Examining Internet Freedom in Latin America (EXLILA)

Country report: Colombia

Juan Diego Castañeda and Amalia Toledo

Karisma Foundation

Association for Progressive Communications (APC)
March 2016

This report was produced as part of the APC project Examining Internet Freedom in Latin America (EXLILA). The project is funded by the Open Society Institute (OSI) and APC and coordinated by Derechos Digitales.

Table of contents

1. Executive summary

Although Colombia has challenges guaranteeing internet access to all its population, the internet has become an essential tool for the development of many activities and the exercise of fundamental rights like freedom of expression and access to knowledge.

Legislation and jurisprudence applicable to the internet have not been systematic, and this has often had major effects on whether the internet will continue to be a free and open tool. The principle of net neutrality, for example, has developed in such a way as to allow the creation of different plans differentiated according to the market, which in practice may lead to counteracting this very principle. Regulations on surveillance of communications, although important for criminal investigation, do not have the necessary judicial checks and balances, and lack a serious analysis of need and proportionality, as in the case of the powers exercised by intelligence agencies. Finally, although systematic internet filtering does not occur, there is a regime for blocking child pornography that pursues an entirely necessary purpose but lacks controls and the possibility to exercise the right to a defence.

The problematic cases included in this report show that there is still a long way to go in enforcing the current regulations on situations occurring on the internet. In one case, an online news commentator was imprisoned and fined for libel. In another, a student is being prosecuted for copyright infringement for sharing on a digital platform some academic material previously published on the internet.

But the most relevant cases have to do with the illegitimate use of surveillance tools. Former officials of the government and security agencies have been convicted for illegally intercepting communications from high court magistrates, opposition leaders and journalists. A campaign adviser in the presidential elections admitted illegally intercepting communications between officials and other actors involved in the peace dialogue with guerrillas of the Revolutionary Armed Forces of Colombia (FARC). Finally, investigations by international organisations have revealed surveillance and hacking systems previously unknown to the general public.

Given this scenario, it is increasingly urgent to enforce international regulations of human rights in digital environments; strengthen legal capacities, especially concerning understanding of the internet; develop and implement models of participation in the construction of policies and standards for the internet, that guarantee the involvement of civil society, academia and the technical community on an equal basis; and promote monitoring by civil society of legislative, judicial and administrative developments affecting the net.

This report will give a rapid overview of current regulations and the most relevant cases – in the courts and the media – affecting positively or negatively the exercise of human rights by Colombian citizens. We will review regulations on net neutrality, cyber crime, child protection, criminal investigation and intelligence activities, data retention and anonymity, emphasising the problems that many of these regulations pose for the protection of fundamental rights. We will also look at some of the most representative court cases or those reported in the media, which will show that there is still a long way to travel towards recognition and protection of the internet as a space for the exercise of rights and freedoms. Finally we will present some recommendations intended to promote the potential for democratisation and the empowerment of citizens through access to and use of the internet.

2. Introduction

The first internet experience in Colombia was in 1988, when an internal network was set up in the Universidad de los Andes.[1] The early 1990s saw the first interconnection between several Colombian universities and the University of Columbia in the United States. Since then, the expansion of the internet in the country has been constant and unstoppable.

Nowadays, the internet has become an essential tool in Colombian society. While challenges remain for connectivity and access to the network in the country, it is undeniable that everyday life depends largely on online interactions and activities that give people a voice they often lack in physical spaces, increase their incomes, connect them with friends, relatives, colleagues and even with the government, allow them to purchase goods and services online, transform them into content generators, and a great many other things. Cyberspace has become an arena for political and citizens' participation, and for the exercise of human rights to an extent never seen before.

The development of the internet has not been without its social, technological, legal and judicial challenges. Addressing these challenges has, on many occasions, endangered the exercise of human rights themselves. We are in the presence of a tool which allows us to create new ways of interacting every day, in all phases of our life, and this partly requires a process of trial and error. It also requires continual updating and revision of our knowledge of emerging practices, the technologies and applications that are constantly being developed, and the reform of legal regulations and doctrines that have been made obsolete by the new reality.

