Submission to the study on private ICT sector responsibilities

Introduction

Founded in 2003, the Center for Technology and Society (CTS/FGV) aims to study the legal, social and cultural implications resulting from the advancement of information and communication technologies. CTS/FGV produces academic research and policy papers that may impact the development of public policies, so they will uphold democracy, fundamental rights and the preservation of the public interest. The four lines of research developed by the Center are: Creative industries, culture and access to knowledge; Internet governance and Human Rights; Digital democracy, communication and participation.

Among other networks, CTS/FGV is part of the IGF Dynamic Coalition on Platform Responsibility [1] and since 2014 has been developing a project on corporate responsibility of online platforms. The project "Terms of Service and Human Rights" developed a methodology to analyse the degree of protection of privacy, freedom of expression and due process offered by the Terms of Service (ToS) of a variety of online platforms. Some of the main goals of the project are to: (i) trigger international debate on the role of online platforms' providers as cyber-regulators and on their responsibility to respect human rights; (ii) produce evidence on the impact of ToS on individuals' human rights; (iii) encourage platform responsibility and foster a competition environment based on the respect of human rights standards; (iv) encourage governance mechanisms grounded on the respect of three fundamental components of the rule of law online: privacy, freedom of expression and due process and (v) stimulate the formation of a community to discuss and develop projects on the subject.

The Center for Technology and Society welcomes the initiative of the United Nations Special Rapporteur on the Protection and Promotion of the Right to Opinion and Expression to raise debate on the private sector's responsibility to protect freedom of expression. We are pleased to submit a contribution to the call on "Freedom of expression and the private sector in the digital age", which currently is a central topic in Internet Governance. We remain available to offer complementary information in any of the subjects discussed below, as well as to develop further studies in relation to the project.

Specific questions

At a minimum, the actors within the ICT sector that implicate freedom of opinion and expression include search engines and data processors, social media, news media, Internet Service Providers (ISPs), telecommunications providers, e-commerce, surveillance and cybersecurity firms. The Special Rapporteur would welcome input that identifies the ways in which these *or other* private corporate actors implicate freedom of expression.

Besides the listed corporate actors, others might impact on the right to freedom of opinion and expression in the digital environment. They include e-mail and cloud services, instant messaging apps, browsers and other types of software, domain name providers, advertising companies, etc. One possible way of classifying these services would be according to the three main layers in which the Internet is structured.

In the infrastructure layer, for instance, network operators have the possibility to implement directly their terms of service via Internet traffic management practices. Blocking or throttling packets, as well as creating "fast lanes" may have a detrimental effect on the freedom to receive and impart information. In the logical layer, ICANN develops policies that guide the introduction of new gTLDs into the domain name system. Domain names often entail expressive and communicative elements, and controversies on whether to approve the creation of new gTLDs such as .fail, .sucks or .islam, reveal the impact that ICANN's policies may have on freedom of expression. Moreover, the process to evaluate community applications has led to some quite controversial results. The new gTLD .gay was assigned to a company instead of to the applicants from the gay community. This causes an impact on freedom of expression and freedom of association. ICANN's policies and dispute resolution mechanisms have to be adopted by domain name registries and registrars as a condition to their accreditation to the ICANN system. Finally, in the crossing of logical and content layers, a number of online platforms regulate their cyberspaces through comprehensive terms of service that users can only accept on a "take-it-or-leave-it" basis. These actors heavily influence – either through their policies or their algorithms - the conditions in which expression will take place online. And with the emergence of the so-called Internet of Things (IoT), several non-traditional ICT industries might also start to interact with ICT companies and impact on the right to freedom of expression online. In this scenario, there is a clear need for further empirical studies aimed at understanding the characteristics of this diversity of actors and their impact on freedom of expression. However, beyond the particularities of each specific service, it seems like some issues are relevant for all – or at least most – of them.

