New technologies and their impact on the promotion and protection of human rights in the context of assemblies and peaceful protests: the situation of Latin America

I. Introduction

The organizations that sign this document are part of the "Al Sur" consortium, an organized group of 11 organizations from the civil society in Latin America that seeks to strengthen human rights in the digital environment.

This report will share information on how new technologies have enhanced human rights in the context of assemblies and peaceful protests in Latin America, but, at the same time, how the use of new technologies by local States sometimes undermine the rights of assembly and peaceful protests.

In this document, we will show relevant examples from several countries in our region that will configure a regional picture of the different uses of new technologies, including common challenges and opportunities. Based on that, we will recommend some relevant measures for States and stakeholders.

II. How technologies have facilitated the organization of assemblies including peaceful protests

- *Documentation of assemblies including peaceful protests*

Websites and social media have helped to document abuses in street protests in Latin America. This is the case of 1DMX.ORG in Mexico, a website that was born in the context of demonstrations in 2012[1] that was dedicated to informing and documenting abuses committed against the opposition to the former president Enrique Peña Nieto. The platform compiled photographs and videos made by the citizens, and refute the version official version on the facts.[2]

In this same line, “Rompe el Miedo” (Break the Fear) Network,[3] created by Articulo 19 Mexico, is a platform that aims to protect people through the documentation or observation of social or high-risk mobilizations. Through the use of social media, protesters, journalists, and NGOs use the hashtag #RompeElMiedo to document police aggressions and different pieces of information related to a rally as well.

In the context of the Brazilian protests organized at 2014 World Cup, social networks were used by the protesters “to report on the violent actions of the police by uploading photos and

[1] https://es.wikipedia.org/wiki/Disturbios_del_1_de_diciembre_de_2012_en_M%C3%A9xico
[2] https://www.derechosdigitales.org/7028/la-censura-politica-en-internet-es-real-el-caso-de-1dmx-org/
[3] https://coberturaderiesgo.articulo19.org/?cat=4

videos, as well as to respond to the distorted way in which the major television channels were covering events."[4]

#NiUnaMenos ("Not one [woman] less") is a hashtag that represents the feminist movement in Argentina, and it has become a viral hashtag across Latin America every time there is a massive demonstration against gender-based violence and femicide.[5] The hashtag was first used in peaceful protests held on June 3, 2015, in Argentina. In this country, there are also other exciting examples of how activists and organizations have responded in various ways to restriction on manifestations, using video to document and collect evidence to denounce violence by government forces.[6]

- *Organize, inform and amplify assemblies including peaceful protests*

There are many examples of how social networks have been critical to organize assemblies and peaceful protests, especially in movements led by young people, but also on how those platforms have been strategically used to inform and amplify movements to broader audiences. Here are some examples:

According to some researchers, in the Chilean student mobilization in 2006, well known as "Movilización Pingüina," the Internet was used by the movement to get information and to inform to other audiences, as well as to identify and coordinate activities.[7] In 2011, and very influenced by the "Movilización Pingüina," the "Chilean Winter Protests" came up, where students again raised for an educational reform.[8] In these protests, social networks helped to disseminate information, catalyze the movement, and support their activities.[9] Moreover, researchers in Chile have concluded that -in a context of mobilizations and social protests- there is a positive relationship between the use of Facebook and Twitter and the participation of young people, specifically in student mobilizations and protests against the construction of the HidroAysén dam.[10] In their investigation, they observed that, although online social media does not pose a reinvention of the way Chilean youth protest, at least they become a space for amplification of both the protests and the demands that motivate them.

In Mexico, Twitter was used to express dissatisfaction with the conditions in which the presidential elections of 2012 were held. This movement took advantage of two of the types of digital activism previously exposed: it facilitated a simple adhesion using the hashtag #YoSoy132 and summoned the protest in the public square through social networks.[11] For many authors, #YoSoy132 is a testimony on how digital tools and platforms operated as an

---

[4] http://generationeuropa.eu/?p=1103

[5] https://www.theguardian.com/world/2016/oct/20/argentina-women-south-america-marches-violence-ni-una-menos

[6] https://lab.witness.org/activists-argentina-use-videos-denounce-increasing-institutional-violence/

[7] https://www.redalyc.org/pdf/773/77325885012.pdf

[8] https://www.theatlantic.com/photo/2011/08/student-protests-in-chile/100125/

[9] https://dialnet.unirioja.es/servlet/articulo?codigo=5791963

[10] http://cip.udp.cl/medios/wp-content/uploads/2016/01/Capitulo_8-Scherman__Arriagada_y_Valenzuela_pp_181-199-libre.pdf