This report will give a rapid overview of current regulations and the most relevant cases – in the courts and the media – affecting positively or negatively the exercise of human rights by Colombian citizens. We will review regulations on net neutrality, cyber crime, child protection, criminal investigation and intelligence activities, data retention and anonymity, emphasising the problems that many of these regulations pose for the protection of fundamental rights. We will also look at some of the most representative court cases or those reported in the media, which will show that there is still a long way to travel towards recognition and protection of the internet as a space for the exercise of rights and freedoms. Finally, we will present some recommendations intended to promote the potential for democratisation and for the empowerment of citizens through access and use of the internet.

3. General regulatory framework

Colombia recognises the right of all persons to freedom of expression and protection of personal and family privacy, as well as the right to self-determination of data, or habeas data.[2] Some of the relevant international human rights instruments which Colombia has signed are:

- American Declaration of the Rights and Duties of Man (1948)
- Universal Declaration of Human Rights
- International Covenant on Civil and Political Rights
- American Convention on Human Rights (Pact of San José, Costa Rica)
- Convention on the Rights of the Child

[1]Cobos, T. (2010, 12 January). Historia de internet en el mundo y su llegada a Colombia. *Tania Lu, mi blog*. tanialu.co/2010/01/12/historia-de-internet-en-el-mundo-y-su-llegada-a-colombia

[2]Constitución Política. (1991). Articles 15, 16 and 20. www.constitucioncolombia.com/titulo-2/capitulo-1

- International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families
- Convention on the Rights of Persons with Disabilities
- Convention on the Elimination of All Forms of Discrimination against Women, and its Optional Protocol.

Constitutional jurisprudence has on countless occasions analysed conflicts between the right to freedom of expression and other basic rights, such as to honour and good name, as well as violations of the right to privacy. In general, fundamental rights are recognised equally within and outside the digital environment.

3.1. Net neutrality

There is no comprehensive regulation of the internet in Colombia. It may be noted that in the National Development Plan, article 56 stipulates that internet service providers (ISPs) "may not block, interfere with, discriminate or restrict the right of any internet user to use, send, receive or offer any legal content, application or service over the internet."[3] However, at the end of the section, ISPs are permitted to "make offers according to the needs of market segments or their users based on usage and consumption profiles, and this shall not be understood as discrimination."

This exception was taken to the extreme in Resolution No. 3502 of 2011[4] of the Commission for Regulation of Communications, the telecoms regulator. It said ISPs "may offer internet access plans that limit access to generic types of services, contents or applications." This has led to the proliferation of internet plans based on zero rating,[5] the most famous of them being Facebook's Internet.org, now known as Free Basics (see the Problematic cases section).

3.2. Cyber crime

There are precedents for the creation of various types of offences based on actions on the internet (see the section on Problematic cases). Criminal law also establishes some offences specifically related to information and communications technologies (ICTs), which were introduced in 2009.[6] The reform included several offences in the Criminal Code, such as unlawful access to a computer system, interception of digital data or use of malicious software.

3.3. Blocking of child pornography

Colombia has not implemented any specific regulations on blocking or filtering internet content, with the sole exception of child pornography. Law No. 679 of 2001[7] and Decree No. 1524 of 2002[8] empower a division of the National Police to review digital content denounced as child pornography and to determine whether or not it should be blocked. If the decision is taken to block it, the URL is notified to the Ministry of Information and Communications Technologies, which in turn notifies the ISP, which proceeds to block

[3]Ley No. 1450. (2011). *Plan Nacional de Desarrollo 2010-2014*. www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101

[4]www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45061

[5]https://en.wikipedia.org/wiki/Zero-rating

[6]Ley No. 1273. (2009). *Ley de delitos informáticos.* www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[7]www.mintic.gov.co/portal/604/articles-3685_documento.pdf

[8]www.mintic.gov.co/portal/604/articles-3554_documento.pdf

the site. Criteria for blocking child pornography are set by a commission made up of the Colombian Institute for Family Welfare, the Ombudsperson's Office, the Attorney General's Office and UNICEF representatives.

