Telecommunications and Internet Access Sector: Latin America

Report to the Special Rapporteur on the Protection and Promotion of the Right to Freedom of Expression of the United Nations

Derechos Digitales[1]

Executive summary

The infrastructure aspects of internet access are frequently overlooked when discussing human rights. However, policies and practices regarding the way internet networks and related services are handled and administered can affect heavily the ability of users to communicate and express themselves online in a safe, private and fair environment.

While internet access rates have grown rapidly in Latin America, access gaps have subsisted across every country in the region, along with other factors that create differences in people's opportunities to get online, such as economic imbalances, race, gender and geographical location. Meanwhile, monopolistic practices, government inaction and the unfair attribution of the radio-electrical spectrum contribute to the perpetuation of these gaps. Moreover, in countries where governments exert control over DNS and IXP administration, there are additional risks for content filtering and extensive communication surveillance. At the same time, the fragility of the underlying infrastructure creates risks in user's ability to access online networks in a consistent and reliable manner. Electricity outages and network shutdowns are not infrequent and leave citizens without any alternative for remaining connected.

Although data collection and retention standards vary widely across the region, in general ISPs are considered responsible for storing and delivering data related to users' activity and communications to law enforcement officers. Low standards for the protection of these data, lack of transparency in the way they are stored, handled

[1] This report was authored by Marianne Díaz Hernández, public policy officer at Derechos Digitales.

and shared, lack of accountability mechanisms for the users to exert control over their personal information, and the ability for ISPs to act as subsidiary law enforcement in order to avoid penalties against themselves, are only a few of the risks these practices entail for the citizens' privacy and freedom of expression.

1. Introduction

This report presents a summary of instances of state regulations, measures and arrangements that affect the way citizens access telecommunications and Internet networks and services in Latin America, how they influence telecommunication companies, ISPs and associated businesses' practices regarding access to internet networks, and their impact on freedom of expression in the digital context. While not intending to provide a comprehensive analysis about all the different implications of legal and extralegal measures that regulate telecommunications and their impact on freedom of expression in the region, this report aims to provide an approximation to the issue at hand and its ramifications in Latin America.

The state of internet connectivity and the environment for ISPs and telecommunication companies varies widely between countries in Latin America. Factors as cost, availability, quality and coverage differ not only from one country to another, but also within each national territory, causing access gaps that separate urban from rural capabilities, along with imbalances caused by economic status, gender, race, and other factors. In this context, legal and extralegal measures taken by the States can limit in many ways private companies' ability to respect and ensure online freedoms. ISPs and associated businesses can be forced to comply with measures to take down or block content, or even to implement shutdowns of internet and phone services. Regulations can also require intermediaries to retain personal data from their users and turn it over to state actors, or even to implement surveillance technologies and communication backdoors, thus affecting freedom of speech and privacy.

Latin America has the fastest growing internet connected population in the world[2], and mobile penetration is an extremely important mechanism to access the internet all over the region, with average penetration rates of more than 100 % for mobile, while keeping a low fixed broadband penetration rate[3].

2. Access

2.1. Access gap. Infrastructure and cost.

Fixed broadband and mobile internet penetration has advanced very rapidly in Latin America through the last several years[4]. However, important barriers still persist in relation to infrastructural development and connectivity cost. While telecommunication rates have experienced important reductions that mean that the average income per mobile subscriber has lowered significantly between 2004 and 2015, there are still significant income barriers that affect middle and lower classes' ability to access the internet in a consistent, reliable manner. Meanwhile, the cost of infrastructure deployment for ICT companies and access to devices for citizens remains high, meaning that governments need to step up and assume responsibilities in widening and deepening access, which not only means subsidising infrastructure deployment for the private sector, but possibly reducing tax impositions in internet costs for lower classes, particularly in countries where these costs are high (for instance Argentina, where about 24 % of the total cost per month of mobile broadband access correspond to taxes).

