# Terms of Service and Human Rights: an Analysis of Online Platform Contracts

# Terms of Service and Human Rights: an Analysis of Online Platform Contracts

Jamila Venturini
Luiza Louzada
Marilia Maciel
Nicolo Zingales
Konstantinos Stylianou
Luca Belli

Editora Revan

*Coordination and Revision:*
Flávio Jardim

*Translation*
Cibeli Hirsch

*Book Cover*
Mariana Vianna Abramo

*Printing*
(On off-set 75g paper, after eletronic paging in Bembo ITC, c. 11/13)
Divisão Gráfica da Editora Revan

Cip-Brazil. Cataloguing-in-source
National Union of publishers of books, RJ

T298

Terms of service and human rights: an analysis of online platform contracts / Jamila Venturini ... [et. al.]. - 1. ed. - Rio de Janeiro : Revan, 2016.
148 p. ; 21 cm.

*Translation* of: Termos de uso e direitos humanos: uma análise dos contratos das plataformas online

Includes bibliography and index
ISBN 978-85-7106-574-1

1. Communication and technology-social aspects.
2. Information technology. I. Venturini, Jamila. II. Title.

16-37692 CDD: 079
CDU: 07

09/11/2016 10/11/2016

# Table of Contents

**List of tables.....8**

**Preface.....11**

**Introduction.....13**

**Background.....17**

1. The role of internet intermediaries.....19

2. The role of Terms of Service in online platforms.....22

**Methodology.....27**

1. Criteria for the analysis of the Terms of Service.....29

1.1 Freedom of expression.....29

1.2 Privacy.....33

1.3 Due process.....39

2. Analysis.....44

2.1 Identification and storage of Terms of Service and related documents.....44

2.2 Terms of Service analysis and codification.....46

2.3 Crossing results and assigning weights to each answer.....47

2.4 Statistical analysis and computation of the level of agreement ...49

**Results.....53**

1. Freedom of expression.....53

1.1 Content monitoring, blocking, filtering and removal.....53

1.2 Information on reporting inappropriate or abusive content....56

1.3 Notification and right to be heard in case of content removal...58

1.4 Notification and possibility of questioning individual account termination .....59

1.5 Anonymity and the use of pseudonyms....60
2. Privacy....61
2.1 Minimization of data collection ....61
2.2 Viewing and copying personal data available on the platform....63
2.3 Editing and deletion of personal data ....63
2.4 Permanent account deletion ....65
2.5 Permanent deletion of personal data ....65
2.6 Scanning of private communications ....66
2.7 Tracking users' activities on other websites ....67
2.8 Third-party tracking ....69
2.9 Data retention ....71
2.10 Data aggregation from different services ....73
2.11 Data aggregation from different devices ....74
2.12 Data sharing for commercial reasons ....75
2.13 Data sharing for processing or technical reasons ....76
2.14 Data sharing for other purposes ....77
2.15 License on shared content ....79
2.16 Encryption ....80
2.17 Data sharing with government or law enforcement authorities ....82
3. Due process ....83
3.1 Notification requirements for changes in the Terms of Service ....83
3.2 Notification requirements before termination of services ....84
3.3 Availability of earlier versions of contracts ....85
3.4 Conflict resolution among users ....86

3.5 Conflict resolution between users and platforms .....87
3.6 Right to present a class action .....87
3.7 Mandatory arbitration for dispute resolution .....88
3.8 Imposition of specific jurisdiction for dispute resolution .....90
3.9 Other limitations on the access to justice .....91

**Final remarks.....93**

1. General remarks on plataform Terms of Service .....93
2. Specific remarks .....96
2.1 Freedom of expression .....96
2.2 Privacy .....100
2.3 Due process .....103

**Conclusion .....107**

**References .....108**

**News.....112**

**Annex I - Related projects and civil society initiatives ..113**

**Annex II - Analyzed platforms and documents .....117**

**Annex III - Recomendations on Terms of Service and Human Rights .....127**

# List of Tables

**Table 1 -** Criteria for the analysis of freedom of expression and specific references on international human rights documents - P. 31

**Table 2 -** Criteria for the analysis of privacy and specific references on international human rights documents - P. 35

**Table 3 -** Criteria for the analysis of due process and specific references on international human rights documents - P. 41

**Table 4 -** Reference table for crossing responses of three independent coders and their assigned weight - P. 48

**Table 5 -** Level of agreement of the three coders by analysis criterion - P. 49

**Table 6 -** Aggregated results and level of agreement regarding content analysis, blocking, filtering or removal - P. 54

**Table 7 -** Aggregated results and level of agreement regarding the existence of clear information on how to report inappropriate or abusive content - P. 57

**Table 8 -** Aggregated results and level of agreement regarding notice and right to be heard in case of content removal - P. 58

**Table 9 -** Aggregated results and level of agreement regarding notice and possibility of questioning individual account termination - P. 59

**Table 10 -** Aggregated results and level of agreement regarding anonymity or the use of pseudonyms - P. 60

**Table 11 -** Aggregated results and level of agreement regarding data collection minimization - P. 61

**Table 12 -** Aggregated results and level of agreement regarding the possibility of viewing and copying personal data available - P. 63

**Table 13 -** Aggregated results and level of agreement regarding the possibility to edit and delete personal data - P. 64

**Table 14 -** Aggregated results and level of agreement regarding the possibility of permanent account deletion - P. 65

**Table 15 -** Aggregated results and level of agreement regarding the possibility of permanent deletion of personal data - P. 66

**Table 16 -** Aggregated results and level of agreement regarding the scanning of private communications - P. 66

**Table 17 -** Aggregated results and level of agreement regarding the tracking of user activities in other websites - P. 68

**Table 18 -** Aggregated results and level of agreement regarding third-party tracking - P. 69

**Table 19 -** Aggregated results and level of agreement regarding data retention - P. 72

**Table 20 -** Aggregated results and level of agreement regarding data aggregation from different services - P. 74

**Table 21 -** Aggregated results and level of agreement regarding data aggregation from different devices - P. 74

**Table 22 -** Aggregated results and level of agreement regarding data sharing for commercial reasons - P. 76

**Table 23 -** Aggregated results and level of agreement regarding data sharing for processing or technical reasons - P. 77

**Table 24 -** Aggregated results and level of agreement regarding data sharing for other purposes - P. 78

**Table 25 -** Aggregated results and level of agreement regarding the imposition of broad licenses on shared content - P. 80

**Table 26 -** Aggregated results and level of agreement regarding the encryption of transmitted information - P. 81

**Table 27 -** Aggregated results and level of agreement regarding the encryption of stored information - P. 81

**Table 28 -** Aggregated results and level of agreement regarding data sharing with government and/or law enforcement authorities - P. 83

**Table 29 -** Aggregated results and level of agreement regarding the need of notification before changing terms - P. 84

**Table 30 -** Aggregated results and level of agreement regarding the need of notification upon termination of services - P. 85

**Table 31 -** Aggregated results and level of agreement regarding the availability of previous versions of contracts - P. 85

**Table 32 -** Aggregated results and level of agreement regarding the existence of alternative mechanisms for dispute resolution among users - P. 86

**Table 33 -** Aggregated results and level of agreement regarding the existence of alternative mechanisms for dispute resolution between users and platforms - P. 87

**Table 34 -** Aggregated results and level of agreement regarding the possibility to start a class action - P. 88

**Table 35 -** Aggregated results and level of agreement regarding mandatory arbitration - P. 88

**Table 36 -** Aggregated results and level of agreement regarding the imposition of specific jurisdiction for dispute resolution - P. 90

**Table 37 -** Aggregated results and level of agreement regarding the existence of other limitations the access to justice - P. 91

# Preface

For many years, the Council of Europe has been developing instruments which address the challenges of the Internet with the underlying premise that human rights prevail over the general terms and conditions imposed on Internet users by companies.

The findings of this report, partly based on the Council of Europe's Guide to Human Rights for Internet Users, demonstrate just how difficult it can be for Internet users to understand and thereby consent to the terms of service of online platforms in order to make fully informed decisions on issues which affect their human rights such as content restriction policies and the processing of personal data.

The report is therefore a valuable source of reference for the Council of Europe's human rights work on intermediary liability, algorithms, and the development of standards for the blocking, filtering and takedown of illegal Internet content.

Dialogue and co-operation with the private sector is becoming ever more important when dealing with the fast pace of technological change. In line with the UN's Guiding Principles on Business and Human Rights, the Council of Europe is establishing partnerships with Internet companies to promote respect for human rights and the rule of law online.

Moreover, the importance of close co-operation with research and academic communities in the field of the information society can hardly be overstated. These and other multi-stakeholder partnerships are essential for the implementation of the Council of Europe's Internet Governance Strategy 2016-2019.

*Jan Kleijssen*

Director of Information Society and Action against Crime

# INTRODUCTION

This report presents the results of the research carried out for the "Terms of Service and Human Rights" project developed by the Center for Technology and Society of Fundação Getulio Vargas Rio de Janeiro Law School (CTS/FGV). Founded in 2003, CTS/FGV aims to study the legal, social and cultural implications arising from the advancement of information and communication technologies. It focuses on academic research and science dissemination that may impact the creation of public policies committed to democracy, fundamental rights and the protection of public interests regarding technological progress.

The project was developed between September 2014 and March 2016, and analyzed the Terms of Service of 50 online platforms, by assessing how they deal with the human rights to, freedom of expression, privacy, and due process. The goals of the project were to (i) prompt international debate on the role of platforms as regulators in the online environment and their responsibility to respect human rights; (ii) produce evidence of the impact of Terms of Service on the human rights of Internet users; (iii) encourage the responsibility of platforms through competition, based on the respect for international human rights standards; (iv) encourage governance mechanisms based on respect for freedom of speech, privacy and due process, and (v) trigger the creation of a community devoted to discussing and developing projects on corporate responsibility in the information and communication technologies (ICT) sector.

The research originated from a partnership with the Dynamic Coalition on Platform Responsibility (DCPR) of the United Nations' Internet Governance Forum, which is multistakeholder group aimed to discuss the notion of responsibility of online platforms, in

particular with respect to internationally recognized human rights. In parallel with the development of this project, the DCPR produced a set of recommendations on Terms of Service and Human Rights[1, 2], which promote the adoption of "responsible" Terms of Service as a means for online platforms to ensure respect for the rights to freedom of expression, privacy and due process.

The following steps were taken to conduct the project "Terms of Service and Human Rights": (i) elaboration of an analysis methodology based on international human rights documents; (ii) analysis of the Terms of Service of 50 online platforms by three independent analysts[3]; (iii) crossing the results of the three analyses and statistical treatment; (iv) development of conclusions and recommendations. The project analyzed the Terms of Service's impact on users' rights to freedom of expression, privacy and due process and the corporate responsibility of platforms to respect and protect human rights.

Preliminary research results were discussed in several national and international events such as the conference for the International Human Rights Day held by the Council of Europe in Brussels in December 2014; the seminar "Human Rights in the Digital Environment: Perspectives on Terms of Service"[4], held at FGV

1 See DCPR (2015) Recommendations on the Terms of Service and Human Rights. Presented at the 10th United Nations Internet Governance Forum: <http://review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-platform-responsibility-dc-pr/>.

2 Translator's note: excerpts of documents written in British English were maintained in their original form throughout the translation.

3 In addition to researchers from CTS/FGV, two analysts at Tilburg University, working independently, participated in the Terms of Service analysis under the coordination of researcher Nicolo Zingales.

4 More information about the event can be found at: <http://direitorio.fgv.br/eventos/direitos-humanos-no-ambiente-digital-perspectivas-sobre-termos-de-uso>. To watch the full seminar, access FGV Rio de Janeiro Law School's channel on YouTube: <https://youtu.be/Jy_uqjgdFPo>.

Rio de Janeiro Law School, in December 2014 and the World Forum for Democracy, promoted by the Council of Europe and the European Parliament in Strasbourg, in November 2015. The project called for the attention of representatives of Internet companies, civil society and government representatives.

This book is structured as follows: (i) introduction, which discusses the role of intermediaries in providing Internet services and how their Terms of Service influence users' activities; (ii) methodology, which describes the basis for understanding the rights to freedom of expression, privacy and due process in an online context; (iii) results, which map trends identified in the Terms of Service of analyzed online platforms; and (iv) final remarks and conclusion.

# Background

As acknowledged by the Guiding Principles on Business and Human Rights, endorsed by the United Nations Human Rights Council in June 2011[5], the activities of companies can have an impact on virtually the entire international human rights spectrum. Therefore, companies are responsible for respecting and protecting these rights, that is, "to refrain from infringing human rights and addressing the negative impacts on human rights in which they have some involvement".

Such responsibility should be taken through political commitments, voluntary initiatives of private players and appropriate procedures, to show that a company is considering the potential impacts of its activities on human rights, is committed to minimizing them, and is providing redress mechanisms in the event of abuses or violations. Moreover, the principles state that companies must comply with applicable laws and with internationally recognized human rights wherever they operate, and in all contexts, seek ways to honor human rights when faced with conflicting requirements, while considering the risks of causing human rights violations as part of legal compliance.[6]

---

5 The document "Guiding Principles on Business and Human Rights" can be found at: <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

6 The document states that "23. In all contexts, business enterprises should: (a) Comply with all applicable laws and respect internationally recognized human rights, wherever they operate; (b) Seek ways to honor the principles of internationally recognized human rights when faced with conflicting requirements; (c) Treat the risk of causing or contributing to gross human rights abuses as a legal compliance issue wherever they operate".

A number of initiatives and projects developed by the civil society and governmental organizations highlighted the role of the private sector in protecting and respecting human rights within the online environment (see Annex I), once private agents are responsible for conveying information on the Internet by providing access, hosting, transmitting and indexing content. In the A/HRC/17/27[7] report, the UN Special Rapporteur on Freedom of Opinion and Expression stressed that, despite their freedom of initiative, companies providing online services have a corporate responsibility to respect human rights[8] and recommends that they (i) only implement restrictions to the rights to freedom of expression and privacy after judicial intervention; (ii) are transparent about the measures taken; (iii) minimize the impact of any

[7] The document was based on consultations carried out with several countries between 2010 and 2011 and its main concern was the increasing threats to the exercise of freedom of expression on the Internet around the world. Although the recommendations of the UN Special Rapporteur on Freedom of Opinion and Expression do not have a binding nature, both Member States and national and international courts are expected to consider its reports and suggestions when dealing with cases related to the right to freedom of expression (Zingales, 2013).