[11] https://www.derechosdigitales.org/wp-content/uploads/Internet-en-Mx-2016.pdf

informational counterweight and simultaneously generated interconnected options for online activism and street activism.[12]

In 2014 Mexicans reacted with outrage to the disappearance of 43 students from a rural teachers college in the city of Ayotzinapa and a government response that has failed to explain what happened entirely. Using the hashtag #YaMeCansé (I've Had Enough), people express their discontent to the extent that the hashtag was one of the most used labels, appearing on the list of global trending topics for more than a week. At the time, political scientist, John Ackerman, explained that while the current mobilization for the Ayotzinapa case stemmed from grassroots activism, "social networks have greatly helped spread and generalize their message and their causes, as well as to have the enormous international solidarity."[13]

Along the same lines, in Paraguay, the Twitter and Facebook platforms played a crucial role in student mobilization. The student mobilization arose as a result of the serious allegations of corruption in the administration of the National University of Asunción (UNA).[14] The hashtag #UnaNoTeCalles (UNA don't stay quiet) served to summon the protests that extended to all the faculty levels and transcended to other universities, both public and private. The massive demonstrations and vigils achieved the resignation of Rector Froilán Peralta and the initiation of investigations by the Unit of Economic Crimes and Anricottupción of the Public Ministry.

In the context of the protest fired up for the organization of the World Cup in Brazil, people in Rio de Janeiro were involved in massive protests in the streets.[15] According to researchers, the Internet was the primary tool for spreading information about the protests: 91% of people got information about the demonstrations through social networks. Facebook mainly "served both to organize and publicize the protests. It was common that a single event page for each city would be created, a page that would be updated for every new protest. Alternative pages regarding the same protest would also appear, each with its own internal discussion. As such, more than a platform for mobilization, Facebook was, during that period, a space for broad debate, with potential for confrontation and development of discourses".[16]

Moreover, studies in Brazil shows how "favela media activism" is boosted by the use of new media (e.g., Internet, smartphone applications) that is combined with artistic, educational and journalistic techniques to promote critical thinking and political mobilization in favelas.[17]

---

[12] http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-57952014000200004

[13] https://es.globalvoices.org/2014/11/22/yamecanse-la-indignacion-sacude-las-redes-sociales-en-ayotzinapa/

[14] https://www.ultimahora.com/bajo-el-lema-una-no-te-calles-convocan-manifestacion-este-jueves-n931060.html

[15] https://www.theguardian.com/world/2013/jun/21/brazil-police-crowds-rio-protest

[16] https://www.digitalrightslac.net/en/internet-y-democracia-las-manifestaciones-de-junio-en-brasil/

[17] https://blogs.lse.ac.uk/favelasatlse/2014/09/18/types-of-favela-media-activism/

- *Protect human rights that could be potentially affected by the action of States in the context of assemblies and peaceful protests*

New technologies have been used by activists to circumvent censorship and prosecution from governments in the context of demonstrations. Many of them have created guides for local people to, on the one hand, use new technologies to protect their human rights, and, on the other hand, to understand the risks that some of new technologies pose for assemblies and peaceful protests.

For example, in Brazil, with the excuse of guaranteeing order and controlling dissatisfied voices during the 2014 World Cup and the 2016 Olympics, the Brazilian government heavily invested in security gear and expanded its online data gathering capacity for intelligence purposes. In this context, Article 19 and other civil society organizations created Protestos.org, a website that provides information about technologies that might be used by protesters and activists in their struggle for freedom of expression rights and against violations, censorship, and abuses.[18] Some similar examples can also be found in Venezuela,[19] Colombia,[20] Mexico,[21] Nicaragua,[22] among others.

III. The human rights challenges posed by interferences with the availability and use of technologies in the context of assemblies, including peaceful protests.

- *Radio signal blockers*

In 2016, the National Telecommunications Agency of Brazil (Anatel) published the extract of Act No. 50,265, which authorizes the Brazilian Armed Forces to use Radio Signal Blockers - BSR's during the Olympic and Paralympic Games - Rio 2016, in test events and subordinates associated with them, as well as in Law and Order. The rule responded to a demand from CCOMGEX, the Brazilian Army's Electronic Warfare Communications and Electronic Warfare Center, to inhibit the use of not-authorized drones. However, BSR's can cause blackouts in telephone and internet signals in a given area, attacking human rights as communication rights, free speech, access to information, and the right to free assembly and