There is no legal duty whatsoever for the authorities to notify the person affected. Nor is there court supervision of this measure. The blocked page must show a notice to the effect that it has been blocked as child pornography, and must note the existence of Law No. 679 of 2001.

3.4. Surveillance of communications

Surveillance of communications in Colombia includes interception, retention of traffic data and the legal status of use of encryption, as follows.

3.4.1. Interception

Communications may only be intercepted when there is a law which allows it; the rules of that law must be followed and judicial oversight is required.[9] In Colombia, the only body authorised to order interception is the Attorney General's Office, which is in charge of criminal investigation and prosecution of those who can be shown to have committed a crime. Article 250 of the Constitution reads:

> It is the responsibility of the Attorney General's Office to investigate crimes and to press charges against the suspects and to develop records and carry out searches, seizures and interceptions of communications. In these cases the judge who ensures guarantees will review the actions retrospectively, within no more than thirty-six hours.[10]

The same attributions appear in the Code of Criminal Procedure. Specifically, the Attorney General's Office can retain, inspect and return correspondence, intercept communications on any media, retain and seize devices to recover information left when surfing the internet or by other technological means, and carry out selective searches of databases.[11] Of all these actions, only selective searching of databases requires previous authorisation by the supervisory judge. The other actions are carried out at the order of the Attorney General's Office and afterwards are reviewed by the supervisory judge under criteria of legality, necessity and proportionality. If the judge declares the actions are legal, the information recovered may be used in the criminal trial.

The Constitutional Court has taken the view that interception of communications and similar actions are urgent enough to justify supervisory hearings being held after the event.[12] In contrast, selective searches of databases require a previous authorisation hearing because the data are not under the control of the suspected person, and so there is no urgency.

None of the regulations on criminal procedure require that a person being investigated for evidence in a way that affects their right to privacy should be notified. However, the judicial hearing (that legalises the evidence-gathering measure and its results) is not secret, and the person investigated is not barred from

[9]Constitución Política. (1991). Article 15. www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15

[10]Ibid., Article 250. www.constitucioncolombia.com/titulo-8/capitulo-6/articulo-250

[11]Código de Procedimiento Penal. Articles 233-236 and 244. perso.unifr.ch/derechopenal/assets/files/legislacion/l_20130808_01.pdf

[12]Corte Constitucional de Colombia. (2007). Sentencia C-336. www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm

attending. In any case, it could be understood that proper notification is necessary, based on the principle and fundamental right of due process.[13]

3.4.2. Intelligence

Although they are not specifically empowered to intercept communications, intelligence agencies may "monitor the electromagnetic spectrum," according to article 17 of the Law on Intelligence and Counterintelligence Activities.[14] The Constitutional Court ruled on this point:

> Monitoring the electromagnetic spectrum as an action in the field of intelligence and counterintelligence, consists of random and indiscriminate tracking, involving incidental capture of communications that reveal circumstances that lead to avoiding attacks and controlling risks to the defence and security of the Nation. Technically what is occurring is tracking of shadows, images and sounds represented in electromagnetic frequencies and radio waves. Monitoring is not intercepting.[15]

However, it is not clear why monitoring is not considered to involve intercepting communications, since in any case these are "captured" and monitoring can "reveal circumstances that lead to avoiding attacks and controlling risks." Nor is it clear whether the internet may be monitored in the same terms. So far no cases have been presented to the judicial authorities for interpretation of the extent of these powers.