[8] This understanding is enshrined in the Brazilian doctrine and case-law precedents by the theory of horizontal efficiency of fundamental rights, which recognizes that fundamental rights must be respected and protected not only in public law, but also in private law relations. As argued by Sarmento and Gomes (2011), "it seems undisputed that, if oppression and violence against a person come not only from the State, but from multiple private actors present in spheres such as the market, family, civil society and companies, the incidence of fundamental rights in the sphere of relations among individuals becomes an unavoidable imperative. This need is even more urgent in social contexts characterized by severe social inequality and power asymmetry, such as in Brazil. In scenarios such as ours, the exclusion of private relations from the fundamental rights impact radius mean the serious mutilation of these rights, reducing their ability to protect and promote dignity of human beings".

restrictions only to the relevant content and, where possible, (iv) notify users before implementing restrictive measures. Similarly, the Guide to Human Rights for Internet Users of the Council of Europe determines that, to ensure that existing human rights are equally applied both offline and online, States should encourage the private sector to exercise their corporate responsibility, in particular with regard to transparency and accountability[9].

Next, a brief description of the peculiarities of the digital environment will be presented, highlighting the role of private intermediaries in communications, and how Terms of Service regulate the use of online platforms. In addition, the concept of online platforms and how they can impact freedom of expression rights, privacy and due process will be discussed.

## 1. The Role of Internet Intermediaries

The prominence of private intermediation in the Internet environment is remarkable. Data traffic between senders and receivers requires the existence of a number of private agents in infrastructu-

[9] Recommendation CM/Rec(2014)6 of the Council of Europe on the Guide to Human Rights for Internet Users extends to the online environment the obligation of Member States to guarantee human rights and fundamental freedoms in their jurisdictions and to respect the conventions and instruments of the Council of Europe on the right to freedom of expression, access to information, freedom of association, protection against cybercrime, privacy and personal data protection in the online environment. Other international organizations have drawn attention to the same point. In the American sphere, the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights of the Organization of American States (OAS) published, in 2013, the report "Freedom of Expression and the Internet" which includes principles to guarantee human rights, especially freedom of expression and privacy, in the online environment.

ral, logic and content layers[10]. Thus, they are largely responsible for the full exercise of freedom of expression, that is, the right to seek, receive and share information and ideas over the Internet[11].

From the late 1990s to early 2000s, the Internet was considered as a tool able to directly connect users to providers, buyers to sellers, the public to authors, thereby eliminating a number of traditional intermediaries in a phenomenon identified then as "disintermediation". However, it seems more correct to say that the Internet does not determine disintermediation, but that it encourages the emergence of new intermediaries, which replace some of the agents who played essential roles before the Internet era (OECD, 2010; OECD, 2011). What can be observed is what some authors have called a phenomenon of "hypermediation"[12], with the emergence of a wide range of particularly powerful private entities with the ability to regulate access and dissemination of information through private agreements, and to collect large amounts of personal information about users and their activities.

According to the Organization for Economic Co-operation and Development (OECD), the role of intermediaries is key for the digital infrastructure. They offer significant social and economic benefits, by providing Internet access, allowing online commerce, and facilitating communication through social networks,

---

[10] The Internet is made up of three main layers: (i) a physical infrastructure, consisting of the set of electronic networks that allow communication; (ii) a logic layer, i.e., protocols and applications, which allows searching, sharing and accessing information and ideas, and; (iii) a content layer, i.e., the set of information and ideas that are available online. See: Y. Benkler, "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access", Federal Communications Law Journal, vol. 52, 2000.

[11] See: R. MacKinnon, E. Hickock, A. Bar, H. Lim, "Fostering Freedom Online: The Role of Internet Intermediaries" (UNESCO Publication, 2014). Available at: <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>.

[12] See: N. Carr (2009). "Googler in the Middle". *Rough Type.* Available at: <http://www.roughtype.com/?p=1249>.

participatory networks and various web services[13], thereby contributing to the economic growth and facilitating transactions among third parties on the Internet[14]. Similarly, the UN Special Rapporteur on Freedom of Opinion and Expression highlighted the key role that the private sector plays, acting as a facilitator of freedom of expression and strengthening the individual participation in the economic, social, cultural and political spheres. However, despite such benefits, intermediates can also use technology to restrict human rights, by setting the Internet's infrastructure in such a way as to allow censorship, mass surveillance and even state intrusion.[15]

Besides facilitating communication among users, intermediaries also play the role of Internet gatekeepers[16], exerting a form of sovereignty over networks and platforms, through their logic architecture (codes or algorithms) and rules that are set and controlled exclusively by them (Lessig, 1999; MacKinnon, 2012; Belli,

[13] See: OECD (2011) The Role of Internet Intermediaries in Advancing Public Policy Objectives DSTI/ICCP(2010)11/FINAL. Available at: <http://www.oecd.org/internet/ieconomy/48685066.pdf>.

[14] OECD. (2010). The Economic and Social Role of Internet Intermediaries. Available at: <http://www.oecd.org/internet/ieconomy/44949023.pdf>.

[15] La Rue, F. 17 April 2013. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". Office of the United Nations High Commissioner for Human Rights. (A/HRC/23/40). pp. 19-20. Available at: <www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>.

[16] See: Zittrain. J. (2006). "A History of Online Gatekeeping". Harvard Journal of Law & Technology. Vol. 19, No. 2, pp. 253-98. Available at: <http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf>. E Pasquale F.A. (2010). "Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries". Northwestern University Law Review. Vol. 104, No. 1, p. 105. Available at: <www.law.northwestern.edu/lawreview/v104/n1/105/LR104n1Pasquale.pdf>.

2016). Contractual conditions governing the relationship between online services and their users are defined by Terms of Service, which can be considered as the actual "law of the platform" (Belli & De Filippi 2012; Belli 2016), defined and implemented unilaterally by service providers. Such contractual rules can limit the spread of certain types of content and condition the participation of users to provide a range of information about their activities.

## 2. THE ROLE OF TERMS OF SERVICE IN ONLINE PLATFORMS

Different organizations and players use various terms to refer to the so-called online platforms, depending on the subject area within which these platforms are discussed. In an economic sense, for example, a platform is the entity that allows or facilitates the interaction between two sides in a market[17]. According to the European Commission, "[o]nline platforms can be described as software-based facilities offering two-or even multi-sided markets where providers and users of content, goods and services can meet. As such, the term can cover a wide range of different types of platform, whose functions and characteristics can differ considerably. Examples of types of platforms include: communications and social media platforms; operating systems and app stores; audiovisual and music platforms; e-commerce platforms; content platforms, which may include content aggregators as well as software/hardware solutions; and search engines. [...] Since the value of these platforms to consumers increases with their size (network effects), they may in

[17] *"A market is two-sided if at any point in time there are: i) two distinct groups of users; ii) the value obtained by one type of user increases with the number or with the "quality" of the other kind of user; and iii) an intermediary platform is necessary to internalize the externalities created by one group for the other group. Examples include Internet search engines and portals composed of advertisers and users; retail e-commerce platforms composed of buyers and sellers; and payment networks composed of cardholders and merchants"*. See: OECD 2011, pp. 28-29.

some cases become very large and act as key players for the wider Internet[18]. To make an analogy, an online platform is an application that allows users to search, receive and disseminate information and ideas through the Internet[19].

Any person attempting to register in any online platform will probably be faced with the need to agree to the following statement: "I have read and accept the Terms of Service". "Terms of Use" or "Terms of Service" are the agreements governing the relationship between users and service providers in the online environment[20]. They are usually accompanied by other documents such as privacy policies, cookies policy, community standards, among others.

Terms of Service are standardized contracts, defined unilaterally and offered indiscriminately on equal terms to any user. Since users do not have the choice to negotiate, but only accept or reject these terms, Terms of Service are part of the legal category of adhesion agreements. In fact, these agreements establish a kind of "take it or leave it" relationship, replacing the traditional concept of bargained clauses among contracting parties (Lemley, 2006).

Once a user accepts the terms, and in line with the civil law principle that a contract must be respected by the parties *(pacta sunt servanda),* both are obliged to fulfill what is agreed therein and the company's policies are binding upon the user. Even in cases when an explicitly agreement with the Terms of Service is not required, the relationship between users and service providers will be governed by such a standardized contract, considering the interpretation that, by using the services, users agree with the

---

18 See European Commission. (2015). A Digital Single Market Strategy for Europe - Analysis and Evidence, COM (2015) 192, p. 52.

19 See DCPR (2015).

20 As stated by Bygrave (2015), the use of contracts to regulate Internet activities refers to the very origins of the network and the influence of research funding agencies in the United States. According to the author, contracts have become popular because they are easy to elaborate and distribute to a large number of anonymous users.

company's policies, even if they have not expressly stated so (tacit consent). Similarly, there are instances in which Terms of Service explicitly state that the mere use of the service constitutes acceptance of the contract (consent by performance).

Since such terms are generally long, dense and formulated in language that is hard to be understood by anyone who does not have legal training (Bygrave, 2015), people hardly ever read these contracts (Loren, 2004). When they do, they find them difficult to understand (Bakos, Marotta-Wurgler & Trossen, 2013). This scenario is even more problematic in the online environment, both because these contracts are written in fine-print in an environment in which color pictures stand out over texts (Kim, 2012) and because the situations in which customers come across with contracts of this sort became increasingly abundant[21, 22].

This scenario seems to point to a market failure characterized by the fact that potential customers do not take into account contractual terms to make their decisions. This dynamic would incentivize vendors and service providers to commit to no more than the minimum required by law, and draw up terms with "anti-social" standards (Bygrave, 2015, p. 31), biased against users, (Bakos, Marotta-Wurgler & Trossen, 2013) and failing to meet their legitimate expectations.

Some theories, guided by free-market principles, seek to reject such concerns on the basis that a minority of users who actually read and understand Terms of Service could ensure a control against any unfair terms. When drafting Terms of Service, companies would take into account this informed minority, thus raising their quality. One can criticize the lack of empirical evidence of

[21] According to a study carried out by the Carnegie Mellon University, in the United States, a user would have to set aside eight daily hours during 76 days only to read the privacy policies of an average of 1,462 pages visited in one year (McDonald & Cranor, 2008).

[22] The web campaign called *The biggest lie* draws attention to the unsustainability of this contract model in the Internet. Visit: <http://www.biggestlie.com> for more information.

this theory, especially in the face of a study that found, based on a significant sample, that in the online software purchase and sale market, very few consumers – between 0.5% and 0.22% – read adhesion contracts, the so-called *End User License Agreements* or *EULAs* (Bakos, Marotta-Wurgler & Trossen, 2013). The conclusion is that even if the validity of the theory of informed minority is taken into consideration, such a small group of users would be insufficient to control the clauses unilaterally established by the platforms and influence the terms of these agreements, which reinforces the concern with this type of regulation.

The scenario becomes more complex in the case of online platforms, once Terms of Service lay down the rules to publish and share content and the methods of collecting and processing personal data. Thus, more than regulating consumer relations, these contracts now have concrete implications on the implementation of human rights.

In Brazil the effect of unfair terms is mitigated by a restrictive interpretation of the principle of autonomy[23], incorporated in the Brazilian Consumer Protection Act (art. 51, Law 8078/1990), in case of any breaches resulting from the implementation of unfair terms, the aggrieved party should seek the recognition of his rights in court, which may be too costly for the user.

International organizations have expressed their opinions on the Terms of Service of online platforms. The UN Special Rap-

[23] The horizontal effect of fundamental rights in Brazilian doctrine and court precedents diverges from the American doctrine of state action, in which the autonomy of will is treated completely differently. While in Brazil fundamental rights enshrined in the Constitution guide the whole application of private law, in the US, fundamental rights are enforceable only to public authorities, based on the understanding that, conversely, freedom of association and the autonomy of independent states would be impaired, to the extent that the federal government, under the pretext of implementing the Constitution, could interfere in matters assigned to federal states, undermining their autonomy (Sarmento & Gomes, 2011).

porteur on Freedom of Opinion and Expression, for example, recommends that such terms should be clear and aligned with international human rights standards. In contrast, the Guide to Human Rights for Internet Users of the Council of Europe reaffirms that human rights prevail over the terms and conditions imposed on Internet users by any private agent and stresses that States have the obligation to respect, protect and promote human rights, as well as to supervise the private sector.

The methodology of the "Terms of Service and Human Rights" project arises from the recommendations of various international documents, notably the Guide to Human Rights for Internet Users of the Council of Europe. The following section will detail the parameters established by international human rights standards regarding freedom of expression, privacy and due process and how they were converted into a methodology for analyzing Terms of Service. In addition, the following section describes the process for analyzing Terms of Service and extracting results.

# METHODOLOGY

The methodology of the "Terms of Service and Human Rights" departed from the challenge of developing specific parameters that could assess the adequacy of the Terms of Service of online platforms regarding human rights. A number of documents developed by international organizations served as the basis for developing analysis criteria. These include treaties such as the Universal Declaration of Human Rights[24] and the International Covenant on Civil and Political Rights,[25] the American Convention on Human Rights (Pact of San José, Costa Rica)[26] and the Chapultepec Declaration.[27]

In addition, criteria were based on the structure of the Guide to Human Rights for Internet Users, elaborated by the Council of Europe, which not only consolidates a set of rights and freedoms already enshrined in the European context[28], but also reflects the principles present in the main international human rights instruments. The Guide has an important role in translating the provisions of international treaties to the online environment, in an easier and

[24] Adopted and proclaimed by Resolution 217 A (III) of the United Nations General Assembly on December 10, 1948 and signed by Brazil on the same date.

[25] Incorporated into the Brazilian legal framework by the Decree n. 592/1992.

[26] Incorporated into the Brazilian legal framework by the Decree n. 678/1992.

[27] Signed by President Fernando Henrique Cardoso in 1996 and by President Luiz Inácio Lula da Silva in 2006.

[28] The Guide is based on the European Convention on Human Rights and other conventions and instruments of the Council of Europe, such as the Convention on Cybercrime (Budapest Convention), the Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

accessible language to the user. In this sense, the influence of the Guide goes beyond the 47 member states of the Council of Europe.