[18] https://protestos.org/index.html
[19] https://www.accessnow.org/venezuela-escapa-a-la-censura/
[20] https://sinmiedo.com.co/
[21] https://infoactivismo.org/riesgos-digitales-durante-y-despues-una-protesta/
[22] https://drive.google.com/file/d/12NCPWbzkO9sZaj1LAwQunL0-oQjepmXI/view

peaceful protests.[23] At the time, Lucas Teixeira of Coding Rights said: "Mobile phones and the internet are essential in this context of protests. Third parties' access to them would confuse and facilitate police violence, and it would hinder journalistic coverage".[24]

More recently, the Country's National Telecommunications Agency (Anatel) authorized the use of BSR's in locations such as President Jair Bolsonaro and Vice President Hamilton Mourao's official residencies, workplaces, or even areas where they "are imminent to be."[25] The authorization was given to the Office of Institutional Security of the Presidency, and the range of such blockages will extend through 200 meters from locations mentioned above. The measure will be active until December 31st, 2022 and "must be restricted to specific, episodic, urgent and temporary operations, in which concrete evidence of potential or imminent risk of actions necessary to preserve the security of the President of the Republic and the Vice-President of the Republic is identified."[26] As a public authority, this measure could be disproportionate as it could undermine the work of journalists but also the right to peaceful demonstration.

- *Cell-Site Simulators or IMSI Catchers (also known as Stingrays)*

The Cell-Site Simulators or IMSI Catchers are“devices that masquerade as legitimate cell-phone towers, tricking phones within a certain radius into connecting to the device rather than a tower.” According to Privacy International, “once connected to an IMSI catcher, mobile phones reveal information that can identify their users, and that process also permits the IMSI catcher to determine the location of the phones. Some IMSI catchers also can block or intercept data transmitted and received by mobile phones, including the content of calls, text messages, and web sites visited”.[27]

As specialists have acknowledged it, IMSI catchers are an unusual threat to the right to freedom of peaceful assembly as they conduct surveillance on all individuals within a particular physical area, de-anonymize those individuals, and even intercept and manipulate their communications and data. This is particularly worrisome in Latin America, where

---

23 https://www.cartacapital.com.br/sociedade/olimpiadas-no-brasil-201cpremiam201d-a-industria-da-vigilancia/

24 https://www.vice.com/pt_br/article/3dp8wy/como-o-brasil-aprimorou-seu-aparato-de-vigilancia-social-para-as-olimpiadas

25 https://www.telecompaper.com/news/anatel-permits-mobile-signal-blocking-to-protect-bolsonaro-and-vice-president--1312082

26 https://static.poder360.com.br/2019/10/ATO-No-6.277-DE-8-DE-OUTUBRO-DE-2019-ATO-No-6.pdf

27 https://www.ohchr.org/Documents/HRBodies/CCPR/GCArticle21/PrivacyInternational.pdf

governments have already purchased this technology, like Mexico,[28] Colombia,[29] and Brazil, at the occasion of the World Cup.[30]

- *Internet shutdowns*

According to Access Now, "an internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do."[31] Many of these internet shutdowns have happened in Latin America, especially in the context of social protests against governments.

Internet shutdowns have occurred in Latin America. In Venezuela, for example,[32] where the Nicolás Maduro's government in Venezuela "has a long history of using internet shutdowns and other forms of censorship to suppress opposition voices and limit the flow information within the country, particularly at moments of heightened tension," according to Access Now.[33] Moreover, Derechos Digitales made a technical analysis of these attacks, affirming that they have increased their complexity in time.[34]

In 2018, the NetBlocks internet observatory detected a series of regional internet outages and disruptions coinciding with widespread protests and violence in Nicaragua.[35] The same organization also recently discovered "that social media backend image and CDN servers were temporarily disrupted in Ecuador with state-run operator Corporación Nacional de Telecomunicaciones (CNT) on Monday, 7 October 2019 amid a spiralling political crisis and widespread protests".[36] The government rejected these reports, but Internet Service Providers, as Telefónica Movistar, acknowledged interferences in its services.[37] Blocking web services are not new in Ecuador. In 2016, an internal document from Telefónica Movistar, revealed by the Ecuadorian journalism platform "Ecuador Transparente", evidenced that the

---

28 https://mx.boell.org/es/2017/03/17/instituto-federal-de-telecomunicaciones-ignora-simuladores-de-torres-moviles

29 https://privacyinternational.org/report/991/shadow-state-surveillance-law-and-order-colombia

30 https://www.vice.com/pt_br/article/3dp8wy/como-o-brasil-aprimorou-seu-aparato-de-vigilancia-social-para-as-olimpiadas