3.4.3. Data retention

Retention of communications traffic data is obligatory for the purposes of criminal investigation and intelligence activities. For criminal investigation, Decree No. 1704 of 2012 obliges network and telecommunications service providers to retain, and hand over to the attorney general's office when requested, information about the subscriber and the location of devices.[16] The lLaw on Intelligence and Counterintelligence, for its part, obliges providers to retain and hand over to intelligence agencies "the record of communications of telephone subscribers involved, technical data identifying subscribers" and all the information necessary to locate the devices.[17]

Neither of the two forms of retention is subject to judicial oversight and it is not clear if they apply only to fixed and mobile telephones, or also to internet data. There is no catalogue of the offences for which the measure is to be used for investigation.

3.4.4. Encryption and anonymity

There is no general prohibition against anonymous expression. However, two points must be made. First, Resolution No. 3067 of 2011[18] of the Commission for Regulation of Communications defined the principles

[13]Constitución Política. (1991). Article 29. www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-29

[14]Ley No. 1621. (2012). *Ley de actividades de inteligencia y contrainteligencia.* www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=52706

[15]Corte Constitucional de Colombia. (2012). Sentencia C-540. www.corteconstitucional.gov.co/relatoria/2012/c-540-12.htm

[16]Decreto 1704. (2014). Articles 4 and 5. www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=48863

[17]Ley No. 1621. (2012). *Ley de actividades de inteligencia y contrainteligencia*, article 44. www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=52706

[18]www.asomovil.org/wp-content/uploads/2015/02/Resoluci%C3%B3n-No.-3067-de-2011-Indicadores-de-calidad-en-Telecomunicaciones.pdf

providers must follow in terms of network security, according to the recommendations in the X.800 series[19] of the International Telecommunication Union. Similarly, banking institutions have a duty to secure their communications.

Second, in spite of the above, article 102 of Law No. 418 of 1997[20] prohibits "sending messages in encrypted or unintelligible language" to users of "communications equipment using the electromagnetic spectrum." The scope of this regulation is unclear and we are not aware of cases where anyone has been penalised in any way for using data encryption in their communications.

4. Problematic cases

4.1. Surveillance of communications

In 2009 it came to light that the former state intelligence organisation, the Administrative Department of Security (DAS – Departamento Administrativo de Seguridad) had illegally tapped private communications of high court magistrates, journalists and opposition leaders.[21] The case, known as "Chuzadas", was the subject of criminal investigation, and the courts convicted, among others, the former director of DAS and the former secretary of ex-president Álvaro Uribe for illegal interception of communications.[22] The role of the internet in the affair is unknown, but it is possible that digital communications of the victims may have been intercepted, as the security organisations have the technical capability to do so.

In February 2014 a covert military intelligence operation became known which allegedly intercepted emails of the persons representing the government and the FARC at the peace talks taking place in Havana, Cuba.[23] The name of the covert operation was "Andromeda" and the same name was used to report the scandal in the media. After the case came to light, 20 members of the military were relieved of duty and five were dismissed.[24] So far some troops have been arrested, but there are as yet no convictions and the authorities have not yet got to the bottom of the case.[25]

In mid-2014, during the presidential election campaign, it became known that former candidate Óscar Iván Zuluaga had hired a supposed information technology expert who provided him with confidential information about the peace process, with a view to enhancing the effectiveness of his campaign.[26] Andrés Sepúlveda, the supposed expert, eventually admitted the offence of interception of personal communications, among others.[27] Investigations against other persons involved are proceeding slowly.