Finally, criteria for the analysis were drawn from statements by the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights of the Organization of American States (OAS) and by the UN Special Rapporteur on Freedom of Opinion and Expression, on the ground that they specifically deal with the implementation of human rights in the online environment.

Although the way human rights are interpreted and implemented on the Internet varies according to the norms of each country, the first phase of project "Terms of Service and Human Rights" focused on the compliance with international human rights standards. As a result, national or regional rules on consumer protection or the protection of personal data, for example, were not considered relevant for this review. Similarly, the analysis did not focus on local versions of the Terms of Service where a platform operated, but rather on the international one (if any) or, alternatively, the English version of the Terms of Service offered on the country of origin of the platform[29]. For next phases or versions of the project, the methodology can be adapted to analyze Terms of Service compliance with local laws.

The analysis focused on the rights to freedom of expression, privacy and due process. Below are the details on the criteria for the analysis in each of these axes and the process of analysis, conducted by three independent analysts.

[29] The policies of online platforms should presumably adapt to local laws; however, the analysis conducted by this project on the Terms of Service of 50 platforms indicated that, in many cases, there was not even a version of the contract in the language of the country where the service is offered. According to an analysis carried out in February 2016, less than half the sample (21) offers all of its policies in Portuguese. The other part of the sample presents their terms fully or partially in English.

# 1. CRITERIA FOR THE ANALYSIS OF THE TERMS OF SERVICE

## *1.1. Freedom of Expression*

According to the Universal Declaration of Human Rights, the right to freedom of expression includes the freedom to seek, receive and impart information and ideas through any media, regardless of frontiers (art. 19).[30] Freedom of expression includes both speeches understood as favorable or inoffensive, as those that may offend, shock or disturb.

Like other human rights, freedom of expression is not absolute and is subject to restrictions in the case of conflicts with other rights. Under international human rights standards, any limitation to the right to freedom of expression must pass the following three-part test:[31]

1. It shall be provided for by laws which, in turn, shall be clear and accessible;
2. It shall serve to protect a legitimate interest recognized under paragraph 3, of Article 19, of the International Covenant on Civil and Political Rights,[32] i.e., protect

[30] United Nations (1948). "Universal Declaration of Human Rights". Available at: <http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf> (accessed on April 5, 2015).

[31] The three-part test derives from Paragraph 3 of Article 19 of the International Covenant on Civil and Political Rights and has been established by international doctrine and case law. The mechanism was reaffirmed as applicable in the A/HRC/17/27 report (paragraph 24) by the UN Special Rapporteur on Freedom of Opinion and Expression and the Joint Declaration on Freedom of Expression and the Internet. Available at: <http://www.oas.org /en/iachr/expression/showarticle.asp?artID=848> (accessed on February 17, 2016) as applicable in the context of the Internet.

[32] Available at: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0592.htm> (accessed on April 5, 2015).

the rights or reputations of others or protect national security, order, health and morals;

3. It shall prove necessary and the least restrictive to achieve its goal, taking into account the principles of necessity and proportionality.

According to A/HRC/17/27 report of the UN Special Rapporteur on Freedom of Opinion and Expression, censorship measures should never be delegated to private agents. It is known, however, that active monitoring measures and content blocking can occur within the Internet environment, where the transmission of information is mediated by private agents, either as a result of domestic laws, the pressure that liability for publishing certain content exerts on intermediaries, or for other reasons, such as compliance with rules of conduct set out in platform Terms of Service. In addition, some platforms implement mechanisms that allow users to report content they deem inappropriate because they violate their rights (such as privacy), local legislation (e.g., child pornography, racism, etc.) or the platform's Terms of Service. In this case, the company is responsible for deciding what can and cannot stay online. These mechanisms are known internationally as "Notice & Takedown" and are inspired by the model established by US copyright law[33].

Following the above-mentioned three-part test, Report A/HRC/17/27 recognizes that information which may be legitimately restricted includes: (i) child pornography; (ii) hate speech; (iii) defamation and (iv) incitement to violence (including genocide, discrimination and hostility toward racial and religious groups) (paragraph 25). In addition, it recommends intermediaries to notify users in advance when implementing any content restriction measure (paragraph 47).

[33] Especially the so-called *Digital Millennium Copyright Act* (DMCA), of 1998, which establishes a mechanism to remove content protected by copyrights if the author notifies platform hosting such content of the presumed violation.

The Guide to Human Rights for Internet Users reaffirms the right to freedom of expression and access to information and opinions of others in the online environment and determines that users should be informed about possible restrictions on freedom of expression, so that they can make informed decisions about their content. It also reinforces the need for mechanisms to respond to demands and complaints from users.

Based on those principles, the following criteria have been developed to identify how platforms act in relation to monitoring content, handling user reports and terminating accounts:

**TABLE 1: Criteria for the analysis of freedom of expression and specific references on international human rights documents**

| Criterion for Analysis | Reference in the Guide to Human Rights for Internet Users of the Council of Europe (English) | Reference to other international human rights documents |
|---|---|---|
| Does the platform scan, block, filter* or remove content for unspecified, undetermined or unclear reasons? | (Freedom of expression and information) 4. public authorities have a duty to respect and protect your freedom of expression and your freedom of information. Any restrictions to this freedom must not be arbitrary, must pursue a legitimate aim in accordance with the European Convention on Human Rights such as, among others, the protection of national security or public order, public health or morals, and must comply with human rights law. Moreover, they must be made known to you, coupled with informa | Inter-American Commission on Human Rights. (2013). Special Rapporteur on Freedom of Expression. Freedom of expres-sion and Internet. Paragraphs 88, 111, 112.<br>United Nations. General Assembly. Report of the Spe-cial Rapporteur on the Promo-tion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraph 76 |

* Even though platforms are advised to only restrict the right to freedom of expression after judicial intervention (see report A/HRC/17/27 of the UN Special Rapporteur on Freedom of Opinion and Expression), it is known that platforms actually implement content filtering or blocking measures to prevent the dissemination of spam and child pornography materials, for example.

| | | |
|---|---|---|
| Does the platform offer clear and transparent information on how users can report content they consider inappropriate or submit takedown requests? | and redress, and not be broader or maintained for longer than is strictly necessary to achieve a legitimate aim;<br>(Freedom of expression and information) 5. your Internet service provider and your provider of online content and services have corporate responsibilities to respect your human rights and provide mechanisms to respond to your claims. You should be aware, however, that online service providers, such as social networks, may restrict certain types of content and behavior due to their content policies. You should be informed of possible restrictions so that you are able to take an informed decision as to whether to use the service or not. This includes specific information on what the online service provider considers as illegal or inappropriate content and behavior when using the service and how it is dealt with by the provider; | United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraph 68. |
| Does the platform offer notification and the right to be heard before removing user-generated content as a result of a third-party complaint? | | Inter-American Commission on Human Rights. (2013). Special Rapporteur on Freedom of Expression. Freedom of expression and internet. Paragraphs 107, 108.<br><br>United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraphs 42, 47 and 76. |
| Does the platform provide notice and ability to challenge the decision when terminating the account of a particular user? | (Effective Remedies) 1.1. your Internet service provider, providers of access to online content and services, or other company and/or public authority should inform you about your rights, freedoms and possible remedies and how to obtain them. This includes easily accessible information on how to report and complain about interferences with your rights and how to seek redress; | United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraph 4 |

| | | |
|---|---|---|
| Does the platform allow users to remain anonymous or use a pseudonym? | (Freedom of expression and information) 6. You may choose not to disclose your identity online, for instance by using a pseudonym. However, you should be aware that measures can be taken, by national authorities, which might lead to your identity being revealed. | La Rue, Frank. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40. Paragraphs 23, 48 and 49.<br><br>United Nations. Human Rights Council. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye. A/HRC/29/32. May 22, 2015. Paragraphs 61, 62, 63. |

### *1.2. Privacy*

According to the Universal Declaration of Human Rights, "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".[34] Other documents reiterate privacy protection, such as the International Covenant on Civil and Political Rights, the American Convention on Human Rights and the European Convention on Human Rights, adding that

> there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the pro-

[34] United Nations (1948). "Universal Declaration of Human Rights". Available at: <http://www.un.org/en/universal-declaration-human-rights/> (accessed on June 6, 2016).

tection of health or morals, or for the protection of the rights and freedoms of others.[35]

Considering the impact that the automated processing of personal data can have on the right to privacy, the Guide to Human Rights for Internet Users sets out some privacy protection principles.[36] In particular, the document recommends public authorities and private enterprises to respect specific rules and procedures when processing users' personal data. According to the document, such data can only be subject to processing as provided by law or under users' consent.[37] Furthermore, users should be offered clear information on which data are processed or transfer-

[35] Council of Europe (1950). "European Convention on Human Rights". Available at: <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=536&lID=4> (accessed on February 17, 2016).

[36] It is worth noting that Europe recognizes the right to personal data protection as a fundamental and independent right. The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was the first legally binding international document on data protection. For a detailed history of the evolution of the concept of data protection in the legal systems of different countries, see DONEDA, Danilo. "Da privacidade à proteção de dados pessoais". Rio de Janeiro: Renovar. 2006.

[37] The idea of consent stems from the understanding that only data subjects can authorize the processing of their personal data and it is considered an essential condition to allow individuals to fully enjoy their right to self-determination. Its goal is to give people control over their data and the ability to make decisions about its processing, considering related costs and benefits (Solove, 2013). In Europe, under the current 95/46/EC Directive, and in Brazil, under the Civil Rights Framework for the Internet (Law 12,965/2014), consent is a condition that legitimizes personal data processing, which should be free (i.e. not forced), informed (the individual must be provided with all the information in a clear and intelligible form) and specific (in relation to a particular purpose). In the US, the idea that individuals have a number of rights which allow them to manage their personal data has prevailed since the 1970s, including notification and consent.

red to third parties, when, by whom and for what purpose. Finally, users should exercise control over their personal data, which includes the ability to verify whether they are accurate and request corrections or their permanent exclusion.[38]

As for surveillance and interception measures promoted by the State, the Guide states that interferences with the right to privacy can only occur in exceptional circumstances defined by law and that the user must know clearly and precisely which laws and policies apply accordingly.

Based on these principles, the following criteria for the analysis of Terms of Service were defined:

**TABLE 2: Criteria for the analysis of privacy and specific references on international human rights documents**

| Criterion for Analysis | Reference in the Guide to Human Rights for Internet Users of the Council of Europe (English) | Reference to other international human rights documents (in English) |
|---|---|---|
| Does the platform affirmatively minimize data collection? | (Privacy and data protection) You have the right to private and family life on the Internet which includes the protection of your personal data and respect for the confidentiality of your correspondence and communications. | Inter-American Commission on Human Rights. (2013). Special Rapporteur on Freedom of Expression. Privacy. Paragraph 131. |

[38] The UN Special Rapporteur on Freedom of Opinion and Expression recognized the importance of adopting high standards for the protection of personal information, considering the increase in the collection and processing of personal data (including communication data or metadata) in connection with online communications and the impact this may have on the privacy of individuals. See the report A/HRC/23/40 of the UN Special Rapporteur on Freedom of Opinion and Expression on communication surveillance in the exercise of human rights to privacy and freedom of opinion and expression at: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement> (accessed on February 17, 2016).

| | | |
|---|---|---|
| Is the user allowed to view and copy all the personal data available on the platform? | (Privacy and data protection) 3. your personal data should only be processed when laid down by law or when you have consented to it. You should be informed of what personal data are processed and/or transferred to third parties, when, by whom and for what purpose. Generally, you should be able to exercise control over your personal data (check its accuracy, request a correction, a deletion or that personal data is kept for no longer than necessary); | Inter-American Commission on Human Rights. (2013). Special Rapporteur on Freedom of Expression. Privacy. Paragraph 138<br><br>Declaration of Principles on Freedom of Expression of the Inter-American Commission on Human Rights (2000). Principles 3 and 8.<br><br>United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. Monday, May 16, 2011. Paragraph 58. |
| Is the user allowed to edit and delete all the personal data available on the platform? | | Declaration of Principles on Freedom of Expression of the Inter-American Commission on Human Rights (2000). Principle 3.<br><br>United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraph 58. |
| Does the platform allow full and permanent account deletion? | | |
| Does the platform allow the removal of all personal data generated by the user within a reasonable period after account deletion? | | |

| | | |
|---|---|---|
| Does the platform allow third party tracking? | (Privacy and data protection) You have the right to private and family life on the Internet which includes the protection of your personal data and respect for the confidentiality of your correspondence and communications.<br><br>(Privacy and data protection) 4. you must not be subjected to general surveillance or interception measures. In exceptional circumstances, which are prescribed by law, your privacy with regard to your personal data may be interfered with, such as for a criminal investigation. | Inter-American Commission on Human Rights. (2013). Special Rapporteur on Freedom of Expression. Privacy. Paragraph 131.<br><br>La Rue, Frank. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40. Paragraph 22.<br><br>United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraph 58. |
| Does the platform scan user content that is not publicly available (e.g., emails, private messages, etc.)? | | |
| Does the platform track users in other websites? | | |
| Does the platform store user data for longer than necessary for its operation, or as required by law? | (Privacy and data protection) 3. your personal data should only be processed when laid down by law or when you have consented to it. You should be informed of what personal data are processed and/or transferred to third parties, when, by whom and for what purpose. Generally, you should be able to exercise control over your personal data (check its accuracy, request a correction, a deletion or that personal data is kept for no longer than necessary); | |
| Does the platform aggregate data from different services? | | United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraph 58.<br><br>La Rue, Frank. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40. Paragraph 22 |
| Does the platform aggregate data across devices? | | |

| | | |
|---|---|---|
| Does the platform share data with third parties beyond what is specifically required by law, for commercial purposes? | (Privacy and data protection) 3. your personal data should only be processed when laid down by law or when you have consented to it. You should be informed of what personal data are processed and/or transferred to third parties, when, by whom and for what purpose. Generally, you should be able to exercise control over your personal data (check its accuracy, request a correction, a deletion or that personal data is kept for no longer than necessary); | Inter-American Commission on Human Rights. (2013). Special Rapporteur on Freedom of Expression. Surveillance of communications on the Internet and freedom of expression. Paragraphs 131 and 162.<br><br>United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraph 58.<br><br>La Rue, Frank. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40. Paragraph 22 |
| Does the platform share data with third parties beyond what is specifically required by law, for processing or technical purposes? | | |
| Does the platform share data with third parties beyond what is specifically required by law, for other than commercial and technical purposes? | | |
| Does the platform ask for a license on user content for other purposes than the ones for which it was originally shared? | | Inter-American Commission on Human Rights. (2013). Special Rapporteur on Freedom of Expression. Privacy. Paragraph 131. |
| Does the platform encrypt or allow encryption of transmitted personal information or content? | | Inter-American Commission on Human Rights. (2013). Special Rapporteur on Freedom of Expression. Privacy. Paragraph 116<br>La Rue, Frank. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40. Paragraphs 23, 48 and 49.<br>United Nations. Human Rights Council. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye. A/HRC/29/32. Friday, May 22, 2015. Paragraphs 61, 62, 63. |
| Does the platform encrypt or allow encryption of stored personal information or content? | | |

| | | |
|---|---|---|
| Does the platform disclose data to law enforcement or for judicial purposes only following a specific legal process? | 4. you must not be subjected to general surveillance or interception measures. In exceptional circumstances, which are prescribed by law, your privacy with regard to your personal data may be interfered with, such as for a criminal investigation. Accessible, clear and precise information about the relevant law or policy and your rights in this regard should be made available to you; | United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraph 75<br><br>La Rue, Frank. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40. Paragraph 29<br><br>Special Rapporteur on Freedom of Expression. Surveillance of communications on the Internet and freedom of expression. Paragraph 162 |

## *1.3. Due Process*

The key elements of the right to a due process include the rights to access to justice, to the equality of the parties, to be heard, to contradictory clauses and to full defense. Considered an important complement of the substantive law, due process was elevated to the category of a human right in documents such as the Universal Declaration of Human Rights (art. 10) and the Pact of San José, Costa Rica (art. 8).