31 https://www.accessnow.org/keepiton/

32 https://vesinfiltro.com/noticias/alert-2019-04-30/

33 https://www.accessnow.org/social-media-shutdown-in-venezuela-is-a-warning-of-what-is-to-come-as-political-tensions-rise/

34 https://www.derechosdigitales.org/12791/venezuela-que-esta-pasando-con-los-bloqueos-en-internet/

35 https://netblocks.org/reports/nicaragua-regional-internet-disruptions-amid-protests-gdAmMvA9

36 https://netblocks.org/reports/evidence-of-social-media-disruptions-in-ecuador-as-crisis-deepens-oy9RN483

37 https://www.eluniverso.com/noticias/2019/10/11/nota/7556084/cnt-descarta-bloqueos-redes-sociales-movistar-denuncia-afectacion

Ecuadorian government could block access to websites in the country without any previous court order.[38]

IV. The human rights challenges posed by the use of new technologies, including ICTs, in the context of assemblies, including peaceful protests.

- *Facial recognition*

This technology facilitates the capture, storage and processing of people's biometric information, that is, their biological, morphological and behavioral traits, which are then converted into a comparable matrix or template that can be read by computers. Once these digital templates are linked to a person's profile, they can be used to verify identity in a process of probabilities and not certainties. As the Asociación por los Derechos Civiles (ADC) acknowledges: "In the case of facial recognition, algorithms responsible for finding similarities between templates with facial features may contain biases derived from their programming and / or training."[39]

As Privacy International acknowledges, this technology "has been used in protests but also in other public gatherings, music concerts and football matches, shopping centres and high streets, and festivals. There is a valid concern that it could eventually be rolled out across all public spaces". According to Coding Rights, Brazilian activists suspected that they have been under surveillance at demonstrations because of the use of facial recognition goggles.[40] That's why many civil society organizations across Latin America are worried about facial recognition effects on freedom of assembly and peaceful protest, as this technology is already present in Chile,[41] Mexico,[42] Colombia,[43] Paraguay,[44] Ecuador,[45] Argentina,[46] among many others.

---

38 https://www.enter.co/chips-bits/seguridad/gobierno-de-ecuador-habria-bloqueado-ilegalmente-varios-sitios-web/

39 "Tu yo digital", Asociación por los Derechos Civiles (ADC), Fundación Karisma, InternetLab, Red en Defensa de los Derechos Digitales (R3D), abril de 2019, disponible en: https://adc.org.ar/wp-content/uploads/2019/06/050-tu-yo-digital-04-2019.pdf

40 https://chupadados.codingrights.org/en/sai-para-cacar-equipamentos-de-vigilancia-no-rio-olimpico/

41 https://www.msn.com/es-cl/noticias/chile/los-drones-polic%C3%ADa-con-reconocimiento-facial-que-vigilar%C3%A1n-santiago-las-24-horas-del-d%C3%ADa/ar-BBUW9Z4?li=AAggXBX&parent-title=%C2%BFpor-qu%C3%A9-nos-da-sue%C3%B1o-despu%C3%A9s-de-comer&parent-ns=ar&parent-content-id=AAowh6S

42 https://www.sinembargo.mx/13-08-2019/3628039

43 https://noticias.canalrcn.com/nacional-bogota/asi-funciona-el-sistema-reconocimiento-facial-se-implementa-transmilenio

44 https://www.tedic.org/biometria-y-video-vigilancia-la-enajenacion-continua-de-nuestros-derechos-parte-2/

45 https://www.metroecuador.com.ec/ec/noticias/2019/07/02/camaras-reconocimiento-facial-quito.html

46 https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

In Paraguay, TEDIC requested details of the facial recognition software implemented in more than 100 cameras over the country, as well as the purpose of the implementation, the data retention period, and their impact assessment on human rights. Finally, the information was denied by the Ministry of Security, claiming that the information was a part of national security. Given that the law requires that anything that constitutes national security has to be determined by a specific law (which is not the case), TEDIC presented an action of unconstitutionality for manifest arbitrariness, among other arguments in order to defend privacy and freedom of speech.[47] This situation creates insecurity concerning the rights mentioned above, as far as not knowing how the software works, it is not possible to determine the extent of how the right to protest would be affected.

In Colombia, Fundación Karisma researched about a facial recognition system designed and probed in the public transportation system Transmilenio in 2016, but the system failed thanks to the lack of a central database to compare[48]. Likewise, since 2016, the National Civil Registry started the consolidation of a database for facial recognition using the photos from the National ID System. In 2017, the National Police and the Colombian government bought a facial recognition system called BioFinder developed by the firm Hertha to identify citizens in public and private surveillance systems and recognize individuals during their patrolling activities using devices designed by the French company IDEMIA[49].