According to CET.la, the ICT market at the base of the pyramid cannot be appropriately served by the economic structure of the mobile business in the region[5]. Mobile internet penetration in Latin America has skyrocketed in the last years[6], but

---

[2] The Park Group (2015). Social Media in Latin America 2015
http://www.thesparkgroup.com/social-media-latin-america-2015/
[3] Analysis of ITU Spectrum Recommendations in the Latin America Region – 4G Americas - August 2013.
http://www.4gamericas.org/files/4614/0758/9072/Analysis_of_ITU_Spectrum_Recommendations_in_Latin_America-August_2013.pdf.
[4] KATZ, Raúl: Iniciativas para el cierre de la Brecha Digital en América Latina. Centro de Estudios de Telecomunicaciones de América Latina. http://cet.la/download/93/
[5] KATZ, Raúl, Ibid.
[6] UN, CEPAL: Estado de la banda ancha en América Latina y el Caribe 2016
http://www.cepal.org/es/publicaciones/estado-la-banda-ancha-america-latina-caribe-2016

one of the main reasons is precisely the socioeconomic and the rural gap: people who can't access fixed broadband at home (be it because of installation costs or just because of geographical unavailability) will end up connecting through prepaid mobile phones, and thus paying a much higher data cost in the long term, while enjoying a lesser-quality service.[7]

Most Latin American countries have plans or policies regarding universal access, and the majority of them consider that the development of fibre-optic infrastructure is an essential step toward bridging the gap, however, the approach towards this development varies. While Argentina and Brazil consider that governmental presence in infrastructure development is strategic and essential, other countries, like Colombia, consider that their role must be as facilitator and enabler for private development[8] (through incentives and fiscal measures).

2.2 Spectrum attribution and allocation

The ways in which the electromagnetic spectrum is handled, administered, licensed and priced affect users ability to access the internet. High spectrum prices and short term licenses may influence negatively the providers' ability to invest in infrastructure development and to recover those investments in a timely manner[9]. Uncertainty and unpredictability in terms of how licenses over spectrum are granted and renewed create an unstable climate for investment. In Latin America, there are different processes in place for how licenses over the spectrum can be granted and renewed, and the duration varies widely (from 30 years in Chile, to 5 years in Paraguay). While in some places, like Guatemala, the only requirement for license renewal is that the spectrum allocated is currently being used, in many places the authority that can grant or deny the permit is an administrative body with relative independence, which can have negative consequences in cases where the procedure is not transparent or straightforward enough. In Venezuela, for instance, spectrum allocation has been used as a mean for political retaliation -particularly in those cases

[7] APC, Spectrum use in Latin America: Supplementary summary report. www.apc.org/es/system/files/ca_sintesis_final_EN-EDITED-F.pdf
[8] APC, Ibid.
[9] GSMA: Spectrum in Latin America, January 4, 2016 http://www.gsma.com/latinamerica/spectrum-in-latin-america

where telecommunication companies are linked to media- or as a way to exert pressure over ISPs in order to make them comply with extralegal measures on surveillance or data retention. Meanwhile, other countries have or had irregular procedures that granted authorities a great leeway allowing them to administer the spectrum without previous public tender, a practice that has been denounced as opaque and unfair[10]. Public standard and procedure setting processes are also either non existent or just uneffective; these decisions are mostly taken directly by the regulatory agencies, which are often tightly ruled by the Executive branch. The tendency is to consider the spectrum as communal asset under supervision of the State[11], however decision making processes are often considered technical and strategical issues that are mostly handed in private by regulatory agencies with very little to no public consultation at all, and thus end up favoring certain economic and political interests.