---

[19] https://es.wikipedia.org/wiki/X.800

[20] www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6372

[21] Revista Semana. (2009, 21 February). El DAS sigue grabando. *Revista Semana.* www.semana.com/nacion/articulo/el-das-sigue-grabando/100370-3

[22] El Tiempo. (2015, 30 April). Condena de 14 años para Hurtado y 8 para Bernardo Moreno por chuzadas. *El Tiempo.* www.eltiempo.com/politica/justicia/caso-chuzadas-del-das-condena-a-maria-del-pilar-hurtado-y-bernardo-moreno/15660280

[23] Revista Semana. (2014, 8 February). ¿Alguien espió a los negociadores de La Habana? *Revista Semana*. www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3

[24] Blu Radio. (2015, 23 January). Purga en inteligencia de las Fuerzas Militares por escándalo de Andrómeda. *Blu Radio*. www.bluradio.com/88548/purga-en-inteligencia-de-las-fuerzas-militares-por-escandalo-de-andromeda

[25] El Espectador. (2014, 5 October). Legalizan captura de tres uniformados del Ejército por caso Hacker. *El Espectador*. www.elespectador.com/noticias/judicial/legalizan-captura-de-tres-uniformados-del-ejercito-caso-articulo-520717

[26] Revista Semana. (2014, 17 May). El video del 'hacker' y Zuluaga. *Revista Semana*. www.semana.com/nacion/articulo/el-video-del-hacker-con-oscar-ivan-zuluaga/388438-3

In mid-2015, large quantities of information were leaked from the Italian firm Hacking Team,[28] which led to the discovery that the National Colombian Police (DIPON) had had dealings with the firm and had purchased some of its products, specifically the "Galileo" programme, malicious software capable of infecting computers and extracting information from them, as well as of remotely switching on microphones or web cameras.[29] While concrete evidence is lacking that this software has been used, recently journalists reported being the targets of illegal spying, with the supposed purpose of discouraging their investigations of police corruption.[30] One of the journalists said that information being worked on in their personal computer was deleted, and on one occasion the mouse cursor began to move by itself.[31] The government has created a commission to investigate the case[32] and the Attorney General's Office has opened a formal investigation that is still under way.[33]

4.2. Privacy International investigations

In August 2015 the British organisation Privacy International published two reports on the status of surveillance of communications in Colombia.[34] The general conclusion was that surveillance systems exist with different degrees of supervision and regulation. The Attorney General's Office controls a system called Esperanza, which supposedly only has the capability to intercept a limited number of mobile phone lines. Around 2007 it became known that the National Police was acquiring equipment for surveillance of communications within a programme called Single Monitoring and Analysis Platform (PUMA – Plataforma Única de Monitoreo y Análisis) with surveillance capacities that were not altogether clear but, in one way or another, probably include the internet. In mid-2014 the Attorney General's Office announced publicly that it was taking over the PUMA system equipment because it found insufficient guarantees that the equipment would not be abused and because it is the only agency authorised to intercept private communications.[35] In spite of the lack of regulation for the use of interception systems, the Police announced that it would begin trials for the use of PUMA equipment in October 2015.[36]

---

[27]Revista Semana. (2015, 13 February). Juez avaló preacuerdo entre Fiscalía y el hacker Sepúlveda. *Revista Semana*. www.semana.com/nacion/articulo/caso-hacker-juez-avalo-preacuerdo-con-andres-sepulveda/417779-3

[28]Hern, A. (2015, 6 July). Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim. *The Guardian*. www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

[29]Botero, C., & Sáenz, P. (2015, 24 August). En Colombia, el PUMA no es como lo pintan. *Digital Rights Latin America and the Caribbean.* www.digitalrightslac.net/es/en-colombia-el-puma-no-es-como-lo-pintan

[30]Jiménez Herrera, J. (2015, 4 December). "No hay duda de los seguimientos": Vicky Dávila. *El Espectador*. www.elespectador.com/noticias/judicial/no-hay-duda-de-los-seguimientos-vicky-davila-articulo-603572

[31]Vélez, L. (2015, 6 December). El precio de denunciar. *El Espectador*. www.elespectador.com/opinion/el-precio-de-denunciar

[32]El Tiempo. (2015, 7 December). "No vamos a tolerar persecuciones": Santos. *El Tiempo*. www.eltiempo.com/politica/gobierno/no-vamos-a-tolerar-persecuciones-santos/16451813