First, there is a general need for more transparency from corporations in terms of (i) the type of user generated content that is allowed in a particular service (especially in the case of social networks, email and storage services, etc.); (ii) the algorithms and parameters that determine the classification of content (especially in the case of search engines, social networks, news media); (iii) the type of content that might be found in a particular service, especially if it can be offensive or inappropriate to particular groups of people (e.g. children, religious groups, etc.) as well as about content that will not be found because of any of the companies' policies; (iv) information about content that was removed or is being promoted (e.g. advertising) with a clear differentiation between sponsored advertising, news and user generated content; (v) details on the implementation of Internet traffic management practices.

Second, these actors should observe the due process in their practices with both the creation of alternative mechanisms for the resolution of conflicts and the promotion of access to justice. This should include:

- Meaningful notice about requests for removal of content generated by the user, including the justification for such, and right to be heard before the takedown;
- Clear mechanisms for reporting abusive content followed by meaningful notification about the procedures that are being taken, including about the possibility of the request for removal being challenged and instructions on other ways the victim can protect herself in case the content is not removed;
- Meaningful notice and right to be heard before the termination of account for violation of the contract or any other reason;
- Notice about any changes on the contract, particularly if they are meaningful (i.e. affecting the users' rights and obligations);

- The right of users to go to courts in their own jurisdiction and under their countries' legislation.

It is worth noting that several factors influence companies' interference in freedom of expression. In that sense, the State has also played a role in pushing companies to restrict freedom of expression online, especially in countries where this right is not well established as a social value. Any attempt to foster corporate's responsibility in protecting freedom of expression online should also highlight States' duty to protect free speech and to *promote* the respect for human rights by business enterprises. States should not interfere in the design of Internet services and platforms in a way that will undermine the exercise of the rights to freedom of expression and to privacy [2].

Legal and policy issues concerning the ICT sector have become prominent in recent years. These include, to name a very small number of examples, the regulation of content on all platforms and by all services and providers; acquiescence of corporate actors with government mandates or requests to take down content or services, to cooperate with government surveillance, or to localize data; the liability of intermediaries; and the security and privacy policies and technologies adopted by private actors, such as encryption. The Special Rapporteur would welcome input that identifies key legal and policy issues in the ICT sector, as well as legal and policy concerns raised by government regulation of the ICT sector, that implicate freedom of opinion and expression.

Many of the difficulties in dealing with the aforementioned legal and policy issues derive from two factors: a) the tension between a borderless Internet and a world divided into national jurisdictions; b) the attempts to enforce national laws using Internet architecture as a proxy.

The court decision that recently led to the blocking of WhatsApp in Brazil serves as a good example of the problems that these approaches may generate to freedom of expression. In the midst of a criminal prosecution, a Brazilian judge requested WhatsApp to provide information on a user who was under investigation, based on the fact that the Civil Rights Framework for the Internet (Marco Civil da Internet) requests application providers to store their logs for six months. The company repeatedly failed to comply with the court order. Facebook responded that there is no legal representation of WhatsApp in Brazil, while WhatsApp allegedly argued that it does not retain the requested information. Faced with a conundrum, the judge issued a court order determining that telecommunication companies should block WhatsApp for 48 hours. This decision was reverted by the court after 12 hours of blocking, however, the consequences of the measure on the freedom to communicate were profound. WhatsApp is used by 90% of the connected population for everyday communication. It is also used by some public services to communicate with the citizens, because of the high levels of penetration of the technology.

The case shows, on the one hand, the difficulties that public authorities may face to enforce legitimate national laws and court decisions that followed due process. On the other hand, it shows how disproportionate measures - particularly those that tamper with Internet architecture -, may have detrimental consequences. On this case, telecommunication companies were requested to play the role of a private enforcer - probably even disrespecting the principle of network neutrality enshrined in the same Marco Civil. In addition to that, the case also had international consequences: the blocking in Brazil caused disruptions with the functioning of WhatsApp in Argentina and Chile. The deployment of Internet infrastructure does not necessarily correspond to

national borders and it is impossible to neatly contain the consequences of decisions such as this one in a particular jurisdiction.

On the other hand, some responses from policymakers have also been problematic, risking to undermine citizens' expression online. An example of that is a bill that is pending approval in the Brazilian Chamber of Deputies, PL 215/2015. The bill, which originally aimed at establishing more rigor in punishing crimes against honor taking place online, proposes to introduce a mandatory real name policy to access the Internet and a version of the so-called right to be forgotten in the Brazilian legal framework [3].