In many places, large companies cannot guarantee an investment in return that will push them to develop infrastructure for connectivity in poorer areas, particularly in rural sectors, given that the population cannot pay for higher prices that would allow the providers to recover that investment. In order to bridge this gap, measures need to be taken by States to foster the development of infrastructure, which in some cases might mean providing local initiatives with access to the spectrum at costs that make those initiatives viable. An example of these initiatives is the Mexican indigenous Telecommunication Community, a nonprofit that was granted two licenses to operate telecommunications networks by the Mexican Federal Institute of Telecommunications[12]. These populations used to rely on high-cost landline phone booths, and cell phone companies refused to provide service in the area. After this initiative, the organisation installed a cellular network, providing the community

---

[10] MARTY, Belén. "Gobierno de Ecuador revisará más de 300 frecuencias de radio y TV". October 22, 2015. https://es.panampost.com/belen-marty/2015/10/22/gobierno-de-ecuador-revisara-mas-de-300-frecuencias-de-radio-y-tv/

[11] APC, Ibid.

[12] Salazar, Giovanna: "So Long, Phone Companies. Mexico's Indigenous Groups Are Getting Their Own Telecoms." July 26, 2016. https://globalvoices.org/2016/07/26/so-long-phone-companies-mexicos-indigenous-groups-are-getting-their-own-telecoms/

with a service that costs up to 98% less than what they could access through other providers. Public policies that allow for assignation of currently unlicensed frequency ranks and white spaces for community initiatives would provide opportunities for lowering connectivity costs and diminishing the rural gap.

Expectations that the transition to digital television would leave available the upper segment of the UHF band, which could then be re-assigned to mobile services, allowing providers to meet increased demand and traffic growth in the region, seem to still be open to consideration. No Latin American country has completed the analog switch-off process yet. The GSMA Foundation claims that if the Digital Dividend were to be assigned to mobile operators in Latin America, the service coverage would increase to up to 93% of the population[13].

2.3 Monopoly practices and market concentration

The telecommunications market in Latin America has been traditionally characterised by the existence of monopolistic and oligopolistic practices, particularly in large markets such as Brazil and Mexico. Just ten years ago, the Spanish firm Telefónica and the Mexican corporation Grupo Telecom, owners of Telmex and América Móvil, controlled 64% of the regional mobile market[14]. It seems that in some countries the tendency is moving towards a more competitive market[15], opening up spaces for smaller companies to compete after a series of mergers and acquisitions. Mexico has struggled for a very long time against Carlos Slim's monopolistic practices, and has hardened its laws and upped its sanctions against monopolies in telecommunications.

On the other side of the spectrum, public ownership of telecommunication companies, like in Cuba[16], creates a State monopoly in telephone, data, and television markets. Meanwhile, in Venezuela, a combination of a near-monopoly in

---

[13] GSMA, Ibid.
[14] MARISCAL, Judith: "Market Structure and Penetration in the Latin American Mobile Sector". Lima, DIRSI, 2007.
[15] LU, Anne, "M&A disrupts monopoly on the Latin American telecom industry", International Business Times, February 03 2016, http://www.ibtimes.com.au/ma-disrupts-monopoly-latin-american-telecom-industry-1503235
[16] Latin America Report: OpenNet Initiative https://opennet.net/research/regions/la

telecommunications by the State, plus tight price controls imposed by the regulatory agency, translate into a non-competitive environment that leads to the same stagnation and lack of development as a cartel, while keeping prices artificially low.

Cross-ownership of media platforms, where service providers offer a range of services from television to mobile telephony and internet access, while also creating and delivering content to consumers, might raise concerns regarding the free and open flow of information[17].

2.4 Underlying infrastructure

The underlying infrastructure in which the internet frequently relies can be affected by power outages, which can occur often in certain places in Latin America. Electrical shortages caused by periods of drought and by poor infrastructure development can affect basic communication services, such as in Venezuela[18], where in the first months of 2016, power cuts were scheduled for three or four hours a day through the entire country, affecting not only fixed connections but also mobile phone networks, with consequences that lasted for several hours after the outages.

