity challenges," as Nois Radio was asked to prove a bot did not control it. Nois Radio appealed the decisions, but the situation was repeated several times, leading them to state that social network appeal proceedings are ineffective. Additionally, Noís Radio considers that labels like that end up silencing their voice as the warning notices are visible for those who browse in Colombia and other countries due to the application of the private platform's terms of use. "They violate freedom of expression, and they feed the sensation of censorship on the Internet during a situation like the one that Colombia has experienced in recent weeks," as the media outlet directly reported.

Another paradigmatic example is Twitter's labeling of tweets about public hearings before the IACHR during its working visit in Colombia as "potentially sensitive" content, as happened on June 9 in the account of the human rights defender and environmentalist, Francia Marquez.[114]

Blocking problems during the strike have led some journalists to resort to several accounts or use numerical characters in the descriptions of their publications to trick the algorithm. The independent journalist, Jahfrann, in unpublished testimony given to the FLIP, explains it this way: "I've had times when I've wanted to do a Live [broadcast], and the two [Instagram] accounts have been blocked for me. I have to use another channel because Instagram does not respond, you can wait, but they will never reply to you. They simply tell you that they blocked you, and that's it. In addition, there are words that one cannot place; an SOS COLOMBIA is a certain block. So you have to look at what and how to post, and sometimes you don't post; or if you say ALERT, you use a "4" instead of an "A" or type a 3 instead of "E" (4L3RTA). You start playing with these algorithms."

Given these irregularities regarding content control, where it is labeled as dangerous, or publications related to the defense of human rights are blocked, a thorough and contextual evaluation of what is being censored is necessary. Often, the community norms of social networks are ambiguous or extend the Inter-American Convention on Human Rights limits, or—simply put—they are not designed for the Latin American context, much less for a social protest. Which flatly limits the possibilities of expression within the networks.

The challenges of mitigating the impact of content moderation by platforms during social uprisings remain. Although efforts by companies to reduce this impact are identified—such as using more labels and reducing the reach of publications and less content blocking and account cancellation—the feeling of censorship during the protests is permanent. Moreover, the absence of information on how companies deal with these situations does not provide peace of mind to people who depend on these tools to publish content and denunciations of serious human rights violations. In this, there is still much to improve.

4.3. Platform software also crashes and can impact social protest

We have already said that for the communication of the people participating in the protest to happen, the physical infrastructure must work, and content must not be filtered in the internal moderation processes of the platforms, websites, and applications themselves, but also the social network software we use is required to function correctly. The latter is seldom discussed, but it is also crucial during a protest. The problems with the

[114] Francia Márquez M. Tweet from June 9: https://twitter.com/FranciaMarquezM/status/1402648233621475329

software are a third possible explanation for the content publication and distribution problems experienced during the strike.

In the first week of demonstrations, many people and social organizations reported problems uploading content related to the national strike to social networks. Between May 6 and 7, this happened mainly on Instagram.[115] This social network was used to share content related to the strike, videos about possible police abuses, live broadcasts of the march, artistic presentations, and clashes.[116]

On May 6, 2021, reports about Instagram Stories problems were trending in the morning. The phenomenon was so widespread that at the Karisma Foundation, we went from receiving eight reports of problems with content on social networks between April 28 and May 5 to 100 reports only on May 6 in the morning and at night on the same day, the reports reached a total of 800 cases. 90% of the cases that were reported to us were due to problems on Instagram.[117]

That same day, May 6, Facebook, the company that owns the social network Instagram, reported a global failure[118] and fixed it in a matter of a day.[119] In addition, on May 7, Instagram explained that the failure had particular importance in Colombia but that it also affected the Palestinian people[120] and indigenous communities in the U.S. and Canada[121] who commemorated the day against violence against native communities.[122] This statement clarified that the failure was not generalized but affected content related to social, political, and ethnic causes in three specific geographical locations.