According to a report produced by former United Nations Secretary-General Kofi Annan, the rule of law and its principles must be respected and promoted by all "persons, as well as public and private institutions and entities"[39]. Online platforms are thus private players with an obligation to comply with due process.

[39] The rule of law and transitional justice in conflict and post-conflict societies. UN Doc. S/2004/616 (2004), paragraph 6.

The analysis of due process compliance in the context of online platforms included two elements: contract amendments and termination and conflict resolution. In this respect, platforms have a negative responsibility: they should refrain from imposing any impediment to a user's right to a fair trial by a competent authority.

The Guide to Human Rights for Internet Users addresses this issue in its section on effective remedies. According to the document, "[t]he avenues for seeking remedies should be available, known, accessible, affordable and capable of providing appropriate redress" when human rights or fundamental freedoms are violated. According to the Guide, such appeals should not be restricted to the judicial sphere, and may include alternative mechanisms, for instance, in the platform itself, as long as they do not impact users' option to seek judicial relief. The adoption of alternative conflict resolution mechanisms within the platform structure can be considered positive, given that they consist of an alternative way to balance interests. However, parties cannot be forced to participate in this type of process and they will only remain bound to such a procedure while they believe it brings better results than other means.

The Guide to Human Rights for Internet Users also asserts that the State and online service providers should provide users with clear information about their rights and freedoms existing resources in the event of violations and ways to access such information and resources.

Based on these principles, the following criteria for the analysis of Terms of Service were defined:

**TABLE 3: Criteria for the analysis of due process and specific references on international human rights documents**

| Criterion for Analysis | Reference in the Guide to Human Rights for Internet Users of the Council of Europe (English) | Reference to other international human rights documents (in English) |
|---|---|---|
| Does the platform have the obligation to notify users before making changes to its Terms of Service? | (Effective remedies) 1.1. your Internet service provider, providers of access to online content and services, or other company and/or public authority should inform you about your rights, freedoms and possible remedies and how to obtain them. This includes easily accessible information on how to report and complain about interferences with your rights and how to seek redress; (Freedom of expression and information) 5. your Internet service provider and your provider of online content and services have corporate responsibilities to respect your human rights and provide mechanisms to respond to your claims. You should be aware, ho wever, that online service providers, such as social networks, may restrict certain types of content and behavior due to their content policies. You should be informed of possible restrictions so that you are able to take an informed decision as to whether to use the service or not. This includes specific information on what the online service provider considers as illegal or inappropriate content and behavior when using the service and how it is dealt with by the provider; | United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraph 47. |

| | | |
|---|---|---|
| Is the platform allowed to terminate its services to all users without a significant notice? | | |
| Are users allowed to access the Terms of Service they originally agreed with when creating their account? | (Effective remedies) 1.1. your Internet service provider, providers of access to online content and services, or other company and/or public authority should inform you about your rights, freedoms and possible remedies and how to obtain them. This includes easily accessible information on how to report and complain about interferences with your rights and how to seek redress;<br><br>(Freedom of expression and information) 5. your Internet service provider and your provider of online content and services have corporate responsibilities to respect your human rights and provide mechanisms to respond to your claims. You should be aware, however, that online service providers, such as social networks, may restrict certain types of content and behavior due to their content policies. You should be informed of possible restrictions so that you are able to take an informed decision as to whether to use the service or not. This includes specific information on what the online service provider considers as illegal or inappropriate content and behavior when using the service and how it is dealt with by the provider; | |

| | | |
|---|---|---|
| Does the platform offer alternative conflict resolution mechanisms with the right to be heard for disputes among users? | (Effective remedies) 1. You have the right to an effective remedy when your human rights and fundamental freedoms are restricted or violated. To obtain a remedy, you should not necessarily have to pursue legal action straight away. The avenues for seeking remedies should be available, known, accessible, affordable and capable of providing appropriate redress. Effective remedies can be obtained directly from Internet service providers, public authorities and/or national human rights institutions. Effective remedies can – depending on the violation in question – include inquiry, explanation, reply, correction, apology, reinstatement, reconnection and compensation. In practice, this means: 1.1. your Internet service provider, providers of access to online content and services, or other company and/or public authority should inform you about your rights, freedoms and possible remedies and how to obtain them. This includes easily accessible information on how to report and complain about interferences with your rights and how to seek redress; | Inter-American Commission on Human Rights. (2013). Special Rapporteur on Freedom of Expression. Freedom of expression and internet. Paragraph 115<br><br>United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraphs 42, 47 and 76. |
| Does the platform offer alternative conflict resolution mechanisms with the right to be heard for disputes between users and the platform? | | Inter-American Commission on Human Rights. (2013). Special Rapporteur on Freedom of Expression. Freedom of expression and internet. Paragraph 115<br><br>United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraph 47 and 76 |
| Does the platform require users to waive their right to initiate a class action? | (Effective remedies) 2. In the determination of your rights and obligations or of any criminal charge against you with regard to the Internet: 2.1. you have the right to a fair trial within a reasonable time by an independent and impartial court; | United Nations. General Assembly. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/17/27. May 16, 2011. Paragraph 47. |
| Does the platform impose mandatory arbitration? | | |
| Does the platform impose a specific jurisdiction for judicial disputes? | | |
| Does the platform impose further restrictions on users' access to justice? | | |

## 2. ANALYSIS

The criteria above set the boundaries for analyzing the Terms of Service of 50 online platforms (see Annex II), which were selected both for their popularity and as a means to cover a diversity of services and business models. For instance, in order to ensure sample diversity, platforms that are less popular, but are managed by non-profit organizations, were included. Only free services were considered for the sample, prioritizing business models potentially based on the collection and use of personal data.[40] Furthermore, applications for mobile devices were not analyzed in the first phase of the study, although this was a format of interaction offered by some of the platforms in question.

Once the platforms were selected, the analysis was conducted as follows:

1. Identification and filing of Terms of Service and related documents;
2. Analysis and codification of the Terms of Service, according to the above criteria by three different teams;
3. Crossing data generated by three analyses, based on a conflict resolution methodology;
4. Statistical treatment and calculation of the level of agreement for each question.

### *2.1. Identification and Storage of Terms of Service and Related Documents*

The first step of the analysis was to identify all documents which users needed to agree upon, in order to register or use the

[40] The nature of such "free" services can be questioned, since users' personal data often act as a currency in the online environment, in which a large amount of data is produced (and potentially collected, stored and shared) in each interaction. This represents a valuable database for businesses based on the sale of personalized ads, for example.

services of each platform. For the purposes of this study, the following documents were considered part of the "Terms of Service":

- Contracts to which users must necessarily agree to interact (seek, receive and transmit information) on the platform;
- Additional policies explicitly referred to in those contracts, such as Community Standards, Cookie Policies, etc.

The large number of auxiliary documents found in some cases is noteworthy, notably in services offered by larger companies. They may include help pages, explanatory videos, frequently asked questions (FAQ), etc. Although they do not necessarily have a binding nature, the content of such documents may detail, supplement, and in some cases even contradict the Terms of Service. However, the analysis did not include those documents to the extent that they were not presented in a clear and conspicuous manner as a legal instrument to which users must consent to join the platform.[41] Policies related to optional premium services (such as paid services, accounts for corporate profiles, etc.) were not analyzed either.

Even with the indicated methodology, in some cases it was difficult to determine precisely which policies bind the user to the platform. Despite referring to complementary policies, some documents were not always clear and the references were not made in an explicit and direct form, as noted in the following clause:

> Our Services are very diverse, so sometimes additional terms or product requirements (including age requirements) may apply. Additional terms will be available with the relevant Services, and those additional terms become part of your agreement with us if you use those Services.

[41] For an analysis of technology companies' policies that included documents beyond binding contracts, please check the project called "Ranking Digital Rights" in <https://rankingdigitalrights.org>.

For this reason, sometimes it was necessary to actively search for policies that could be relevant to the analysis in the platform. This included searching for links in footers or other locations on the web page that would lead to Terms of Service, Privacy Policies or Community Standards (or their equivalents) and excerpts of help pages to which the main documents made direct reference.

The need to include a further step in the identification of binding documents evidenced an important result of this research: there is a lack of clarity about which documents must effectively be read and agreed to, before using a platform. The table in Annex II indicates which documents have been analyzed for each platform and any discrepancies in the analysis of researchers 1, 2 and 3[42].

Once all relevant documents were identified, their copies were stored in PDF *(Portable Document Format)* in order to record the date and version of the analyzed policies and the URL (Uniform Resource Locator) where they were originally found.

### *2.2 Terms of Service Analysis and Codification*

After storing the relevant documents, the next step was to proceed with the analysis, which consisted in reading each document and filling a specific worksheet with the clauses considered relevant to each of the human rights criteria mentioned above. The process was replicated by three independent coders,[43] who were provided with common guidelines but were not in contact with one another, and did not exchange information among themselves during the analysis.

After identifying relevant clauses, a set of relevant questions (see below) were answered with the following codes:

---

[42] From a methodological point of view, the subjective differences among analyzed documents were addressed when results were crossed (see section 2.3).

[43] In addition to a team located at CTS FGV, two students at the Law School of the University of Tilburg in the Netherlands conducted Terms of Service analyses.

- Yes - Y
- No - N
- Empty (i.e. no relevant clause was found) - E
- Contradictory (i.e. contradictory clauses found) - C

The decision to carry out three distinct and independent analyses of the Terms of Service's provisions was aimed at measuring the degree of subjectivity intrinsic in the assessment. The crossing of the three analyses was followed by a statistical computation, which identified the level of agreement amongst coders for each question, thus offering a reliability parameter for the final results.

### *2.3 Crossing Results and Assigning Weights to Each Answer*

In order to reach final answers for each platform and criterion, data obtained from the three independent analyses was crossed, according to the following rules:

- If there were conflicting interpretations, the majority answer would prevail;
- Affirmative (Y), negative (N) or contradictory (C) answers prevailed over empty responses (E), even if the empty ones were the majority. The reason for this decision was that, if at least one of the coders was able to identify a relevant clause for a certain criterion, it should be taken into account in the final results;
- Contradictory responses (C) predominated over other responses, even though two of the three coders had agreed upon it.

This approach, combined with the statistical calculation of the level of agreement detailed below, also sought to overcome any discrepancies amongst the documents analyzed for each platform (see item 2.1).

According to the adopted methodology, if only one of the analysts found relevant provisions to respond a particular question, this particular analysis would prevail over empty responses. Therefore, a final result would only be considered empty (E) if all three analysts had found no relevant clauses for that analysis criterion (see Table 4). Thus, the results would not be affected by the eventual lack of attention of any of the coders. The assumption behind this methodology was that any provision found and understood by an ordinary user as binding could influence his/her behavior toward the platform and; therefore, should be considered in the analysis.

In addition to a final result, each response was given a weight depending on the level of agreement of the coders. If they all agreed, the assigned weight was one (1). If the correlation was partial, the assigned weight was 0.5, and if there were three completely different answers, i.e. no agreement, the weight was zero (0). The level of agreement for each question was calculated from the weighted average mean of each platform (sum of the weights divided by the total analyzed platforms, i.e. 50).

**TABLE 4: Reference table for crossing responses of three independent coders and their assigned weight**

| Possible combinations | Final result | Weight |
|---|---|---|
| Y,Y,Y | Y | 1 |
| Y,Y, N | Y | 0.5 |
| Y,Y, E | Y | 0.5 |
| Y,Y, C | C | 0.5 |
| Y, N, N | N | 0.5 |
| Y, N, E | C | 0 |
| Y, N, C | C | 0 |
| Y, E, E | Y | 0.5 |
| Y, E, C | C | 0 |
| Y, C, C | C | 0.5 |
| N, N, N | N | 1 |
| N, N, E | N | 0.5 |

| | | |
|---|---|---|
| N, N, C | C | 0.5 |
| N, E, E | N | 0.5 |
| N, E, C | C | 0 |
| N, C, C | C | 0.5 |
| E, E, E | E | 1 |
| E, E, C | C | 0.5 |
| E, C, C | C | 0.5 |
| C, C, C | C | 1 |

### *2.4. Statistical Analysis and Computation of the Level of Agreement*

The purpose of calculating the analysts' level of agreement for each of the questions was to identify the degree of reliability of the results obtained. Very low levels of agreement could either indicate that the developed criteria were subjective and open to broad interpretation or that the clauses of the Terms of Service were ambiguous or unclear and, therefore, more detailed interpretation guidance would be needed for future analysis.

The level of agreement found after the statistical treatment ranged from 63% – regarding the obligation to provide notification if there was any change in the terms – to 95%, with respect to (i) the requirement to waive the right to initiate a class action and (ii) mandatory arbitration in case of disputes.