Power outages are commonplace in most Latin American countries; both Brazil[19] and Argentina[20] have reported major issues as a consequence of their widespread outages, but other countries (Puerto Rico, Mexico, Colombia, Chile) have experienced important electrical failures within the last two years[21]. While the severity of the situation is not the same in all cases, this brings to light that the fragility of online communications in many cases relies in general service

---

[17] JENSEN, Mike: "Digital convergence: Global trends in broadband and broadcast media concentration". March 18, 2016
https://www.apc.org/en/news/digital-convergence-global-trends-broadband-and-br

[18] DIAZ, Marianne: "In Venezuela, Electrical Shortages Limit Basic Communication — and Free Expression". Global Voices Advox, June 8, 2016
https://advox.globalvoices.org/2016/06/08/in-venezuela-electrical-shortages-limit-basic-communication-and-free-expression/

[19] O'NEIL, Shannon K., "Lights Out: Brazil's Power Problem." August 12, 2014,
http://blogs.cfr.org/oneil/2014/08/12/lights-out-brazils-power-problem/

[20] SMINK, Verónica: "Argentina: qué hay detrás de los apagones que enfadan a los ciudadanos", December 17, 2014
http://www.bbc.com/mundo/noticias/2014/12/141215_argentina_apagones_cortes_electricos_verano_irm

[21] Latin America, Power Outage on Google Map http://www.mapreport.com/areasubtopics/l-d-o.html

infrastructure, which can be underdeveloped or weak. Some rural areas in Latin America lack basic services altogether, making it a challenge to bridge the so-called "last mile" of connectivity.

2.5 Shutdowns

Partial or total shutdowns of internet services have occurred in recent years in different Latin American countries. In Venezuela, where the different physical layers of the internet are controlled directly by the central government[22], the Ministry of Communications shut down the internet in the entire country for twenty minutes in election day in 2013[23], and then again in the state of Táchira for about 36 hours[24]. In Ecuador, in 2014, a government order caused ISPs to block Google and YouTube for about half an hour[25]. The blocking in Ecuador was performed by the Association of Internet Providers of Ecuador (AEPROVI) in compliance with a government's request, while in Venezuela, the shutdown was performed by CANTV, the state-owned ISP, leaving over 90% of the population without broadband service at a crucial moment[26].

While the most worrying aspect of these shutdowns might be their enforcement by the Executive branch without any previous judicial procedure, it is also worth mentioning the repeated blocking of the WhatsApp service by the Brazilian government, in response to WhatsApp denial to hand over information in the course of a criminal investigation[27]. Brazil's five main mobile operators had to block

---

[22] APC, Ibid.
[23] DIAZ, Marianne: "Venezuela: Internet blocked for "three minutes" on Election Day ". April 15, 2013. https://advox.globalvoices.org/2013/04/15/venezuela-internet-blocked-for-three-minutes-on-election-da/
[24] DIAZ, Marianne: "Venezuela: The Internet Goes Dark in Táchira ". February 22, 2014 https://advox.globalvoices.org/2014/02/22/blackout-in-venezuela-the-internet-goes-dark-in-tachira-censorship-access/
[25] FRANCESCHI, Lorenzo: "Ecuador Briefly Censored Google and YouTube, Leaked Document Shows". April 14, 2016. https://motherboard.vice.com/read/ecuador-briefly-censored-google-and-youtube-leaked-document-shows
[26] FREEDOM HOUSE, Freedom on the Net 2013: Venezuela https://freedomhouse.org/report/freedom-net/2013/venezuela
[27] BBC: "WhatsApp in Brazil back in action after suspension", July 20, 2016 http://www.bbc.com/news/world-latin-america-36836674

WhatsApp all over the country, a measure that also affected users in neighboring countries[28] (reportedly Venezuela, Argentina and Chile).