In the case of Instagram, as reported by the same platform, we are talking about a problem at scale with the software in charge of evaluating the availability of the content that is uploaded to the social network, specifically, on a component that is responsible for deleting re-publications whose original content had been previously deleted. Strangely, it mainly affected those days in places where there were collective expressions of socio-political causes.

Other examples of software failures that resulted in the censorship of material related to the national strike are what happened on May 4, when the trending functionality on Twitter failed; or the one that took place on May 18 on Facebook where users of the social network reported the disabling of the option that allowed live broadcasts.

Finally, we highlight that the policy assumed by Facebook, as an internet intermediary, to recognize the soft-

[115] El Espectador. Represión en la calle, sensación de censura en redes. Accessed at: https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/represion-en-la-calle-sensacion-de-censura-en-redes-column/

[116] Revista 070. Los en vivo: estar vivos y ser vistos. Accessed at: https://cerosetenta.uniandes.edu.co/los-en-vivo-estar-vivos-y-ser-vistos/

[117] Fundación Karisma. #ParoNacionalColombia ¿Qué pasó con las historias de Instagram el 6 de mayo?. Accessed at: https://web.karisma.org.co/paronacionalcolombia-que-paso-con-las-historias-de-instagram-el-6-de-mayo/

[118] Infobae. Una falla técnica dejó sin visibilidad las publicaciones de usuarios de Instagram. Disponible en: https://www.infobae.com/america/tecno/2021/05/10/una-falla-tecnica-dejo-sin-visibilidad-las-publicaciones-de-usuarios-de-instagram/

[119] Official Instagram account. Tweets of May 6: https://twitter.com/InstagramComms/status/1390376354332487681?s=20 and https://twitter.com/InstagramComms/status/1390485897787883523?s=20

[120] Logically. Palestinians Bear The Brunt Of Big Tech Moderation. Accessed at: https://www.logically.ai/articles/no-platform-has-a-public-moderations-policy-for-war-zones

[121] Vice. Instagram Stories About Violence Against Indigenous Women Are Disappearing. Accessed at: https://www.vice.com/en/article/jg8843/instagram-stories-about-mmiwg-violence-against-indigenous-women-are-disappearing

[122] Official Instagram account. Tweet from May 7: https://twitter.com/GrupoPONALSAR/status/1392910787904147457?s=20

ware problem and its consequences through trills is a good practice that should be extended to other platforms in cases where problems with the software affect the exercise of rights of the users of these platforms.

4.4 A brief call for intermediaries to persist and deepen their transparency policy

During May 2021, and for the first time in the history of the protest in Colombia, problems related to internet access and connectivity as well as content moderation and flaws in social media software have been evident, and they have materialized thanks to the fact that in some cases we saw internet providers recognize the importance of providing public information about their actions.

Movistar and Emcali acted before the reports of internet shutdown in Cali on May 4 and 5, Instagram did it after the reports of blocking of stories on May 6, neither Twitter nor Facebook have said anything about what happened on May 4 and May 18, respectively. Nevertheless, although these transparency exercises are important, they are not generalized; they respond more to particular situations and, in addition, the information provided by private companies does not allow to determine the origin of the problems of access and use of the Internet during the protest, they allow determining that there were failures. Given that for political reasons or institutional design, the Colombian State has not determined the origin of the internet problems during the strike, a sense of censorship is created, where the only certainty is that there were problems.

Regarding moderation in social networks, the protest in Colombia confirmed that it is one issue that generates the most uncertainty among people who neither understand what is happening nor receive information about how platforms decide on the applicable rules in social networks during the protests. The little information they offer worsens when the software fails and impacts people at key moments of social mobilization.

Finally, despite the depth and breadth of the IACHR's references to the Internet in its observations and recommendations to Colombia document, it is striking that it did not make any mention or call to service providers to persist and deepen their transparency policies regarding the information related to the mediation and provision of internet service, a call that the U.N. and the IACHR itself have made on other occasions. We must not forget that the impact of possible requests made by the authorities to remove content or requests for information about their users in the framework of the strike that could be evidenced in the transparency reports remains to be seen.