- *Drones*

Drones are also on the agenda of public officials. In Rio de Janeiro, the program "Sentinela Carioca" imposes the use of drones to monitor "crowded places and large events."[50] The program allows drones to be flying over the capital of Rio de Janeiro, collecting information from cars, buildings, and, of course, people - which can jeopardize the citizens' right to privacy and informational self-determination. One possible application to the RPAs (Remotely Piloted Aircrafts) would be for monitoring traffic and eventually collecting data on vehicle registration plates. However, the purpose of which the images will be collected is still unknown. The most noteworthy assignment to the program is the one related to the supervision of communities and favelas.

Besides, using such technologies without the necessary guarantees of transparency and regulation opens space for other rights to be violated. For example, there is no guarantee that drones could not be tracking demonstrations and activists who participate in activities at the public place (the collected information can be crossed-over with the already existing archives in intelligence centers and police forces about activists). In Chile, during recent years, different local authorities in Santiago province have implemented the use of unmanned spacecraft - such as surveillance balloons and drones - equipped with high-resolution

[47] https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/
[48] https://karisma.org.co/?wpdmdl=8291
[49] https://archive.org/details/biometria2
[50] Tamari, Mariana. (November, 2018) Em dezembro, sem saber, estaremos “dando close” para drones sentinelas. Carta Capital. Available at: https://old01.cartacapital.com.br/blogs/intervozes/emdezembro-sem-saber-estaremos-201cdando-close201d-para-drones-sentinelas

cameras in massive surveillance programs intended to provide public safety.[51] In the same lines, drones have been used to surveil constantly and repress indigenous communities in the south of the country in recent years.[52]

- *Social media intelligence (SOCMINT)*

Just days before the XI Ministerial Conference of the World Trade Organization (WTO) in Argentina, 64 human rights defenders and activists from 21 civil society organizations were notified by the WTO that although they had been accepted and duly accredited to participate in the Conference, authorities had decided to deny their accreditation. In a statement from December 2017, the Ministry of Foreign Affairs justified this decision by establishing that some of the registrants "had made explicit calls to manifestations of violence through social networks, expressing their vocation of genetics schemes of intimidation and chaos."[53]

This is just one example in the region of the use of Social media intelligence (SOCMINT) by States. SOCMINT refers to the collection of tools that allow governments to monitor social media channels, conversations, and internet use, including monitoring of content and other data.

These techniques have also been used by police in intelligence labors. In Brazil, for example, the police used Tinder (a dating app) to spy on activists, infiltrate the movements, and stop protests in the context of the national protests in 2016.[54] More recently, different reports from media outlets have informed the use of social media by the police in Chile (Carabineros) to infiltrate indigenous communities in the south of Chile to inform new mobilizations, among other aspects.[55]

According to ADC (Argentina), the use of SOCMINT must be discussed in-depth and before any public policy implemented by the States concerning its exploitation. In its adoption, States should be concerned about how to protect fundamental rights such as privacy and freedom of expression, assembly, and association, including the role of the private sector.[56]

In this same line, Privacy International has stated, "the unregulated use of SOCMINT negatively affects the exercise of the right to freedom of peaceful assembly. It has a chilling effect on individuals wishing to organise online, as well as using social media platforms to organise and promote peaceful assemblies. Furthermore, the degree of intrusiveness does

---

[51] K. González and D. Aguayo. (April, 2017). Las Condes inicia vigilancia con drones. Available at: https://www.latercera.com/noticia/las-condes-inicia-vigilancia-drones/

[52] https://indigenoussurveillance.net/wp-content/uploads/2019/08/Tipos-de-vigilancia_Drones_IndigenousSurveillance_V1.pdf

[53] https://cancilleria.gob.ar/es/actualidad/comunicados/sobre-la-acreditacion-de-ongs-la-conferencia-ministerial-de-la-omc-en-buenos

[54] https://www.vice.com/en_us/article/78kdga/spies-use-tinder-and-its-as-creepy-as-youd-think

[55] https://ciperchile.cl/2019/08/08/informes-reservados-de-carabineros-asi-se-infiltran-los-agentes-encubiertos-en-la-zona-mapuche/

[56] https://adcdigital.org.ar/wp-content/uploads/2018/10/Seguidores-que-no-vemos.pdf

not only constitute an unlawful interference with the right to privacy, but it also directly undermines the exercise of freedom of peaceful assembly".[57]

- *Using new technologies to persecute members of social organizations and movements*

Several examples of States using new technologies to undermine the right of assembly can be found in Latin America.