**TABLE 5: Level of agreement of the three coders by analysis criterion**

| Axis | Criterion for Analysis | Level of agreement |
|---|---|---|
| Due Process | Does the platform have the obligation to notify users before making changes to its Terms of Service? | 63% |
| Privacy | Does the platform offer clear and transparent information on how users can report content they consider inappropriate or submit takedown requests? | 64% |

| | | |
|---|---|---|
| Privacy | Are users allowed to edit and delete all personal data available on the platform? | 66% |
| Privacy | Does the platform share data with third parties beyond what is specifically required by law, for processing or technical purposes? | 66% |
| Freedom of expression | Does the platform analyze, block, filter or remove content for unspecific, undetermined or unclear reasons? | 68% |
| Freedom of expression | Does the platform offer clear and transparent information on how users can report content they consider inappropriate or submit takedown requests? | 69% |
| Privacy | Does the platform allow full and permanent account deletion? | 69% |
| Privacy | Is the user allowed to view and copy all the personal data available on the platform? | 73% |
| Freedom of expression | Does the platform offer notification and the right to be heard before removing user-generated content as a result of a third-party complaint? | 74% |
| Due Process | Is the platform allowed to terminate its services to all users without a significant notice? | 74% |
| Freedom of expression | Does the platform allow users to remain anonymous or use a pseudonym? | 74% |
| Privacy | Does the platform share data with third parties beyond what is specifically required by law, for commercial purposes? | 76% |
| Privacy | Does the platform share data with third parties beyond what is specifically required by law, for other than commercial and technical purposes? | 76% |
| Privacy | Does the platform disclose data to law enforcement or for judicial purposes only following a specific legal process? | 76% |

| | | |
|---|---|---|
| Privacy | Does the platform allow the removal of all personal data generated by the user within a reasonable period after account deletion? | 77% |
| Privacy | Does the platform ask for a license on user content for other purposes than the ones for which it was originally shared? | 79% |
| Due Process | Does the platform impose further restrictions on users' access to justice? | 79% |
| Privacy | Does the platform encrypt or allow encryption of transmitted personal information or content? | 80% |
| Privacy | Does the platform scan user content that is not publicly available (e.g., emails, private messages, etc.)? | 80% |
| Privacy | Does the platform track users in other websites? | 80% |
| Due Process | Are users allowed to access the Terms of Service they originally agreed with when creating their account? | 82% |
| Privacy | Does the platform allow third party tracking? | 83% |
| Due Process | Does the platform impose a specific jurisdiction for judicial disputes? | 83% |
| Privacy | Does the platform aggregate data across devices? | 83% |
| Privacy | Does the platform encrypt or allow encryption of stored personal information or content? | 84% |
| Due Process | Does the platform offer alternative conflict resolution mechanisms with the right to be heard for disputes between users and the platform? | 86% |

| | | |
|---|---|---|
| Privacy | Does the platform aggregate data from different services? | 88% |
| Freedom of expression | Does the platform notify and allow questioning before eliminating the account of a particular user? | 88% |
| Due Process | Does the platform offer alternative conflict resolution mechanisms with the right to be heard for disputes among users? | 93% |
| Privacy | Does the platform affirmatively minimize data collection? | 94% |
| Due Process | Does the platform require the user to give up his right to initiate a collective action? | 95% |
| Due Process | Does the platform impose mandatory arbitration? | 95% |

# Results

Results for the three axes of analysis are presented below. In addition to the aggregated quantitative data, which provide an overview of the practices of the 50 analyzed platforms in relation to the developed criteria, excerpts of the clauses considered in the analysis are presented, by way of illustration of the challenges in interpreting the analyzed documents. Information about the documents analyzed as part of the Terms of Service can be found in Annex II.

## 1. Freedom of Expression

### *1.1. Content Monitoring, Blocking, Filtering and Removal*

The first criterion considered in the Freedom of Expression analysis was monitoring, blocking, filtering or removing content for unspecific, undetermined or unclear reasons. As noted, international human rights recommend clarity with any condition aiming to restrict freedom of expression[44]. However, almost 50% of the platforms (46%) contain clauses stating that some kind of monitoring will be conducted without specifying what type of content may be affected, or only doing so ambiguously.

Flickr, a photo-sharing platform owned by Yahoo, offers an example of a clause providing an affirmative response (Y)[45], in stating that the company has the right to remove or refuse any content that violates their policies or that is "objectionable".

> You acknowledge that Yahoo may or may not pre-screen Content, but that Yahoo and its designees shall have the right (but not the obligation) in their sole discretion to pre-screen, refuse,

[44] See section on methodology.

[45] For explanations about the methodology and the process of analysis, see the section on research methodology.

> or remove any Content that is available via the Yahoo Services. Without limiting the foregoing, Yahoo and its designees shall have the right to remove any Content that violates the TOS or is otherwise objectionable.

In another point, the platform also states that content may be removed if it violates the rights of Yahoo, of others, or their policies.

> In addition to all other legal remedies available to Yahoo, You acknowledge that Yahoo has the right to remove Your Content from the Service or refuse to include Your Content in the Service, suspend or terminate Your Yahoo account or refuse to grant You access to any current or future use of the Service or any Yahoo service, with or without warning, if Yahoo, in its sole discretion, believes You have: (i) violated or tried to violate the rights of Yahoo or others; or (ii) violated or tried to violate or acted inconsistently pursuant to these Additional Terms or any other terms of the TOS.

Twenty other platforms (40%) presented contradictory results, either because the same analyst identified contradictory clauses in their policies, or because different analysts obtained different answers to this criterion, and were unable to reach an affirmative or negative response after crossing the results.

**TABLE 6: Aggregated results and level of agreement regarding content analysis, blocking, filtering or removal**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform analyze, block, filter or remove content for somewhat specific, undetermined or unclear reasons? | 23 | 4 | 20 | 3 | 68% |

Only 8% of the analyzed platforms explicitly state either that they will not monitor content, or that, they will do so in specific situations, such as to eliminate materials that violate their policies,[46] for example. This is the case of the file-sharing platform Rapidshare,[47] which explicitly states under its terms that it does not open or examine user content for any purpose.

> RapidShare does not open or examine the data of its users and the data is neither catalogued by RapidShare, nor is the content listed anywhere. Only you, the owner of the files, control whether others may access the files, how files are accessed and which files may be accessed. RapidShare does not incorporate a search function allowing the querying of the RapidShare storage infrastructure.

Another platform that is committed to neither filtering nor blocking content is Wikipedia, stating that it does not monitor or delete the contributions sent by users, except in rare exceptions:

> Generally we do not contribute, monitor, or delete content (with the rare exception of policies like these Terms of Service or legal compliance for DMCA notices). This means that editorial control is in the hands of you and your fellow users who create and manage the content. We merely host this content.

This is a particular platform, however, due to its collaborative nature, which allows its community of users to act as editors.

---

[46] Policies concerning what content is allowed on the platform are usually specified in documents called Community Guidelines. Among those platforms that perform some type of monitoring and filtering, the reasons given are (i) the elimination of speech considered to be restricted and which is, in fact, illegal in many countries, such as hate speech, child pornography or incitement to violence and (ii) their content policies, which often go beyond this type of speech and have to do with factors such as the platform's priority target group or the type of service it offers.

[47] RapidShare services were discontinued in the course of this research. However, its analysis was kept in order to highlight common practices of this particular type of platform.

> Because the Wikimedia Projects are collaboratively edited, all of the content that we host is provided by users like yourself, and we do not take an editorial role. This means that we generally do not monitor or edit the content of the Project websites, and we do not take any responsibility for this content. Similarly, we do not endorse any opinions expressed via our services, and we do not represent or guarantee the truthfulness, accuracy, or reliability of any submitted community content. Instead, we simply provide access to the content that your fellow users have contributed and edited.

Freenode, on the other hand, is an example of a platform which clearly shows the reasons for monitoring content in their policies, stating that it will not tolerate the incitement to violence motivated by racism or religious intolerance or any behavior leading to harassment or creating alarm or distress. Moreover, its terms state that the platform has zero tolerance towards discrimination by race, religion, gender, sexual preference, defamation and slander.

> In accordance with UK law, freenode has no tolerance for any activity which could be construed as: incitement to racial hatred, incitement to religious hatred, or any other behavior meant to deliberately bring upon a person harassment, alarm or distress. We do NOT tolerate discrimination on the grounds of race, religion, gender or sexual preference and run with a zero-tolerance policy for libel and defamation. While we believe in the concept of freedom of thought and freedom of expression, freenode does not operate on the basis of absolute freedom of speech and we impose limitations e.g.. on "hate speech". We expect all members of the community to treat other community members with respect and reserve the right to terminate anyone's access to our services should they be found to be in breach of policy.

### *1.2. Information on Reporting Inappropriate or Abusive Content*

Most platforms (70%) provide clear and transparent information in their Terms of Service on how users may report content they deem inappropriate. Only one shows contradictory clauses on this matter, while 14 (28%) offer no relevant provisions, which in this case indicates that they do not provide information on how to report abusive content.

The relatively low level of agreement obtained in this criterion (69%) may be due to a disagreement among analysts on whether the description of the mechanism imposed by the Digital Millennium Copyright Act (DMCA) would be enough to provide a positive answer, since it only deals with copyright violations and not with other types of abuses to privacy, for instance. The DMCA is a United States statute establishing a notice and takedown system, whereby hosting platforms are liable for copyright-infringing material they host if they have actual or constructive knowledge of infringement or, after receiving a "notice" of infringement by the relevant copyright owner, they fail to expeditiously remove the infringing material[48]. In this case, it is worth noting that, according to the adopted conflict resolution methodology applied by crossing results (see Methodology), answers that considered the DMCA sufficient for reporting prevailed over the opposite conclusion.

Even platforms with a detailed policy on content do not clearly specify the mechanisms for reporting inappropriate material or challenging removals beyond the DMCA mechanism. This does not necessarily mean, however, that they do not provide other solutions or mechanisms that do not appear in their Terms of Service and that were therefore not considered in this analysis.

**TABLE 7: Aggregated results and level of agreement regarding the existence of clear information on how to report inappropriate or abusive content**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform offer clear and transparent information on how users can report content they consider inappropriate or submit takedown requests? | 35 | 0 | 1 | 14 | 69% |

[48] See 17 U.S. Code § 512 ©.

### *1.3. Notification and Right to be Heard in Case of Content Removal*

The following criterion evaluated whether platforms offer notifications and the right to be heard before removing content as a result of third-party complaints. Despite the existence of recommendations of the contrary in international human rights documents[49], only 4% of platforms provide authors with the possibility of defending themselves, should any of their content be subject to a removal request. In addition, four platforms (8%) showed contradictory terms, while 36% did not provide any information about this.

**TABLE 8: Aggregated results and level of agreement regarding notice and the right to be heard in case of content removal**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform provide notifications and the right to be heard before removing user-generated content as a result of third-party complaints? | 2 | 26 | 4 | 18 | 74% |

The majority of platforms (52%) explicitly state that they may remove content based on third-party notification without offering any justification, notification or opportunity to be heard to the user who originally shared it. Tumblr, for instance, states that, if it identifies content that violates the privacy of others, it may remove it without notice or the right to be heard.

[49] See the section on Methodology.

> Don't post content that violates anyone's privacy, especially personally identifying or confidential information like credit card numbers, social security numbers, unlisted contact information, or private photos of your ex's junk (no matter how remarkable). [...] If we conclude that you are violating these guidelines, you may receive a notice via email. If you don't explain or correct your behavior, we may take action against your account. We do our best to ensure fair outcomes, but in all cases we reserve the right to suspend accounts, or remove content, without notice, for any reason, but particularly to protect our services, infrastructure, users, and community. We reserve the right to enforce, or not enforce, these guidelines in our sole discretion, and these guidelines don't create a duty or contractual obligation for us to act in any particular manner. You can report violations of these guidelines to us directly.

### *1.4. Notification and Possibility of Questioning Individual Account Termination*

Another criterion analyzed was whether a platform notifies users about the termination of their account and offers them the opportunity to question such a decision. In this case, none of the platforms does so, while 88% expressly state that they may delete accounts without prior or even subsequent notification. Four platforms (8%) presented contradictory clauses and in two platforms (4%), no relevant information on this criterion was found.

**TABLE 9: Aggregated results and level of agreement regarding notice and possibility of questioning individual account termination**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform notify and allows questioning before eliminating the account of a particular user? | 0 | 44 | 4 | 2 | 88% |

### *1.5. Anonymity and Use of Pseudonyms*

The following criterion analyzed whether platforms allow anonymity or the use of pseudonyms. Both clauses that explicitly authorized this practice or that otherwise stated that using a true identity was mandatory were considered. Results show that a significant number of platforms (32%) does not allow anonymity or the use of pseudonyms, while 28% do. One of them is Wikipedia, which states that users do not have to register in order to use its services, or to contribute with content and interact with the platform.

> We believe that you shouldn't have to provide personal information to participate in the free knowledge movement. You do not have to provide things like your real name, address, or date of birth to sign up for a standard account or contribute content to the Wikimedia Sites. [...] You are not required to create an account to read or contribute to a Wikimedia Site, except under rare circumstances. However, if you contribute without signing in, your contribution will be publicly attributed to the IP address associated with your device.

Finally, 8% of the platforms presented contradictory clauses and 32% had no relevant provisions on this criterion.

**TABLE 10: Aggregated results and level of agreement regarding anonymity or the use of pseudonyms**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform allow users to remain anonymous or use a pseudonym? | 14 | 16 | 4 | 16 | 74% |

## 2. PRIVACY

### *2.1. Minimization of Data Collection*

The first item analyzed in privacy was whether the platform affirmatively minimizes the collection of personal data in its policies. This criterion presented a high level of agreement and indicated that most platforms (76%) do not commit to doing so (empty result).