States have also showed concern about the power that corporations have in determining the rules that will apply online. In that sense, policymakers have also tried to intervene in order to strengthen issues like transparency and due process – usually falling into the jurisdiction issues due to the global character of the Internet when trying to apply their rules. In Brazil, the Civil Rights Framework for the Internet (Marco Civil da Internet), Law No. 12.965/2014, provides that: (i) users' personal data should not be transferred to third parties without the users' freely given, informed and specific consent; (ii) users have the right to access clear and complete information about the collection, use, storage, processing and protection of their personal data which can only be used to purposes that (a) justify collection, (b) are not forbidden by law and (c) are explicitly laid down in services contracts or terms of use; (iii) users have the right to consent about the collection, use, storage and processing of personal data and that consent should be separated from other contractual clauses. According to the Law, companies' terms of use should be public and clear and, besides the above-mentioned, should include clear and full information setting forth the details concerning the protection to connection records and records of access to internet applications, as well as on traffic management practices that may affect the quality of the service provided. It also highlights that all obligations predicted in the Brazilian Consumer Protection Act are applicable to the interactions that take place on the Internet.

It remains yet to be seen how Brazilian courts will interpret some of the above-mentioned provisions of the Marco Civil. However, the Judiciary already has elements to invalidate several clauses since Law No. 12.965/2014 also determines that any contractual clause that undermines the confidentiality of private communications on the Internet or that do not provide an alternative to the contracting party to adopt the Brazilian forum for resolution of disputes arising from services rendered in Brazil should be declared null.

Finally, the global character of the Internet has also raised other concerns such as with the need for plurality and diversity. Especially in sectors that are subject to network effects and therefore highly concentrated such as social media, it seems important to think about mechanisms to foster competition and a diverse environment. While it could be argued that everyone has the opportunity to express themselves in these media, they have their own rules that limit certain types of expression. These rules are often associated with cultural or moral values that usually reflect their origins or the culture of the majority of it's public, which may impact on the expression of minorities or local cultures. [4]

The Special Rapporteur is aware of a wide range of existing projects that identify relevant human rights principles or obligations of the private ICT sector, and he would welcome input that identifies those projects as well as strengths or weaknesses of existing approaches.

Several studies have shown that Internet companies' policies are often complex, long and difficult for the average user to understand. They are usually distributed into more than one page and can be complemented by help pages, tutorials, Q&A, etc., which, despite not being effectively part of the contract, may specify or contradict its terms. In addition, the use of excessively legal and often vague terms also makes it harder for the average user to understand the terms she is accepting. At the same time, however, the length and complexity of a company's terms of use, privacy policies or other policies do not always reflect transparency in terms of their practices to their users. When it comes to the consent for the collection, use, storage and processing of personal data, terms usually ask for a general "take it or leave it" consent.

The Terms of Service and Human Rights Project ran by the Center for Technology and Society at Fundação Getúlio Vargas Law School in Rio de Janeiro (CTS/FGV), developed a methodology to analyse the degree of protection of privacy, freedom of expression and due process offered by the Terms of Service (ToS) of a variety of online platforms. The standards identified as a basis for the methodology derive from existing international human rights documents, including most notably the Council of Europe's Guide to Human Rights for Internet Users. Between September 2014 and May 2015, the Project has analysed the policies of a corpus of 50 platforms in a pilot experience aimed at enhancing the methodology and to identifying the main practices adopted by platform providers. Preliminary results bring evidences that confirm some of the issues pointed out before:

- More than 60% affirm on their ToS that they track users in other websites and 75% that allow third party tracking on their own websites;
- Around half of the platforms do not have clear information on their ToS regarding the aggregation of personal data between different services or across devices, making it difficult for the user to know how her data is being used;
- Most platforms share data with third parties for various reasons (commercial, technical, etc.) but usually do not specify the recipients of that data;
- Although around 60% of the platforms offer information about how to report inappropriate content, most did so only for copyright violations and specified the DMCA mechanism without giving further information on how to report other type of offenses;
- Around half of the platforms had no information on the encryption of content or personal information transmitted or stored. Although 42% affirm on their ToS that they will encrypt transmitted data, most did so only for certain type of data such as credit card information;
- Only one third of the platforms explicitly say they allow anonymity. Most platforms have no information on this;
- Only 11% of the platforms analyzed commit to sharing data for law enforcement or judicial purposes only following a specific legal process on their ToS;
- Only one third of the platforms commit to issuing prior notice before making changes to the ToS;
- Almost half of the platforms (44%) reserve themselves the right to terminate its' services (for all customers) without prior notice and 86% to terminate the account of a particular user without notice;
- Just 22% of the platforms say on their policies they will allow users to access the ToS they originally agreed and around 70% give no information on that;
- 85% of the platforms impose on their contracts a specific jurisdiction for judicial disputes;

- Almost half of the platforms affirm they will scan, filter, block or remove content for unspecified, unclear or undetermined reasons;
- Half of platforms also reserve the right to takedown user generated content after request without notice.

The complete report with the final results of the project should be launched in March. The center is also planning to develop a second phase focused on the Internet of Things and its interaction with the so-called "smart cities".

Besides the Terms of Service & Human Rights Project, together with the IGF Dynamic Coalition on Platform Responsibility the CTS/FGV has also developed Recommendations on Terms of Service and Human Rights [5], which aims at offering guidelines for companies in developing their policies in accordance with international human rights standards for freedom of expression, privacy and due process.

Conclusion

The increasing reliance on a variety of intermediaries makes the Internet a hyper-regulated environment where both national legislations elaborated by "traditional" sovereigns and private ordering defined by a new wave of private sovereign (Lessig, 1999; MacKinnon, 2012; Belli, 2016) shape the Internet experience of the regular user. Particularly, the Snowden revelations seem to have called the general public's attention to something that has always been in the core of the Internet architecture: the fact that all communications and activities taking place online require the intermediation of a number of private entities that unilaterally regulate a myriad of essential components of the Internet structure. In this context, it is unquestionable that private corporations have an important role in guaranteeing freedom of expression online.

The responsibility of private undertakings to respect human rights is explicitly recognized in the United Nations' Guiding Principles on Business and Human Rights, which also affirm their joint duty with States to provide effective remedies against violations. However, a definition is missing of the standards against which such responsibility can be measured in the context of online platforms. In that sense, international guidelines at the UN level could help stimulating companies' corporate responsibility, as well as giving the private sector references in how to be more transparent and accountable. On the other hand, this type of specific document is relevant for the development of new initiatives dedicated to fostering corporate responsibility and have an educational role for both the private and the public sector.

References

[1] See more information at http://www.intgovforum.org/cms/2008-igf-hyderabad/event-reports/74-dynamic-coalitions/1625-dynamic-coalition-on-platform-responsibility-dc-pr.
[2] Examples of attempts to intervene in the design of Internet services are the demands for the implementation of filters against child pornography or copyright violating material or for backdoors in encrypted technologies. About the later, a coalition of organizations has organized a letter in defense of encryption, for more information see https://securetheinternet.org.
[3] For more information about the PL215/2015, see Danny O'Brien's article https://www.eff.org/deeplinks/2015/10/brazils-terrible-pl215 and a joint study done by Brazilian scholars http://www.internetlab.org.br/wp-content/uploads/2015/10/Nota-t%C3%A9cnica_CTS-GPOPAI-ILAB.pdf (in Portuguese).

[4] The deletion of a picture of an indigenous couple from the Ministry of Culture Facebook page in 2015 raised a debate about this in Brazil. The minister interpreted the fact as a threat to national sovereignty and a disrespect to the national culture and started a judicial process against Facebook. For more information see http://agenciabrasil.ebc.com.br/cultura/noticia/2015-04/ministerio-da-cultura-aciona-facebook-por-censurar-foto-de-casal-indigena (in Portuguese).
[5] The Recommendations can be found at http://review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-platform-responsibility-dc-pr/.