3. Neutrality

3.1 Zero-rating practices

Chile was the first Latin American country to implement a net neutrality law back in 2010, followed by Brazil's Marco Civil in 2014. The Chilean legislation, however, is not to be construed as a blanket ban in all zero-rating practices, but a prohibition against certain mobile operators that offer free access to specific social networks[29]. Initiatives such as Wikipedia Zero would not be forbidden under this provision, and it is to be noted that Chilean mobile providers continue to offer mobile plans that include access to certain applications. According to a 2016 poll, 51% of Latin American providers offer some sort of free or unlimited access to social networks[30], and several countries have welcomed initiatives such as Facebook's Free Basics (formerly known as Internet.org), including Colombia, Guatemala, Perú and Panamá. In 2015, Brazil announced an agreement with Facebook to implement Free Basics in the country,[31] which once again comes to prove that Marco Civil did not grant enough protections to net neutrality.

Zero-rating practices in general, and Free Basics in particular, have been considered a threat to privacy and free access to information by many local and global civil society organisations. Initiatives such as Free Basics undermine free competition and

---

[28] El Nacional, "Bloqueo de Whatsapp en Brasil estaría afectando el servicio en Venezuela", December 20, 2015 http://www.el-nacional.com/tecnologia/Bloqueo-Whatsapp-Brasil-afectando-Venezuela_0_758324175.html

[29] VERA HOTT, Francisco: "¿Es deseable tener excepciones a la neutralidad de la red?", Derechos Digitales, October 01, 2014. https://www.derechosdigitales.org/7929/wikipedia-zero-en-chile-es-deseable-tener-excepciones-la-neutralidad-en-la-red/

[30] PAUTASIO, Leticia: "Encuesta Zero Rating: 51% de los operadores latinoamericanos ofrece redes sociales ilimitadas". September 21, 2016 http://www.telesemana.com/blog/2016/09/21/encuesta-zero-rating-51-de-los-operadores-latinoamericanos-ofrece-redes-sociales-ilimitadas/

[31] AQUINO, Miriam: "Governo cria comissao para estudiar o Internet.org do Facebook", June 10, 2015. http://www.telesintese.com.br/governo-cria-comissao-para-estudar-o-internet-org-facebook/

create an enclosed and reduced version of the internet[32], where available content is determined by companies (or under a private company's "guidelines"), not by users. In practice, this damages the free flow of information and the ability to actively participate in online content production and expression, and in consequence may also impact freedom of expression. These initiatives also constitute a threat against privacy by fostering the concentration of personal information in a few services[33], thus facilitating surveillance both by governments and by companies. Furthermore, zero-rating practices foster the creation of a market with "enhanced" access for certain players, harms innovation, and allows providers to create unfair advantages toward certain information or communication channels, thus impairing others[34].

3.2 DNS and IXP administration

Control over the internet Domain Name System (DNS) is being increasingly used as a censorship mechanism. DNS administration is being co-opted for political purposes, and several of these practices can constitute threats or violations to freedom of speech: domain name seizures; local DNS redirection; DNS injection, among others[35] . The hierarchical structure of DNS administration creates several different chokepoints where access to content can be restricted. According to research from the Venezuelan Press and Society Institute (IPYS), DNS blocking has been used in the country to restrict the free flow of information in every local ISP[36]. By means of this technique, DNS servers respond incorrectly to requests for services they want to block. This response may contain incorrect information, an error message or a

---

[32] BOGADO, David and RODRIGUEZ, Katitza: "Does Internet.org Leave Latin Americans Without A Real Internet?". EFF, April 20, 2015.
https://www.eff.org/deeplinks/2015/04/does-internetorg-deprive-latin-americans-real-internet

[33] PALLERO, Javier: "Facebook en la OEA y Zero Rating: neutralidad en peligro en Latinoamérica", April 22, 2015.
https://www.accessnow.org/facebook-en-la-oea-y-zero-rating-neutralidad-en-peligro-en-latinoamerica/

[34] KAUR, Valerie: "36 leading scholars to federal officials: Only the FCC can protect the open internet". January 29, 2015
https://cyberlaw.stanford.edu/blog/2015/01/36-leading-scholars-federal-officials-only-fcc-can-protect-open-internet

[35] BRADSHAW, Samantha, DeNARDIS, Laura; The politicization of the Internet's Domain Name System: Implications for Internet security, universality, and freedom. New Media & Society August 8, 2016.