**TABLE 11: Aggregated results and level of agreement regarding data collection minimization**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform affirmatively minimize data collection? | 11 | 1 | 0 | 38 | 94% |

Clauses related to data collection require users to consent with the collection of certain types of information – usually only a few are specified as examples – without detailing for which purposes they may be used. One example of this practice is Airbnb, which informs users that it will collect, store and process information provided during registration and use of the platform, as well as data collected automatically:

> We receive, store and process information that you make available to us when accessing or using our Platform. Examples include when you: fill in any form on the Platform, such as when you register or update the details of your user account; access or use the Platform, such as to search for or post Accommodations, make or accept bookings, pay for Accommodations, book or pay for any associated services that may be available (such as but not limited

> to cleaning), post comments or reviews, or communicate with other users; [...] We may also receive, store and process Log Data, which is information that is automatically recorded by our servers whenever you access or use the Platform, regardless of whether you are registered with Airbnb or logged in to your Airbnb account, such as your IP Address, the date and time you access or use the Platform, the hardware and software you are using, referring and exit pages and URLs, the number of clicks, pages viewed and the order of those pages, and the amount of time spent on particular pages. [...] We may also use web beacons and tracking URLs in our messages to you to determine whether you have opened a certain message or accessed a certain link.

Even though the collection of such data can be designed to offer more personalized services – that is, services based on users' interests identified from the processing of their personal data – the text does not specify how this data will be used and the type of assumptions that can be extracted from them through profiling practices, for example.

Similar clauses can be found in several of the analyzed platforms. The Terms of Service of Dropbox, for example, state that besides registration and usage data, other information, including location data will be collected automatically when available.

> We collect information from and about the devices you use to access the Services. This includes things like IP addresses, the type of browser and device you use, the web page you visited before coming to our sites, and identifiers associated with your devices. Your devices (depending on their settings) may also transmit location information to the Services.

Among the platforms that are committed to collecting as little data as possible is MyKolab,[50] which offers services like storage and email.

---

[50] MyKolab, launched in 2013 as a free service, became a paid service called Kolab Now during the project.

We will only keep the minimum of logs and debug information necessary to ensure that we can improve the service and resolve issues that may have occurred.

### *2.2. Viewing and Copying Personal Data Available on the Platform*

Regarding users' ability to view and obtain a copy of data sent to the platform, only 20% of the sample commit to this in their policies, while 32% explicitly state that they will not allow the viewing and copying of data. Another 10% contain contradictory clauses and 38% do not provide any information on this topic.

**TABLE 12: Aggregated results and level of agreement regarding the possibility of viewing and copying personal data available**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Is the user allowed to view and copy all the personal data available on the platform? | 10 | 16 | 5 | 19 | 73% |

### *2.3. Editing and Deletion of Personal Data*

Regarding the possibility of modifying or deleting personal data, the situation is reversed: 74% of platforms state in their policies that this kind of action is allowed to users and only 6% that it is not; 16% shows contradictory clauses and 4% does not present any relevant information in this regard.

**TABLE 13: Aggregated results and level of agreement regarding the possibility to edit and delete personal data**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Is the user allowed to edit and delete all the personal data available on the platform? | 37 | 3 | 8 | 2 | 66% |

In the case of platforms that allow editing and deletion of personal data, it is common to find clauses like this one from Academia.edu platform:

> Correcting/Updating or Removing Information
>
> All Academia.edu Members may review, update, modify or remove any of their Personal Information in their profile page at any time by logging into their Account and accessing features such as Edit Profile and Account Info. If you completely delete all such information, then your Account may become deactivated. If you would like us to delete your record in our system, please contact us at privacy@academia.edu a request that we delete your Personal Information from our database. We will use commercially reasonable efforts to honor your request. We may retain an archived copy of your records as required by law or for legitimate business purposes.

It should be noted that the great majority of platforms does not specify whether it is possible to edit and delete only information generated or submitted by the user or if it includes all records collected automatically. Other platforms presented unclear clauses on the possibility of permanent deletion of stored data, such as is the case for MySpace:

> Further, deleted Content may persist in archival copies on Myspace servers for a reasonable period of time. You understand and

> agree that once Content is distributed to a Linked Service, or incorporated into other aspects of the Myspace Services (e.g., as part of a derivative work), Myspace is under no obligation to delete or ask other Users or a Linked Service to delete that Content; therefore, it may continue to appear and be used indefinitely.

### *2.4. Permanent Account Deletion*

The next criterion analyzed whether platforms allowed users to completely and permanently delete their account. The majority (68%) stated this was possible. Thirteen platforms (26%) showed no relevant clauses on this matter and 6% explicitly said they did not allow users to delete their account.

**TABLE 14: Aggregated results and level of agreement regarding the possibility of permanent account deletion**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform allow full and permanent account deletion? | 34 | 3 | 0 | 13 | 69% |

### *2.5. Permanent Deletion of Personal Data*

Only 12% of the platforms commit in their policies to the exclusion of personal data generated by their users or collected in other ways after the account cancellation. The majority (60%) do not provide any information about this. Five platforms, 10% of the total, explicitly say they will not allow the definitive exclusion of personal data after the deletion of an account and 18% provided contradictory information on this issue.

**TABLE 15: Aggregated results and level of agreement regarding the possibility of permanent deletion of personal data**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform allow the removal of all personal data generated by the user within a reasonable period after account deletion? | 6 | 5 | 9 | 30 | 77% |

*2.6. Scanning of Private Communications*

The following analyzed whether platforms require users' consent to automatically analyze private communications (e.g. email messages or conversations). Almost half (44%) of the platforms state they can perform this type of operation and only 6% declare that will not do so. Another 46% of the sample did not contain relevant clauses, which may be an indication that they do not perform such activities.

**TABLE 16: Aggregated results and level of agreement regarding the scanning of private communications**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform scan user content that is not publicly available (e.g., emails, private messages, etc.)? | 22 | 3 | 2 | 23 | 80% |

Among the platforms that required users' consent to perform data collection by scanning private communications are the services offered by Google. In the case of their email platform Gmail, for example, the Terms of Service state that automated systems analyze users' content to offer personalized ads, provide relevant search results and perform spam detection.

> Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.

A platform that explicitly states it does not scan users' private content is the email service Riseup:

> We will not read, search, or process any of your incoming or outgoing mail other than to protect you from viruses and spam or when directed to do so by you when troubleshooting.

### *2.7. Tracking Users' Activities on Other Websites*

The following criterion analyzed the monitoring of users' activities on other websites, usually performed through technologies such as cookies. Since the use of these technologies can serve various purposes, some necessary for the correct operation of the platform, it was considered that such monitoring occurred if policies (i) explicitly stated that information on the use of other websites could be collected or (ii) mentioned the use of cookies in a comprehensive way without specifying what kind of data would be collected and for which purposes.

The analysis considered that if a platform made use of cookies or other technologies for tracking only with the express consent of users (e.g. through opt-in mechanisms), it would not be counted among those that do so by default. It should be noted, however, that this is not the most common practice, prevailing the use cookies by default, which gives less autonomy to users over their personal data.

**TABLE 17: Aggregated results and level of agreement regarding the tracking of user activities in other websites**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform track users in other websites? | 33 | 2 | 0 | 15 | 80% |

It was observed that 66% of platform policies make it clear that they may track users' activities on other sites. An example is MySpace:

> You may be served with targeted advertising on the Myspace Services and on websites, applications, and other platforms owned or controlled by third parties based on information about you collected both on and off the Myspace Services, including advertisements based on your and location/or Usage Information.

Among them, some commit to respecting the "Do not track"[51] signal, which allows users to configure their web browsers to not allow the use of cookies and other tracking technologies. This is the case of Pinterest, for example:

> Also, we support the Do Not Track setting browser, and you can learn more about how it Affects our collection and use of off--Pinterest date.

[51] "Do Not Track" is a technology that allows users to opt out of being tracked by websites, including analytics services, advertising networks and social platforms. Developed by a group of researchers, activists and technology companies, it can be set directly in the *browser* and sends a signal to each page accessed informing it is the user's choice not to be monitored while browsing on the web. According to its developers, although some agents currently honor the option sent by users, many still do not. For further information see: <http://donottrack.us/> (accessed February 25, 2016).

Two platforms (4%) commit to not tracking users on other websites and 15, i.e. 30% of the total, provide no information about this in their policies. An example of a commitment to not tracking users' activities on other websites can be found in a MyKolab clause:

> Cookies are used only in so far as they are required for the technical working of the system, and we never use them to track you on third-party sites.

### *2.8. Third-Party Tracking*

In addition to monitoring the activities of their users on other websites, platforms can allow others to install monitoring technologies on their pages, a practice known as *third-party tracking.* Such technologies include cookies and beacons, as well as "social buttons"[52] and analytics tools. In this case, 80% of the analyzed platforms allow this type of activity.

**TABLE 18: Aggregated results and level of agreement regarding third-party tracking**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform allow third party tracking? | 40 | 2 | 2 | 6 | 83% |

[52] A study on Facebook's Terms of Service identified how their so-called "social buttons" are used to track the activities of users and non-users on other pages. For further information see: <http://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf> (accessed on February 25, 2016).

Many platforms allow the collection of data by third parties by default in their terms. An example is the video-sharing website Vimeo, which declares that it may allow others to install tracking technologies on its website to collect information about users.

> We may allow third-parties, including our authorized service providers, IAC companies, advertising companies, and ad networks, to display advertisements on our site. These companies may use tracking technologies, such as cookies, to collect information about users who view or interact with their advertisements. Unless expressly stated otherwise, our website does not provide any personal information to these third parties. This information allows them to deliver targeted advertisements and gauge their effectiveness.

Another example is the file-sharing platform 4shared, which explains the functions of "social buttons" and how they can be used to track users' activities on other websites.

> Our Service includes Social Media Features, [...] or interactive mini-programs that run on our site. These Features may collect your IP address, which page you are visiting on our site, and may set a cookie to enable the Feature to function properly. Social Media Features and Widgets are either hosted by a third party or hosted directly on our Site. Your interactions with these Features are governed by the privacy policy of the company providing it.

Viber is an example of a platform that offers users the opportunity to choose not to provide their data to third parties. It offers services such as phone calls, text messages, videos, etc. Their Terms of Service state that an analytics tool collects users' data by default, but explains how users can choose not to allow it, which may be considered as a good practice.

> Viber uses Google Analytics to help us anonymously track and report user/visitor behavior information and users' standard log information to the Site and the Viber App. [...] In personally Identifying data is included in this type of reporting. Google Analytics may have access to your information only for the pur-

> poses of performing these tasks and on behalf of Viber and under obligation similar in those in this Privacy Policy. [...] If you do not want your information to be part of this statistical information gathering, you can disable Google Analytics using the application settings; visit the 'More' screen, tap settings, then disable Google Analytics Collect Data option.

Two platforms explicitly state that they will not allow third-party tracking. MyHeritage, a service that allows users to build their family tree, is one of them:

> Advertiser Cookies: The Website does not include third party advertising on family sites. There are no advertiser cookies on family sites.

Finally, two platforms (4%) contain terms considered contradictory and six (12%) do not have relevant provisions to meet this criterion.

### *2.9. Data Retention*

Regarding data retention, most of the analyzed services (58%) contain clauses in their terms that may allow data to be retained for longer than would be necessary for the proper operation of the platform and its due compliance with legal obligations. It is understandable that certain data may have to be stored for longer periods in situations such as fraud prevention or the identification of violations in the Terms of Service. However, clauses considered broad or generic in that sense were assessed as excessive for the purposes of the present analysis. This is the case of Facebook, which features the following clause:

> Information we receive about you, including financial transaction data related to purchases made with Facebook, may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm.

**TABLE 19: Aggregated results and level of agreement regarding data retention**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform store user data for longer than necessary for its operation, or as required by law? | 29 | 4 | 12 | 5 | 64% |

Twelve platforms (24%) were considered to have ambiguous terms, which may be interpreted as an indication that excessive retention may occur, at least for certain data. The platform Ask.fm is an example: on the one hand, it states that it will delete data within a period of 90 days, explaining that automatic records and backup files will also be deleted:

> Should you choose to leave Ask.fm, rather than deactivate your account, you may do so by selecting the "I want to leave Ask.fm" tab on the Contact Us page. Once received, we will process your request to leave as soon as practicable. Once processed, your profile data will be removed from the Services and your questions to friends will be converted to anonymous questions (in other words, questions you have asked will remain visible but will appear to be from an anonymous user). You will be able to reactivate your account by logging back in for a period of 30 days after your request to leave Ask.fm is processed. At the end of that period your account will be deleted and all "likes" which you have added to questions will be removed. We will delete your data as soon as reasonably practicable, but in certain cases limited types of data, including log files and backups, may take up to 90 days to be fully deleted.

On the other hand, it explains that some information may be kept for fraud prevention, investigations, customer support, the protection of the platform's rights and properties, among others.

> We may access, preserve or disclose any of your information if we are required to do so by law, or if we believe in good faith that it is reasonably necessary to (i) respond to claims asserted against us or to comply with legal process (for example, subpoenas or warrants), including those issued by courts having jurisdiction over us or you, (ii) enforce or administer our agreements with users, such as the TOU; (iii) for fraud prevention, risk assessment, investigation, customer support, providing the Services or engineering support, or (iv) protect the rights, property or safety of Ask.fm, its users, or members of the public.

Finally, 8% of the platforms explicitly state that they do not retain data for longer than necessary for their operations or for the fulfillment of any legal obligation. In 10% of the cases, no relevant clauses on the subject were found.

### *2.10. Data Aggregation from Different Services*

The following criterion refers to the aggregation of data between services, i.e. the combination of user data collected from different services of a same company or from affiliated companies. More than half of the analyzed platforms (52%) request consent from their users to perform this type of combination, usually by default. Among them is Academia.edu, which states that, when defining the terms "use" and "process" (referring to user data) states they include, among other actions, the combination of data between affiliated companies.

> As used in this policy, the terms "using" and "processing" information include using cookies on a computer, subjecting the information to statistical or other analysis and using or handling information in any way, including, but not limited to collecting, storing, evaluating, modifying, deleting, using, combining, disclosing and transferring information within our organization or among our affiliates within the United States or internationally.

> You provide consent and all rights necessary to enable users to sync (including through an application) their devices with any information that is visible to them on Facebook. [...] We collect information from or about the computers, phones, or other devices where you install or access our Services, depending on the permissions you've granted. We may associate the information we collect from your different devices, which helps us provide consistent Services across your devices.

### *2.12. Data Sharing for Commercial Reasons*

Regarding the sharing of personal data with third parties for commercial reasons, most platforms (62%) contain clauses in their policies requiring users' consent to perform it by default. Among them is Delicious:

> Other than the foregoing, we do not share Personal Information with third parties except as follows: Non-Identifying and Service Usage Information. We may share Non-Identifying Information and Service Usage Information in aggregated or non-aggregated formats with third parties for industry analysis, demographic profiling and other purposes. Any information shared in these contexts will not contain your Personal Information.