In Chile, for example, Operación Huracán, an investigation conducted by the Carabineros (Chile's police force), was convened to investigate supposed links between leaders from Mapuche indigenous communities and illicit terror organizations in the southern Araucanía region. After a great media coverage, the operation led to the arrest of eight Mapuche leaders in September 2017. Carabineros said that they were capable of breaking the encrypted messages of applications such as WhatsApp. The Prosecutor's Office later found that the eight Mapuches arrested were charged based on fake evidence which the Carabineros themselves had planted on the mobile telephones of the community members.[58] This implantation was possible because of the use of software, Oxygen Forensic, especially purchased by Carabineros for this operation.[59]

In Mexico, an intrusive malware called "Pegasus", (commercialized by the Israel-based company NSO Group) has been used by several governmental agencies to target journalists, human rights defenders, lawyers, public health and anti-corruption activists as well as the international body of independent experts appointed to investigate the disappearance of the 43 students from Ayotzinapa in 2014.[60] In June 2017, the seriousness of the case drove

---

[57] https://www.ohchr.org/Documents/HRBodies/CCPR/GCArticle21/PrivacyInternational.pdf

[58] https://www.derechosdigitales.org/wp-content/uploads/tecnologia-y-vigilancia-en-huracan.pdf

[59] https://indigenoussurveillance.net/wp-content/uploads/2019/08/Tipos-de-vigilancia_Hackeo-electronico_IndigenousSurveillance_V1.pdf

[60] Artículo 19, Citizen Lab, R3D: Red en Defensa de los Derechos Digitales, SocialTIC. (junio 2017) Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México. Disponible en: https://r3d.mx/gobiernoespia/ ; R3D. Destapa la Vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental. Disponible en: https://r3d.mx/2017/02/11/destapa-lavigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/ ; Perlroth, Nicole (11 de febrero de 2017) Spyware's Odd Targets: Backers of Mexico's Soda Tax. The New York Times. Disponible en: https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?smid=fbshare&_r=0 ;Ahmed, Azam. Perlroth, Nicole. (June 19, 2017) Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families. The New York Times. Disponible en: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html ; Ahmed, Azam. (August 30, 2017) Un empresario activista lucha contra la corrupción en México y se convierte en un blanco del Estado. The New York Times. Disponible en: https://www.nytimes.com/es/2017/08/30/mexico-pegasus-claudio-x-gonzalez-laporte-enrique-peniaeto-corrupcion/ ; Ahmed, Azam. (July 10, 2017) Spyware in Mexico Targeted Investigators Seeking Students. The New York Times. Disponible en: https://www.nytimes.com/2017/07/10/world/americas/mexico-missing-students-pegasus-spyware.html

diverse UN Special Rapporteurs to call upon Mexico to establish an independent and impartial investigation into the deployment of Pegasus. This has also been a reiterated demand from the victims. Nevertheless, to date, the outgoing and entering governments have failed to recognize the establishment of guarantees of such an investigation, and the ongoing criminal proceedings have shown little to none progress.

In Colombia, communications interception scandals (sometimes called by the Colombian Spanish term *chuzadas*) have been a feature of security politics since the 1990s with stories of the illegal interception of private communications by different agencies. In 2009, Special strategic intelligence groups of the DAS conducted targeted surveillance of an estimated 600 public figures including parliamentarians, journalists, human rights activists and lawyers, and judges among others. According to files retrieved during an investigation by the Fiscalía, the DAS intercepted phone calls, email traffic, and international and national contacts lists, using this information to compile psychological profiles of targets and conduct physical surveillance of subjects and their families, including children[61].

It is essential to mention that private companies are also deploying very pervasive surveillance technologies against Latin American citizens. In Brazil, Vale S.A. is alleged responsible for surveilling land rights defenders and environmental activists, as well as journalists and it's own workers, to avoid denounces of several human rights violations and the social-environmental impact that occurs in their businesses.[62] That is the case of other companies as well, such as Anglo American, another mining company accused of surveil and threat citizens of Conceição do Mato Dentro,[63] where the company is being exposed by community leaders who are critical about the construction of a giant dam.[64]

- *Bots on social media*

Bots are armies of automated social media accounts, especially on Twitter, that generate junk messages (spam) associated with hashtags to inflate reachability of specific messages on social media artificially. Some evidence of the use of bots in the context of protests has been studied in Latin America.