CONCLUSIONS AND RECOMMENDATIONS

The general picture of rights in the digital environment during the National Strike is dark. On the one hand, there are multiple complaints of human rights violations in digital spaces, with no evidence of interest on the part of the State to investigate and punish those responsible. On the other hand, the opacity related to the powers to block, patrol, and signal on the Internet is total. The information in this regard from the State is null and what is known is thanks to citizen complaints, investigations by civil society organizations, or even statements from private intermediary companies that have assumed their duty of transparency.

With this opaque outlook, a situation of defenselessness seems to reign in citizens in the face of possible arbitrariness committed by the State. In any case, these are twelve recommendations to protect and promote human rights in the social demonstrations that are to come:

1. The creation by the State of an independent mechanism that periodically reports the status of the infrastructure related to telecommunications is necessary. In order to allow public scrutiny in contexts where internet quality and access to it are essential to protect other rights.

2. We urge the State, specifically law enforcement, to commit to not using signal jammers during protests and to create a policy that respects human rights regarding the transparent use and handling of this type of technology.

3. We demand both the Ministry of Information Technology and Communications and the Superintendency of Industry and Commerce not to deploy their functions of blocking URL, domains, or any other element of the Internet without ensuring that their actions comply with the requirements of legality, necessity, proportionality, and with due process as established by inter-American human rights standards.

4. The National Spectrum Agency should investigate complaints about interference (or not) of the signals during the demonstrations and in the most nerve-racking places of the protest, as long as no changes are made in the institutional framework necessary to protect the rights of citizens.

5. The National Police must adopt a policy that allows easy identification of drones and uncrewed aircraft in its possession. In addition, it must establish clearly and respectfully human rights protocols for the transparent and democratic use of these technologies.

6. It is necessary that the State as a whole, but especially the Ministry of Defense, refrain from participating, using, or promoting narratives that stigmatize digital protest, generalizing the use of expressions such as vandalism or digital terrorism, or pointing out citizen denunciations on the Internet and social media such as fake news. The State must provide information that contributes to public debate and understand its position as one of the main actors in the social crisis we face.

7. The State must evaluate its communications surveillance actions, including "cyber-patrolling" in the light of human rights standards, and adjust the norms of this activity to the criteria of legality, necessity, proportionality, and due process. In other words, law enforcement must adjust its actions to human rights standards

in all matters related to technology and telecommunications, especially concerning "cyber patrolling," "profiling," "cyber threats," and searches of cell phones.

8. In addition to regulating the use of force and weapons in the protest, the State must adapt the internal regulations on the technology used to control social protest to human rights standards. Signal inhibitors and facial recognition cameras, for example, are technology in the hands of the State and suspected of having been used.