It should be noted that although the platform states that it only shares non-identifiable data, the re-identification of anonymous data could be done in a relatively simple way (Sweeney, Abu & Winn, 2013).[53]

---

[53] The debate over the definition of personal data and to what extent anonymous or unidentifiable data is included in this concept has triggered legislative discussions around the world about legal instruments for the protection of personal data. For an overview of how this has played out in Brazil, see the contributions to the public debate on a Draft Law on Personal Data Protection, available at: <http://pensando.mj.gov.br/dadospessoais/> (accessed on March 15, 2016).

**TABLE 22: Aggregated results and level of agreement regarding data sharing for commercial reasons**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform share data with third parties beyond what is specifically required by law, for commercial purposes? | 31 | 10 | 6 | 3 | 76% |

Ten platforms (20%) explain that they will not share users' data for commercial purposes, 12% shows contradictory clauses in their policies, and 6% did not have any provision considered relevant to this criterion. An example of a platform that does not share data for commercial purposes is Riseup:

> We do not share any user information with any other groups or individuals. Within the Riseup Collective, members of the collective have access only to information which they need in order to perform their work.

### *2.13. Data Sharing for Processing or Technical Reasons*

In terms of sharing personal data with third parties for processing or technical purposes, the results are similar: 62% of the platforms yielded affirmative responses (Y). It is likely that in many cases, sharing is due to a decentralized organizational model in which a major company hires third-party services to perform certain operations. An example is SoundCloud, which claims to outsource certain specialized services related to the platform.

> We use certain reputable third parties, some of whom may be located outside of the European Economic Area, to provide us

**TABLE 20: Aggregated results and level of agreement regarding data aggregation from different services**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform aggregate data from different services? | 26 | 0 | 2 | 22 | 88% |

As observed in the table above, no platform explicitly states it will not perform this type of activity; 4% have contradictory clauses and 44% do not have relevant clauses with regard to this criterion.

### *2.11. Data Aggregation from Different Devices*

As to the aggregation of user data collected from different devices, 38% of the platforms state that they perform this type of combination, while one (2%) explicitly states that it does not. Most platforms (60%) do not contain specific provisions on this subject.

**TABLE 21: Aggregated results and level of agreement regarding data aggregation from different devices**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform aggregate data from different devices? | 19 | 1 | 0 | 30 | 83% |

An affirmative example (Y) for this criterion is that of Facebook, which in its policy states that it may link the information collected from different devices.

> with certain specialized services related to the Platform. These third parties will have access to certain information about you, but only where this is necessary in order for those third parties to provide their services to us. Where we transfer personal data to these third parties, we ask and require these third parties to implement appropriate organisational and technical security measures to protect against unauthorised disclosure of personal data, and only to process personal data in accordance with our instructions and to the extent necessary to provide their services to us.

In this case, the platform is committed to ensuring that its contractors comply with their data protection requirements.

**TABLE 23: Aggregated results and level of agreement regarding data sharing for processing or technical reasons**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform share data with third parties beyond what is specifically required by law, for processing or technical purposes? | 31 | 10 | 7 | 2 | 66% |

Ten platforms, 20% of the total, claim they do not share data with third parties for processing purposes, 14% have contradictory clauses and 4% have no relevant provisions on this criterion.

### *2.14. Data Sharing for Other Purposes*

Besides sharing user data with third parties for commercial purposes or processing, the study examined whether platforms shared data for other purposes. Again, it is observed that the ma-

jority (62%) present other reasons to justify third party sharing. Three (6%) explicitly state that they will not do so, while 30% have contradictory clauses, and one platform (2%) does not provide any information about it, which, in this case, may indicate that it does not share data with third parties for purposes other than commercial or technical ones.

**TABLE 24: Aggregated results and level of agreement regarding data sharing for other purposes**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform share data with third parties beyond what is specifically required by law, for other than commercial and technical purposes? | 31 | 3 | 15 | 1 | 76% |

With respect to the reasons presented by platforms to share data with third-parties beyond commercial or technical, they are diverse and sometimes vague. A common example can be observed in Hotmail's clause. It claims that it may share personal information, including the content of private communications, amongst others, to protect its rights and property and to enforce its policies:

> We also may share or disclose personal information, including the content of your communications: (...) To protect the rights or property of Microsoft or our customers, including enforcing the terms governing your use of the services. To act on a good faith

> belief that access or disclosure is necessary to protect the personal safety of Microsoft employees, customers or the public.

### *2.15. License on Shared Content*

The following criterion assesses the requirement of a license on user-generated content that goes beyond the reasons it is originally shared on the platform. It is worth mentioning that a relatively wide license on content, such as videos or photos, may be required for the provision of the offered service, since processing such materials in a digital format requires a certain degree of manipulation. However, licenses that required authorization for use in advertisement, adaptation or were valid for an indefinite period, for instance, were considered as potentially having an impact on user privacy.

The analysis of platform policies showed that most of them, 64% of the total, impose content licenses that go beyond what is necessary for the provision of services and users' expectations in terms of the initial purpose for which the content was shared. One example is the license imposed by Google Drive (and other Google services), which states that users agree to the use, hosting, storage, reproduction, modification and creation of derivative works - such as resulting from translations, communications, publications, public performances, public displays and distributions of their content.

> When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Map).

**TABLE 25: Aggregated results and level of agreement regarding the imposition of broad licenses on shared content**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform require a license on user-generated contents that goes beyond the initial purpose for which they were shared? | 32 | 4 | 5 | 9 | 79% |

Four platforms (8%) contain terms considered as being balanced. Finally, 10% contains contradictory clauses, while 18% provides no information on user-generated content licenses in their terms.

### *2.16. Encryption*

Regarding the protection of data from third-parties, one of the criteria considered was the use of encryption. Results show that platforms encrypt mainly transmitted personal data or content, and few do so in relation to stored content.

Fifty percent (50%) of the platforms state that they encrypt at least some of the **transmitted** data (as opposed to stored data), 4% explicitly affirm that they do not, 2% have contradictory clauses and 44% contain no information about this in their terms.

**TABLE 26: Aggregated results and level of agreement regarding the encryption of transmitted information**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform encrypt or allow encryption of transmitted personal information or content? | 25 | 2 | 1 | 22 | 80% |

Indiegogo is an example of a platform committed to the encryption of transmitted personal data with the SSL (Security Sockets Layer) protocol.

> We may store Personal Information in locations outside our direct control (for instance, on servers or databases co-located with hosting providers). We use Security Sockets Layer (SSL) encryption technology to encrypt sensitive personal information (such as your email or password) before it travels over the internet. Credit card numbers are never stored on our database or servers.

With regards to stored personal data and content, the number of platforms that commit to encryption in their policies is 38%. One affirmative example is Riseup:

> The content of your communications, the calendar date of your last login, your address book, and all backups are stored in encrypted format.

**TABLE 27: Aggregated results and level of agreement regarding the encryption of stored information**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform encrypt or allow encryption of stored personal information or content? | 19 | 2 | 1 | 28 | 84% |

In this case, 4% say they do not encrypt stored content or personal data, 2% have contradictory terms and 56% do not have any information about this in their terms.

### *2.17. Data Sharing with Government or Law Enforcement Authorities*

The last criterion considered in the privacy analysis relates to the sharing of users' personal data with government or law enforcement authorities. Following the recommendations of international human rights standards, the study considered that platform policies should state whether they would respond to this type of request regarding user data only following a specific and valid legal process in the country where the service is provided. Results showed that most (54%) do not commit to this in their terms.

Platform terms most commonly include general clauses that provide few guarantees to users. One example can be found in the platform Academia.edu, which takes an expansive approach to its right to investigate and pursue violations of their policies, which may involve cooperation with state authorities. Moreover, it establishes that it can monitor user access in order to comply with the law or requirements from courts, administrative agencies or other government agencies.

> Academia.edu will have the right to investigate and prosecute violations of any of the above to the fullest extent of the law. Academia.edu may involve and cooperate with law enforcement authorities in prosecuting users who violate these Terms. You acknowledge that Academia.edu has no obligation to monitor your access to or use of the Site, Services or Collective Content or to review or edit any Collective Content, but has the right to do so for the purpose of operating the Site and Services, to ensure your compliance with these Terms, or to comply with applicable law or the order or requirement of a court, administrative agency or other governmental body.

**TABLE 28: Aggregated results and level of agreement regarding data sharing with government and/or law enforcement authorities**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform disclose user data to government authorities only following a specific legal process? | 5 | 27 | 15 | 3 | 76% |

Furthermore, 30% of the platforms have ambiguous terms. Instead, five platforms, 10% of the total, commit to complying with government requests only if there is a valid legal process. One example is the file-sharing platform 4shared:

> Notwithstanding any terms to the contrary in the Terms, 4shared may disclose Customer Data: (i) as required by any applicable Laws; or (ii) in response to a subpoena or other compulsory legal process.

Finally, 6% of the platforms do not provide relevant information relating to this criterion.

## 3. DUE PROCESS

### *3.1. Notification Requirements for Changes in Terms of Service*

The analysis on Due Process was primarily focused on the amendment and termination of contracts. Thus, the first criterion addressed whether platforms had an obligation to notify their users of policy changes. Most of them (56%) have contradictory clauses in that regard. This is due to the fact that many are obliged by their terms to notify users of any significant changes, but not in the case of minor changes such as punctuation, spelling or changes that,

according to their criteria, do not affect the rights and obligations of the contractual parties.[54]

**TABLE 29: Aggregated results and level of agreement regarding the need of notification before changing terms**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform have the obligation to notify users before making changes to its Terms of Service? | 15 | 6 | 28 | 1 | 63% |

Out of the total of platforms analyzed, 30% are committed to notifying users if there is any contractual change and 12% have clauses explicitly stating they will not. Only 2% of the platforms do not contain clauses relevant to this criterion.

### *3.2. Notification Requirements before Termination of Services*

The terms of most platforms (42%) also provide the possibility to cease offering their services without any significant notice to users, which means that they may not even be able to save a copy of their uploaded content. Only 14% commit to giving users a significant notice if their services are canceled. In addition, 8% have contradictory terms and 36% do not have provisions considered relevant to this criterion.

[54] The need to allow users to get to know and to position themselves in relation to contractual changes, even if considered minor, is particularly relevant in the Brazilian context, where, according to the Consumer Protection Code (Law no. 8.078/1990), unilateral changes in contracts are considered unfair practices (Art. 51) and are thus void. Therefore, the law ensures that users are aware and can decide whether or not to continue using a service.

**TABLE 30: Aggregated results and level of agreement regarding the need of notification upon termination of services**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Is the platform allowed to terminate its services to all users without a significant notice? | 21 | 7 | 4 | 18 | 74% |

### *3.3. Availability of Earlier Versions of Contracts*

Another criterion examined the possibility of users to access the terms they originally accepted when creating their accounts.[55] In this case, 32% of platform policies provide for this possibility, while most of them (64%) do not have relevant provisions in this regard. One platform (2%) explicitly states that access will not be possible and another one (2%) has clauses considered to be contradictory.

**TABLE 31: Aggregated results and level of agreement regarding the availability of previous versions of contracts**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Are users allowed to access the Terms of Service they originally agreed on when creating their accounts? | 16 | 1 | 1 | 32 | 82% |

[55] In Brazil, Art. 4 in Decree 7.962/12 ensures that users have a right to access the contract they originally accepted in the case of e-commerce services. To ensure easy service to consumers in e-commerce, the supplier shall: [...] IV - make the contract available to consumers, immediately after hiring, in a medium that allows its conservation and reproduction.

### *3.4. Conflict Resolution among Users*

In addition to addressing the amendment and termination of contracts, the Due Process analysis seeks to identify how conflict resolution occurs between users or between users and platforms. These criteria evaluate whether extrajudicial settlements unilaterally defined by platforms exacerbate the power imbalance between contractual parties. The study also analyzed whether platform policies remove/alienate users' rights to appeal judicial redress mechanisms. In an environment of respect for human rights, in addition to having access to the necessary information to exercise their rights, users should have the possibility to take their demands to an impartial and independent court.

Extrajudicial mechanisms for conflict resolution were included within Due Process as a good practice because in certain situations, they may consist in a more responsive and user-friendly conflict resolution method. However, if the Terms of Service of platforms impose an administrative process as the only means for conflict resolution, the clause is seen as a barrier to accessing justice.

Only 4% of the analyzed platforms have made provisions for alternative user dispute resolution mechanisms. Four platforms, 8%, explicitly state that they do not have this kind of mechanism, one (2%) has contradictory clauses, and the majority (86%) has no relevant information.

**TABLE 32: Aggregated results and level of agreement regarding the existence of alternative mechanisms for dispute resolution among users**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform offer alternative conflict resolution mechanisms involving the right to be heard in user disputes? | 2 | 4 | 1 | 43 | 93% |

### *3.5. Conflict Resolution between Users and Platforms*

Regarding the resolution of conflicts between users and platforms, a larger number of platforms provide alternative mechanisms in their policies: 18% of the total analyzed. Six platforms (12%) explicitly say they do not have such mechanisms and the majority (70%) has no relevant clauses on this subject.

**TABLE 33: Aggregated results and level of agreement regarding the existence of alternative mechanisms for dispute resolution between users and platforms**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform offer alternative conflict resolution mechanisms with the right to be heard in disputes between users and the platforms? | 9 | 6 | 0 | 35 | 86% |

### *3.6. Right to Present a Class Action*

In terms of the right to access justice, 26% of the platforms require users to waive their right to present a class action. An example is the following clause from the platform Dropbox:

> You may only resolve disputes with us on an individual basis, and may not bring a claim as a plaintiff or a class member in a class, consolidated, or representative action. Class arbitrations, class actions, private attorney general actions, and consolidation with other arbitrations aren't allowed.

**TABLE 34: Aggregated results and level of agreement regarding the possibility to start a class action**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform require users to waive their right to initiate a class action? | 13 | 0 | 2 | 35 | 95% |

In addition, 4% have contradictory clauses and the majority (70%) does not contain any information on initiating collective actions.