[36] IPYS Venezuela: "Navegar con libertad: Principales hallazgos de la navegación en Venezuela".
http://ipysvenezuela.org/navegarconlibertad/tag/bloqueos-dns/

refusal to answer. Using DNS to control content can generate a high risk of suppressing lawful speech, along with the creation of jurisdictional conflicts[37].

Domain name registration and deregistration can also become tools to restrict online freedoms. In different countries, country-code top-level domain (ccTLD) administration works according to different models. In those cases where the administration model is highly dependant from the government, such as Venezuela, where ".ve" domains are administered by a body directly dependant from the Ministry of Telecommunications, there might be a lack of trust regarding possible negative decisions to register or renew domains that may be related to criticism of governments[38]. Back in 2012, NIC.ar admitted that certain domain names could not be registered in Argentina, because they contained words that appeared in a list of forbidden terms[39], including words such as the President's first name. Domain name de-registration as a mean to suppress content deemed as unlawful has also been occurring for a long time[40].

In those countries where one or more internet exchange points (IXPs) exist to channel internet traffic, and particularly if they are administered by the State, they can become a tool to centralise censorship and surveillance, through the use of capabilities for filtering or deep packet inspection that can be installed at IXP level[41]. While IXPs can often be seen as an opportunity to improve connectivity[42], there has been pushback from civil society and telecommunication companies in some cases where they have been considered to pose hidden dangers. For instance, in Venezuela,

---

[37] CDT, «The Perils of Using the Domain name System to Address Unlawful Internet Content», September 2011, http://www.cdt.org/fi les/ pdfs/Perils-DNS-blocking.pdf

[38] CELE: "Domain Names: Expression that Deserves Protection". 20 November 2012. Global Voices Advocacy.
https://advox.globalvoices.org/2012/11/20/domain-names-expression-that-deserves-protection/

[39] TORO, Eliana, "Términos prohibidos y censura en dominios de internet"
http://periodicotribuna.com.ar/12318-terminos-prohibidos-y-censura-en-dominios-de-internet.html

[40] Derechos Digitales: "elmercuriomiente.cl: un nuevo caso de censura en Internet". May 7, 2005
https://derechosdigitales.org/7/elmercuriomientecl-un-nuevo-caso-de-censura-en-internet/

[41] Freedom of expression and the private sector in the digital age: Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression by the Association for Progressive Communications (APC).
http://www.ohchr.org/Documents/Issues/Expression/PrivateSector/APC.pdf

[42] AMEGA-SELORM, Charles, et al. "Impact of Internet Exchange Points (IXPs)" August 2009. Open Society Foundation.
https://www.opensocietyfoundations.org/reports/impact-internet-exchange-points-ixps

the creation of a single IXP has been repeatedly proposed and rejected, because the draft regulation gave the State powers to order ISPs to modify their practices in relation to traffic management, which, given the current political context, can be deemed as a way to exert more control over the flow of information[43].

3.3 Content filtering

In some countries, the regulatory agencies have enforced content filtering through financial penalties. Venezuela's telecommunications agency, CONATEL, has ordered ISPs to block hundreds of websites with only an administrative order[44], including media websites[45] and circumvention tools[46]. According to the newspaper *El País*, during the 2014 countrywide protests, CONATEL warned ISPs that they "must comply without delay with orders to block websites with content contrary to the interests of the Government"[47].

In Cuba, where mobile operators are owned and controlled by the government, the mobile provider Cubacel (ETECSA) blocks certain terms and keywords in SMS[48], including words and phrases such as "human rights", "democracy" or "dictatorship". Given that only 25 % of the Cuban population have some form of internet access, and a mere 5 % of them enjoy fixed connectivity, mobile phones (and particularly SMS and MMS) are an essential form of communication for citizens.