In Mexico, for example, researchers Erin Gallagher and Alberto Escorcia studied bots from the former Enrique Peña Nieto. They discovered that these government-bots closely followed hashtags used by protesters to drowning out real conversations with noise: "They've also

---

[61] https://privacyinternational.org/state-privacy/58/state-privacy-colombia
[62] Pozzebom, Elina Rodrigues. (October, 2013). Vale espiona líderes e se infiltra em movimentos sociais, diz ex-funcionário. Senado Noticias. Available at: https://www12.senado.leg.br/noticias/materias/2013/10/24/vale-espiona-lideres-e-se-infiltra-emmovimentos-sociais-diz-ex-funcionario
[63] Sant'anna, Daniel. Maciel, Alice. (March, 2018). AGRESSÕES, VIGILÂNCIA, DESEMPREGO, PERSEGUIÇÃO E ISOLAMENTO: COMO VIVEM OS MORADORES QUE ENFRENTAM A GIGANTE DA MINERAÇÃO. Intercept Brasil. Available at: https://theintercept.com/2018/03/27/ameacas-moradores-mineracao-anglo-american/
[64] Ferraz, Lucas. (January, 2018). Anglo American quer barragem quatro vezes maior que a de Fundão, que rompeu em Mariana. Pública. Available at: https://apublica.org/2018/01/a-sombra-datragedia-de-mariana-video/

seen similar bots create fake hashtags in apparent attempts to push real hashtags out of Twitter's trending list, spread anti-protest messages, and even send death threats to specific activists."[65]

In Brazil, in the context of the Dilma Rousseff's impeachment, researchers analyzed the discussion on Twitter on the days of the pro-impeachment demonstrations: according to FGV, "at least 10% of the interactions about the subject on this day were stimulated by bots, that is, retweets of content originated in an automated account. In the cluster of Dilma Rousseff supporters, this proportion reached 21.43%, which shows the power of influence that this type of account has on the political debate".[66] Another study showed that pro-government protests in March 2015 made use of bots on Twitter, inflating their impact.[67]

- *Spreading of misinformation and disinformation*

Social media can be a significant channel to spread misinformation and/or disinformation in the contexts of protests in Latin America. This could hurt the credibility of the demo organizers, the peaceful surroundings of a protest, produce intentional confusion, etc.

In Brazil, volunteers and influencers in social media and message apps as WhatsApp crate and share fake news and coordinate protests online and in the real world.[68] More recently, amid the Ecuadorian protests from October 2019, media outlets have denounced the use of misinformation[69] and disinformation[70] in social media. More examples in countries in Latin America can be found here[71] and here.[72]

V. Laws, policies and programs that have been developed to address the impact of new technologies in the context of assemblies, including peaceful protests.

It could be stated that in Latin America, the majority of bills, laws, policies, and programs presented by states haven't had the intention to boost the right of assembly and peaceful protest in the context of the use of new technologies. On the contrary, many of them have been seen as dangerous for human rights.

One notable example is the case of a bill from 2014 for a new telecommunications law (Ley Telecom) in Mexico. This bill gave power to the state to block and censor communications

[65] https://www.wired.com/2015/08/pro-government-twitter-bots-try-hush-mexican-activists/
[66] http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/
[67] https://ieeexplore.ieee.org/document/7427441
[68] https://www.theguardian.com/world/2018/oct/25/brazil-president-jair-bolsonaro-whatsapp-fake-news
[69] https://www.elcomercio.com/actualidad/jaime-nebot-imagenes-falsas-fakenews.html
[70] https://www.eluniverso.com/noticias/2019/10/10/nota/7555010/noticia-falsa-fake-news-jose-mujica-twitter-falso-lenin-moreno
[71] http://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf
[72] https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/

deemed a threat to public order and national security.[73] The bill gave the government the ability to mandate telecommunications companies to temporary block or disable phone, radio, and internet connections, in areas where public protests or demonstrations are occurring. Luis Fernando García from Red en Defensa de los Derechos Digitales (R3D), warned that this would mean "turning off the communications switch to prevent the organization of protesters and the denounce of human rights violations during the protests." [74] After social mobilization, this specific part of the bill was dismissed. Moreover, violations of privacy and barriers to freedom of expression through arbitrary and illegal surveillance and anonymity restrictions are clear examples of the obstacles the region is dealing with regarding the exercise of the right to peaceful assembly. Several bills have been introduced in Argentina, as well as in Chile and Guatemala, to create a new criminal offense of expression: the usurpation of digital identity.

Another case is the National Code of Police and Coexistence in Colombia that entered into force in 2017. The new code expands police powers through several provisions designed to "solve the conflicts that affect the coexistence" of Colombians. It includes several provisions that have particularly negative implications with regards to the right to privacy and their collective interpretation, which can lead to a state of surveillance. For example, Article 139 defines public space in a very broad way, including notably "the electromagnetic spectrum". The combined result of these definitions is of significant concern when considering that Article 237 could mean that communications traveling through the electromagnetic spectrum would be excluded from privacy protection. The provision has since been challenged in court[75].