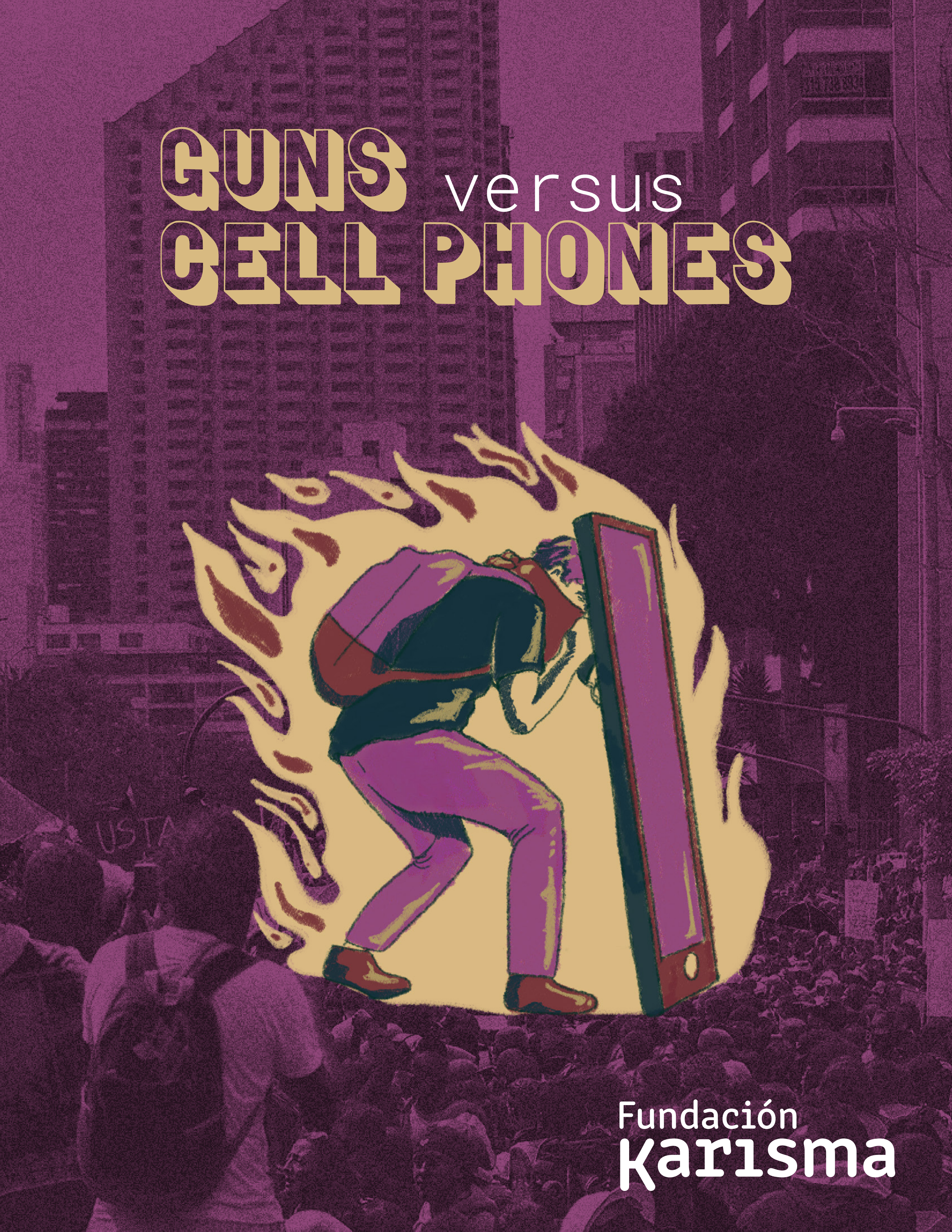
9. We call on the State to carry out the necessary legislative reforms to adjust its institutional framework to guarantee an independent and autonomous communications sector regulator; with functions of surveillance and control of the infrastructure (Internet and spectrum) that can make public enough information to guarantee public scrutiny.

10. It is necessary that all state entities, but especially those with functions of defense or promotion of fundamental rights, analyze the impact that technology has on the exercise of citizenship rights before presenting policies or making proposals regarding the control and management of social protest.

11. We request that internet service providers and online intermediaries, in exercising their responsibility with the people who use their services and under the principle of net neutrality, analyze any request for blocking or interference in the light of human rights standards.

12. In the same vein, we ask the platforms responsible for social media transparency about 1) the content moderation criteria that they use, especially when they can affect the protest and guarantee effective appeal mechanisms, 2) the information on measures used to escalate their responses in content moderation derived from the sudden increase in the use of these platforms during the protests and 3) on the failures in their infrastructures, applications or software, indicating origin and nature, in addition to the impact of the protest and the measures that are adopted to mitigate and prevent them from happening again.

GUNS versus CELL PHONES



Fundación Karisma