[33]*El Espectador.* (2015, 3 December). Fiscalía abrió investigación por seguimientos ilegales a Vicky Dávila. www.elespectador.com/noticias/judicial/fiscalia-abrio-investigacion-seguimientos-ilegales-vick-articulo-603160

[34]Privacy International. (2015). *Shadow State: Surveillance, Law and Order in Colombia.* https://www.privacyinternational.org/sites/default/files/ShadowState_English.pdf; *Demand/Supply: Exposing the Surveillance Industry in Colombia.* https://www.privacyinternational.org/sites/default/files/DemandSupply_English.pdf

[35]El Tiempo. (2014, 30 August). Fiscalía le dice "no" a sistema de interceptación "Puma" de la Policía. *El Tiempo.* www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092

[36]El Tiempo. (2014, 30 September). Plataforma Puma de la Policía entrará en operación, pero limitada. *El Tiempo*. www.eltiempo.com/politica/justicia/plataforma-unica-de-monitoreo-y-analisis-comienzan-pruebas/16390794

The latest surveillance system is the Integrated Digital Recording System (SIGD – Sistema Integrado de Grabación Digital) under the National Police Intelligence Directorate (DIPOL), which is capable of intercepting and monitoring mobile phone and text message communications. It is not clear whether the system provides the authorities with technological capability to monitor internet traffic.

Finally, leaked data from the Italian firm Hacking Team has revealed that the National Police may have agreed to purchase tools capable of intercepting private digital communications.[37] However, this is still a matter under investigation.

4.3. Freedom of expression and net neutrality

4.3.1. The "right to be forgotten"

Another relevant case involves a claim presented by a citizen against the newspaper *El Tiempo* and Google, because when he carried out a search for his name he found a result linking him to the commission of an offence. The Constitutional Court decided to protect his right to honour and good name, and ordered the newspaper to modify its news article to reflect the facts, but also to block the search for the link to the article where the name of the person appears in search engines like Google.[38] On the other hand, the Court took the view that Google was not responsible for the content generated by the newspaper, arguing that this exemption is necessary to protect net neutrality, which is guaranteed as part of the fundamental right to freedom of expression. Finally, the Court ordered the newspaper to make sure that news articles linking people's names with criminal cases were factually correct.

4.3.2. Internet.org

In early 2015, Colombia became the first Latin American country for the launch of Facebook's controversial Internet.org initiative, now known as Free Basics.[39] The project was announced jointly by the government, Facebook creator and owner Mark Zuckerberg, and the telecommunications operator Tigo. Although the project is a purely private deal between Facebook and Tigo, it was presented in Colombia as an important public policy to close the digital divide and provide connectivity for the population still without access to the internet. As this report goes to press, there is still no evidence from the telecommunications operator that Internet.org is fulfilling its goal of stimulating real access to the internet by more people.

In September 2015, Facebook launched the Free Basics platform for the implementation of Internet.org, adopting new guidelines for developers and the default use of https.[40] This move by Facebook was a response to many of the criticisms of its initiative.[41]

---

[37]Botero, C., & Sáenz, P. (2015, 24 August). Op. cit.

[38]Corte Constitucional de Colombia. (2015). Sentencia T-277. https://karisma.org.co/wp-content/uploads/2015/07/TUTELA-EL-TIEMPO.pdf

[39]El Tiempo. (2015, 14 January). Internet.org llega al país de la mano de Facebook. *El Tiempo*. www.eltiempo.com/archivo/documento/CMS-15093976

[40]Internet.org. (2015, 24 September). Update to Internet.org Free Basic Services. *Internet.org by Facebook*. press.internet.org/2015/09/24/update-to-internet-org-free-basic-services

[41]Access Now et. al. (2015, 18 May). Open letter to Mark Zuckerberg regarding Internet.org, net neutrality, privacy, and security. www.accessnow.org/pages/open-letter-mark-zuckerberg-regarding-internetorg