Another policy that introduces a considerable limitation on free assembly and peaceful protest is mandatory SIM card registration schemes. Such policies directly undermine anonymity, especially for people who can only access the internet through their mobile devices. As the UN Special Rapporteur on Freedom of Opinion and Expression stated in his 2015 report, "Compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest."[76] The GSM Association has reported on collateral effects of SIM registration, such as the upsurge of illegal markets for buying and selling stolen or fraudulently registered SIMs; restricting the access to mobile communications through the limitation of the stores where SIM cards can be acquired; and the loss of communication services when SIM cards are not registered before the mandatory deadline.[77]

There's little evidence to sustain that mandatory SIM card registration leads to a reduction in crime, given how these schemes can be eluded, be it by the use of fake IDs, identity theft, or

---

[73] https://www.derechosdigitales.org/wp-content/uploads/Internet-en-Mx-2016.pdf
[74] https://elpais.com/internacional/2014/04/09/actualidad/1397067088_298059.html
[75] https://privacyinternational.org/state-privacy/58/state-privacy-colombia
[76] A/HRC/29/32, May 2015, page 19. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A_HRC_29_32_en.doc
[77] https://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf

merely exchanging phones. Likewise, the lack of a registry is not related to an increased risk of illegal activities or terrorism. Countries such as Colombia,[78] Peru[79] and Argentina[80] have implemented mandatory SIM card registration policies, while others like Mexico tried it in 2009 and was later abrogated given that it did not contribute to the prevention, investigation or prosecution of related crimes.

VI. Some recommendations

- The use of technologies such as IMSI Catchers and automated facial recognition in public spaces are inherently restrictive of peaceful assemblies. States must advance to recognize the right of peaceful assembly in a democratic society and regulate the acquisition and use of such technologies.

- Facial recognition technologies are increasingly being used to monitor public spaces, including demonstrations. Such use of facial recognition technologies may involve the widespread and bulk monitoring, collection, storage, analysis, or other use of the material and not be based on individualized reasonable suspicion; therefore, it could be considered a form of indiscriminate mass surveillance. To protect the human rights of people in assemblies and peaceful protests, States should regulate the use of these technologies based on principles of legality, proportionality and necessity.

- Any measure that restricts freedom of expression or association as internet shutdowns must remain exceptional, be grounded in law, and be strictly necessary and proportional to achieve a legitimate aim. Also, States should be transparent and deliver justifications on how, why, and when government agencies may opt for a disruption of access. At the same time, Internet Service Providers (ISPs) should challenge illegal internet shutdowns requests from governments and inform of this to their customers. The legitimate duties to safeguard public order and national security are not sufficient justification by themselves to restrict communications.

- States must advance to regulate the use of SOCMINT techniques (by them as by third parties) as they could intervene in the right of peaceful assembly online. Law Enforcement Agencies and other security bodies should act based on transparent protocols that outline who, when, and how such techniques will be deployed and used. The regulations on this matter must also include policies for accountability and mandatory prosecution due to the abuse of such technologies by government officials.

- States must advance in the effective protection of personal data, including to prevent its misuse by state institutions, and its overbroad accumulation and processing by

[78] Decree 1630/2011, Ministerio de Tecnologías de la Información y las Comunicaciones, Colombia, available at: https://www.mintic.gov.co/portal/604/articles-3558_documento.pdf
[79] https://hiperderecho.org/2019/06/registro-obligatorio-de-tarjetas-sim/
[80] https://adc.org.ar/2016/11/11/preocupaciones-acerca-del-registro-de-identidad-de-usuarios-de-celulares/

private actors that can be ultimately used by states to persecute protestors and demonstrators. While at the same time facilitating the exercise of data subject rights to access, rectification, cancellation and opposition, for technology users to be certain of the collection and processing by State agencies of their personal information shared online.

- States must implement the appropriate legislative framework to regulate and impose limits on the State usage of surveillance technology, which must include the establishment of necessary safeguards against abuse including:

➔ Specific regulation on the use of surveillance tools like hacking, malware, drones as well as biometric technologies, which incorporates the principles of necessity and proportionality.
➔ Independent judicial authorization and oversight mechanisms.
➔ Regulations that ensure that the use of private surveillance technology is auditable by oversight bodies.
➔ Transparency regarding the general surveillance capabilities of the State and meaningful information regarding the scope and extent of the use of private surveillance technology.
➔ Ensure that individuals that are targeted with private surveillance technologies are eventually notified and have access to a remedy.