---

[43] BRICEÑO, Ysabel: "Venezuela: NAP: An Opportunity to Improve Universal Broadband Access?", June 2009, APC. https://www.apc.org/en/node/8887

[44] TAL CUAL: "Conatel ha bloqueado más de mil páginas web en menos de 12 meses", October 28, 2014. http://runrun.es/nacional/venezuela-2/164995/conatel-ha-bloqueado-mas-de-mil-paginas-web-en-menos-de-12-meses.html

[45] A TODO MOMENTO: "Bloqueo de NTN24 es decisión "presidencial" afirma Conatel", April 24, 2016. http://noticiasvenezuela.org/2016/04/24/bloqueo-de-ntn24-es-decision-presidencial-afirma-conatel/

[46] DIAZ, Marianne: "TunnelBear VPN Service Blocked in Venezuela?". March 12, 2014. https://advox.globalvoices.org/2014/03/12/tunnelbear-vpn-blocked-venezuela-censorship-anonymity/

[47] MEZA, Alfredo: "El régimen venezolano estrecha el cerco sobre internet", March 13, 2014. http://internacional.elpais.com/internacional/2014/03/13/actualidad/1394736119_794503.html

[48] SÁNCHEZ, Yoani and ESCOBAR, Reinaldo, "Cubacel censura los SMS con las palabras 'democracia' o 'huelga de hambre'", September 3, 2016. http://www.14ymedio.com/reportajes/Cubacel-censura-SMS-palabras-democracia_0_2064993492.html

4. Privacy and data protection

4.1. SIM registration

While there is no evidence that mandatory SIM registration leads to a reduction in crime rates[49], several Latin American countries still require identity verification and registration at the point of sale. In many cases, this leads to store clerks to require and handle sensitive information (national identification number, home address, credit card numbers) which then are collected and added to a database that can afterwards be accessed by law enforcement agencies or other government bodies. In Colombia, for instance, SIM card registration is mandatory for all mobile phones, and every service provider must require the user's national ID number, full name, address and contact number, handing over this information to the police afterwards with the objective of creating a "blacklist" for stolen devices[50].

Ecuador, Guatemala, Venezuela, Brazil[51] and Peru also apply mandatory SIM registration both for prepaid and for postpaid services, and for the same reasons than Colombia, with the aggravating factor that Guatemala, Venezuela and Brazil do not have data protection laws, thus creating a massive database of personal information for which the citizens have no safety requirements nor recourse before possible undue uses of said data. In Peru, alongside the requirement for SIM registration, a biometric registration of each device (a fingerprint that must be collated with the National registry of Identification and Civil Status database) is necessary[52]. Venezuela also requires fingerprint registration, but service providers are not required to validate this information against a national database. In Colombia, service providers must grant the police remote access to a database containing the

---

[49] GSMA: "Mandatory registration of prepaid SIM cards. Addressing challenges through best practice". April 2016. http://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/Mandatory-SIM-Registration.pdf

[50] ADC: "Libertad de expresión en el ámbito digital: El estado de situación en América latina". April, 2016 https://adcdigital.org.ar/2016/04/05/libertad-expresion-ambito-digital/

[51] In Brazil's case, registration is not required by law, but it is requested by the rulings of the national telecommunications agency (ANATEL).

[52] TVPERU: "Inició registro biométrico para líneas prepago: Sepa más del 'apagón telefónico'". June 5, 2015. http://www.tvperu.gob.pe/informa/nacional/inicio-registro-biometrico-lineas-prepago-como-sera-apagon-telefonico

names, national ID, address, phone number and service activation date of all mobile phone users[53].