4.3.3. Libel

In a case of disproportionate application of criminal law to the internet, Gonzalo Hernán López was sentenced to 18 months imprisonment and a fine for insulting a public official in the web forum of a newspaper after an article reporting cases of political corruption. In his case, at least, it was understood that libellous expressions on the internet have more weight if they are made on social or collective media.[42]

4.4. Copyright

Diego Gómez is a biology student who is facing up to eight years in prison for sharing a Master's thesis on the internet which was already in digital form and available on several websites.[43] He is charged with violating copyright, even though he was only sharing the thesis as an academic resource for the benefit of other people, without thought of economic gain. The case is currently in the courts and the outcome is unknown. However, through a campaign launched by Karisma Foundation called #CompartirNoEsDelito (Sharing is Not a Crime), Diego has become a key international figure in the defence of open access.[44]

This case shows that practices that have emerged in the digital age and have caused a paradigm shift still clash with legal standards – in this case, copyright law – that are antiquated and out of date.

5. Conclusions and recommendations

The internet has unrivalled capabilities for permitting the exercise of rights such as freedom of expression and access to knowledge, but it may be negatively affected by policies that do not take into account its particular features and the points of view of the multiple stakeholders.

Unfortunately, the Colombian government is not consistent in its respect for fundamental rights when it comes to implementing policies and programmes for the internet, as can be seen by its development of communications surveillance systems. The lack of control and supervision of tools like PUMA or SIGD can hardly create a climate of confidence in which the internet can stand out as a platform for the exercise of fundamental rights. In addition, cases like that of Gonzalo Hernán López and Diego Gómez lead to the conclusion that the judicial branch still has a long way to go in understanding the nature of the net. Although the internet is seldom the focus of a judicial decision, the precedent set by these decisions is at odds with the need to adequately and proportionately enforce legislation designed for an internet-less world.

In this context, the following recommendations may be made:

- In general, international human rights standards should be taken into account, such as the Joint Declaration on Freedom of Expression and the Internet,[45] the Joint Declaration on Surveillance

[42]Código de Procedimiento Penal, Article 223. perso.unifr.ch/derechopenal/assets/files/legislacion/l_20130808_01.pdf

[43]El Espectador. (2014, 20 August). Estudiante podría ir a la cárcel por divulgar tesis en una plataforma virtual. *El Espectador.* www.elespectador.com/noticias/judicial/estudiante-podria-ir-carcel-divulgar-tesis-una-platafor-articulo-511647

[44]Fundación Karisma. (n/d). Compartir no es delito. www.karisma.org.co/compartirnoesdelito. Archivo de prensa. www.karisma.org.co/compartirnoesdelito/?page_id=239

[45]The United Nations 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 Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information. (2011, 1 June). *Joint Declaration on Freedom of Expression and the Internet.*

Programs and their Impact on Freedom of Expression,[46] and the International Principles on the Application of Human Rights to Communications Surveillance,[47] among others, when developing measures that restrict fundamental rights.

- Judicial capacities should be strengthened, especially in regard to understanding of the internet, so that judicial interpretation is consistent with international human rights standards applicable to the internet.
- The authorities should develop and implement models of participation that take into account the points of view of different stakeholders related to the internet, such as civil society, academia and the technical community. Widening the discussion to include these groups will increase the legitimacy of policies for the regulation of the internet. It is worth pointing out that there have already been positive advances in terms of internet governance.
- Civil society should be vigilant of legislative, judicial and administrative developments that affect the internet, in order to seek effective participation and consolidate its role as an interlocutor with the relevant authorities in the creation and implementation of policies affecting the internet. This should be accompanied by advocacy efforts, based on research and in accordance with local needs and international debates around the internet.
- Civil society should also promote and expand local, regional and international support networks to amplify its voice in defence of human rights in digital spaces and unite its efforts and knowledge on issues shared by different countries.

[46]United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights. (2013, 21 June). *Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression.*

[47]https://en.necessaryandproportionate.org/text