Meanwhile, Chile is discussing two bills that seek to institute mandatory SIM registration, and Mexico, which passed a law to require it in 2009, ended the measure in 2011 because it failed to reduce the crime rates and was difficult to implement effectively[54].

4.2. Data retention

Most Latin American countries demand that service providers keep a log of users' communications activity, requiring information that ranges from the phone numbers involved in a call, to IP addresses for online activity. While these data are often unprotected by law, because they are considered "metadata" and thus frequently fall outside of the defined realm of "personal data", a few of these data points are often more than enough to identify and locate a person, without the need of a warrant or even a legal procedure.

Mexico, Brazil, Chile, Colombia, Peru and Venezuela are some of the countries that require ISPs to retain and store user's information for a certain period of time, and to facilitate it to the authorities in case it is required. In Argentina, the law required intermediaries to register and systematise filiation and domiciliary data from their users and their communication logs for ten years, but the statute was declared unconstitutional by the Supreme Court, as it violated the principles of legality, necessity and proportionality[55].

In Peru, Legislative Decree No. 1182 requires that service providers grant the police with access to real-time localisation or geolocalisation data to all mobile phones or electronic devices, after a request that does not need judicial authorisation. While the request needs to fulfil three requisites (namely, that it is a flagrant offence, that it is

---

[53] CASTAÑEDA, Juan Diego. "Data retention in Colombia, one of the longest in the world". February 28, 2015. http://www.digitalrightslac.net/en/la-retencion-de-datos-en-colombia-una-de-las-mas-largas-del-mundo/

[54] ADC, Ibid.

[55] ADC, Ibid.

punishable by more than a four-year prison sentence, and that access to this information constitutes a necessary means for research), these requirements are not corroborated until after access has been granted[56].

Personal data registration is also required from online media in Ecuador, where any electronic publication needs to keep track of the name, e-mail address and national ID of every user who creates a comment below an article or post, and create mechanisms to denounce and delete any comments that are deemed unlawful. Electronic media are considered civilly, criminally and administratively liable for comments made by their users in these forums.

Conclusion

The practices and policies of telecommunication companies are extremely important to online privacy and freedom of speech. Business decisions, such as the implementation of zero-rating practices or the installation of new infrastructure, can influence many people's ability to access internet services. While governments have the responsibility to protect human rights and in consequence, the obligation to enforce business standards that avoid any possible harm to freedom of speech and access to information online, it is also true that certain government practices can interfere with the service providers' abilities to respect human rights. Service providers can be forced to comply with measures to take down or block content, to implement shutdowns of internet and phone services or to retain personal data from their users and turn it over to state actors, or even to implement surveillance technologies and communication backdoors, thus affecting freedom of speech and privacy.

[56] MORACHIMO, Miguel: "Nueva norma permite a la Policía saber dónde está cualquier persona sin orden judicial", July 27, 2015.
http://www.hiperderecho.org/2015/07/norma-policia-geolocalizacion-sin-orden-judicial-1182/

Recommendations

- Companies and governments have the responsibility to respect and protect human rights. Data retention, surveillance, and content filtering measures should follow the principles of necessity and proportionality, and be enforced only where the pursued end is legitimate and indispensable. ISPs and states should adopt United Nations' Guiding Principles on Business and Human Rights, and as such, service providers should actively avoid any activity that contributes to harm human rights. Government should refrain from taking measures, and from exerting pressure on ISPs to comply with measures to limit the free flow of information and communications online, including content takedown, web filtering and shutdowns.

- There should be strong mechanisms in place in order to avoid monopolistic practices in the telecommunication sector. This might include fostering community initiatives and allowing the assignation of currently unlicensed frequency ranks and white spaces for smaller companies that could provide opportunities for lowering connectivity costs and diminishing access gaps.

- The implementation of transparency and accountability mechanisms to identify and prevent any practices that could be harmful to human rights is indispensable. Citizens should have readily available and accessible mechanisms to control what information is being collected about their online activities and communications, along with how it is stored, shared and disposed.