### *3.7. Mandatory Arbitration for Dispute Resolution*

Another aspect related to the right to access to justice was analyzed in the criterion on the imposition of arbitration. The imposition of arbitration as a sole method of conflict resolution between a user and the platform removes the possibility of the former to find recourse to a court to protect his or her interests. This type of restriction was found in 34% of the analyzed platforms.

**TABLE 35: Aggregated results and level of agreement regarding mandatory arbitration**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform impose mandatory arbitration? | 17 | 0 | 1 | 32 | 95% |

Some platforms that mandate arbitration have provisions which allow individual actions to be taken to small claims courts and users to seek injunctive or other equitable relief in order to prevent violations of intellectual property rights. One example of this practice is from the platform Academia.edu:

> You and Academia.edu agree that any dispute, claim or controversy arising out of or relating to these Terms or the breach, termination, enforcement, interpretation or validity thereof or the use of the Site or Services (collectively, "Disputes") will be settled by binding arbitration, except that each party retains the right: (i) to bring an individual action in small claims court and (ii) to seek injunctive or other equitable relief in a court of competent jurisdiction to prevent the actual or threatened 6.infringement, misappropriation or violation of a party's copyrights, trademarks, trade secrets, patents or other intellectual property rights (the action described in the foregoing clause (ii), an "IP Protection Action").

The crowdfunding platform Indiegogo contains a similar clause in its terms:

> Each User agrees that any and all disputes or claims that have arisen or may arise between such User and Indiegogo relating in any way to or arising out of this or previous versions of the Terms or your use of or access to the Services shall be resolved exclusively through final and binding arbitration, rather than in court, except that such User may assert claims in small claims court, if such User claims qualify. The Federal Arbitration Act governs the interpretation and enforcement of this agreement to arbitrate. There is no judge or jury in arbitration, and court review of an arbitration award is limited. However, an arbitrator can award on an individual basis the same damages and relief as a court (including injunctive and declaratory relief or statutory damages), and must follow the provisions of the Terms as a court would.

One platform has contradictory terms and 64% do not have any provision on the subject.

### *3.8. Imposition of Specific Jurisdiction for Dispute Resolution*

Determining a specific jurisdiction to resolve possible judicial disputes was widely found in the policies of analyzed online platforms: 86% of them impose this kind of restriction on access to justice.[56]

Facebook, for example, establishes that disputes shall be settled in California.

> You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims.

**TABLE 36: Aggregated results and level of agreement regarding the imposition of specific jurisdiction for dispute resolution**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform impose on users a specific jurisdiction to settle judicial disputes? | 43 | 0 | 1 | 6 | 83% |

Only one of the platforms (2%) has clauses considered contradictory in this regard and 12% contain no information on their policies about the jurisdiction where legal disputes are to be resolved.

[56] According to the Internet Civil Rights Framework for the Internet (Law 12.965/2014), these clauses are deemed automatically void for not "providing an alternative to the contracting party to adopt the Brazilian forum for resolution of disputes arising from services rendered in Brazil" (Art. 8).

### *3.9. Other Limitations on the Access to Justice*

Finally, it was examined whether or not platform policies imposed restrictions on access to justice other than those mentioned above. Results evidenced that most of them (64%) do so.

**TABLE 37: Aggregated results and level of agreement regarding the existence of other limitations on the access to justice**

| Criterion for Analysis | Total Yes (Y) | Total No (N) | Total Contradictory (C) | Total Empty (E) | Level of agreement |
|---|---|---|---|---|---|
| Does the platform impose further restrictions on users' access to justice? | 32 | 0 | 1 | 17 | 79% |

Flickr, for instance, imposes a time limit of one year for users to claim their rights in court:

> You agree that regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to use of the Yahoo Services or the TOS must be filed within one (1) year after such claim or cause of action arose or be forever barred.

OneDrive determines in its terms that in the event of a dispute, users should try to negotiate their interests informally with the platform owner, Microsoft. If no agreement is reached within 60 days, an arbitration process is initiated.

> In the event of a dispute, you or Microsoft must give the other a Notice of Dispute, which is a written statement that sets forth the name, address and contact information of the party giving it, the facts giving rise to the dispute, and the relief requested. You must send any Notice of Dispute by U.S. Mail to Microsoft Corporation, ATTN: LCA ARBITRATION, One Microsoft Way,

> Redmond, WA 98052-6399, U.S.A. A form is available on the Legal and Corporate Affairs (LCA) website (http://go.microsoft.com/fwlink/?LinkId=245499). Microsoft will send any Notice of Dispute to you by U.S. Mail to your address if we have it, or otherwise to your email address. You and Microsoft will attempt to resolve any dispute through informal negotiation within 60 days from the date the Notice of Dispute is sent. After 60 days, you or Microsoft may commence arbitration.

The same type of imposition was found in the provisions of the platform Pinterest, which establishes that users shall seek an informal resolution of any dispute before going to courts for litigation:

> For any dispute you have with Pinterest, you agree to first contact us and attempt to resolve the dispute with us informally.

Among the analyzed platforms, only 2% contain contradictory clauses regarding other barriers to the access to justice and, in 34%, there was no relevant information for this criterion.

# Final Remarks

This section presents general remarks about platform Terms of Service from a qualitative perspective. The comments derive from reading the contracts of 50 platforms. Next, specific considerations are presented on Freedom of Expression, Privacy and Due Process, based on the quantitative data presented in the Results section.

## 1. General Remarks on Platform Terms of Service

The comments laid out below are based on reading and analyzing the Terms of Service of 50 online platforms and are meant to stimulate further discussion and research.

### Difficulties in identifying binding contracts

The research process evidenced problems in identifying which contracts effectively bind users and platforms. This was either due to the large number of pages to which policies refer, or because not all relevant policies are clearly displayed when users create their account. The research identified an average of three binding documents per platform, which was sometimes followed by a series of auxiliary/additional pages, such as help pages, videos, frequently asked questions (FAQ), etc. Although these do not necessarily have a binding character, they can detail, complement or even contradict[57] the main Terms of Service, sometimes leaving

[57] In an article published in the online magazine Motherboard, Sarah Jeong describes the evolution of Twitter policies regarding freedom of expression, explaining how limitations on permitted content started to increase from auxiliary pages and without any change to main community guidelines (known in this case as Twitter Rules): "[…]

users in a situation of uncertainty regarding their rights and obligations. Difficulties in identifying the binding documents create an initial barrier to a due process. Of particular concern are the cases in which users cannot easily identify all applicable contracts when trying to create an account or reading the main terms.[58] The multiplication of additional documents may also hinder the execution of projects that try to analyze or interpret the Terms of Service in order to, for example, make them easier to read and

2015 saw huge changes in Twitter's policies around speech. The Rules themselves didn't change much, but the page linked out to additional resources sprinkled out through the rest of the Support pages that expanded Twitter's policies in radical ways". For further information see: <http://motherboard.vice.com/read/the-history-of-twitters-rules>.

58 A particularly striking example is from Google: when trying to create an account for a specific company service, for instance YouTube, users are taken to a common subscription page for all Google services in which the general Terms of Service are presented - not the ones that would be relevant to that particular service. The main text indicates that other terms may apply, without clearly indicating which ones and where to find them: "Our Services are very diverse, so sometimes additional terms or product requirements (including age requirements) may apply. Additional terms will be available with the relevant Services, and those additional terms become part of your agreement with us if you use those Services." In the case of YouTube, in order to find rules that apply, it is necessary to look for relevant policies at the bottom of the page. It should be noted that according to YouTube's Terms of Service, Google's general terms do not apply to that platform: "By using or visiting the YouTube website or any YouTube products, software, data feeds, and services provided to you on, from, or through the YouTube website (collectively the "Service") you signify your agreement to (1) these terms and conditions (the "Terms of Service"), (2) Google's Privacy Policy, found at <http://www.youtube.com/t/privacy> and incorporated herein by reference, and (3) YouTube's Community Guidelines, found at <http://www.youtube.com/t/community_guidelines> and also incorporated herein by reference. If you do not agree to any of these terms, the Google Privacy Policy, or the Community Guidelines, please do not use the Service".

understand.[59] A higher level of detail on certain issues and the use of hypertext to provide information in a more accessible form may be considered good practices. However, this is only true if key information is presented clearly and succinctly in the applicable agreements, which should be identified as such and displayed prominently to users.

### Technical language and ambiguous terms

Overall, online platform Terms of Service contain not only legal language, but are full of technical terms. The efforts made by certain platforms to provide quick explanations and hyperlinks to elucidate the meaning of these terms in their legal texts is commendable. However, in many situations, there is no clear explanation of the impact the use of certain technologies, such as *cookies,* for example, may have on users' rights.

### Lack of information on aspects considered important for human rights

When it comes to the right to privacy, the model adopted in different jurisdictions is based on the principle of privacy self-management, in which data subjects are responsible for authorizing or not the processing of their personal data considering its possible costs and benefits (Solove, 2013).[60] Therefore, it is essential that they base their decisions on relevant information. The analy-

[59] A number of independent projects seek to translate Terms of Service into a more accessible language and format for users. More information about some of them can be found in Annex I.

[60] Both in Europe, with current Directive 95/46/EC, and in Brazil, with its Civil Rights Framework for Internet, consent is a condition that legitimizes the processing of personal data. It must be free (i.e., not forced), informed (individuals must be provided with all the information in a clear and intelligible form) and specific (in relation to a particular purpose). In the US as well, since the 1970s the prevailing idea is that individuals have a number of rights that allow them to manage their personal data, including notification and consent.

sis of the Terms of Service evidenced, however, a lack of relevant information for promoting the rights to privacy and freedom of expression. As highlighted by the Council of Europe in its Human Rights Guide for Internet Users, users must have access to information on platform content policies in order to make informed decisions about whether or not to use these services.[61] The silence of a significant part of the sample (36%) on the obligation to notify and give users the right to be heard before the removal of content - in addition to platforms that expressly state that they may remove content without any notice (52%) - contradicts that orientation. Similarly, the fact that 60% of the platforms make no mention of the removal of personal data after the deletion of an account makes it difficult for users to make decisions on consenting or not to processing when joining their service. These two cases exemplify information considered important for the exercise of online human rights that are absent from many platforms.

## 2. Specific Remarks

Besides the above general remarks, some conclusions can be drawn from the quantitative analysis of the compliance of Terms of Service with the rights to Freedom of Expression, Privacy and Due Process. They are presented below.

### *2.1. Freedom of Expression*

Online platforms offer few guarantees in their policies on preserving the right to freedom of expression. There is a lack of clear and specific information in the Terms of Service on which content is allowed or not in the platform. There is also little commitment to offering users justification, notice and the right to be heard when content is removed by the platforms' own initiative or after notification from third parties.

[61] Appendix to Recommendation CM/Rec(2014)6, Freedom of expression and information, paragraph 5.

More attention seems to be given to mechanisms for reporting abusive content considered abusive by users. This is not necessarily a negative finding, and in some cases may increase the protection of users' rights. However, it must be balanced with effective guarantees on freedom of expression, so that it does not result in an indirect incentive to the indiscriminate removal of content. The need to mitigate the risk of legal actions relating to copyright infringements or defamation may be the reason for the imbalance between the guarantees given to possible victims of abusive content and content authors. This could also explain the lack of appeal mechanisms in the event of removals, once platforms have developed their policies in order to be able to act quickly in case they experience any kind of pressure arising from content posted by users.[62]

[62] Initiatives aimed at limiting the liability of online intermediaries for third party content are a positive way of easing the pressure on platforms. An example of this type of measure can be found in the Civil Rights Framework for the Internet (12.965/2014), which states: "Art. 18. The Internet connection provider shall not be liable for civil damages resulting from content generated by third parties. Art. 19. In order to ensure freedom of expression and to prevent censorship, the provider of internet applications can only be subject to civil liability for damages resulting from content generated by third parties if, after a specific court order, it does not take any steps to, within the framework of their service and within the time stated in the order, make unavailable the content that was identified as being unlawful, unless otherwise provided by law. §1. The referred court order must include, under penalty of being null, clear identification of the specific content identified as infringing, allowing the unquestionable location of the material. §2. The implementation of the provisions of this article for infringement of copyright or related rights is subject to a specific legal provision, which must respect freedom of speech and other guarantees provided for in art. 5º of the Federal Constitution. §3º Compensation disputes for damages arising from content made available on the internet related to the honor, reputation or personality rights, as well as the removal of related contents by internet application providers, can be presented to special small causes courts. §4º The judge, including the proceeding set forth in §3º, can anticipate, partially or in full, the effects of the request contained in

In addition to the international mechanisms identified in the item Methodology of this report, in Brazil, the Civil Rights Framework for the Internet (Law 12.965/2014) establishes the duty for application providers to notify users whose content is restricted and to provide information that will enable them to exercise their rights to contest and submit a defense (art. 20), which can be considered a good practice.[63]

An analysis of the quantitative data presented in the section Results supports the general perception of how platform Terms of Service deal with the right to freedom of expression. Some comments are presented below:

**Content monitoring is provided in the policies of most platforms in an ambiguous or unclear way**

Monitoring of user-generated content for undefined or unclear purposes is provided in the terms of 56% of analyzed platforms. In addition, another 40% have ambiguous clauses on the reasons for monitoring, which also evidences a lack of clarity. In this sense, more than 90% of the platforms do not offer security to users regarding the reasons for monitoring their content.

**Platforms do not provide notification if there are restrictions on freedom of expression**

When user-generated content removal occurs, affected authors may not receive any notice or opportunity to defend themselves

the initial petition, to the extent that undisputable proof exists of the fact, considering society's collective interest in the availability of the content on the internet, as long as it can be proven that the author's claims are true, that there is reasonable concern of irreparable damage, or of damage that is difficult to repair".

63 As provided on art. 20 of Law 12.965/2014: "Art. 20. Whenever contact information of users directly responsible for contents referred to in art. 19 is available, it will be up to the Internet application provider to communicate them the reasons and information relating to the unavailability of content, with information allowing the contradictory and the ample defense in court, unless express legal provision or express judicial determination to the contrary".

according to the Terms of Service of more than half of the analyzed platforms (52%). Aside from those, 36% are silent about notification and the right to be heard in such cases. This does not necessarily mean that, in practice, platforms are not providing such guarantees, but the absence of a clear commitment in the Terms of Service of 88% of the sample may give rise to abuses. Even more troublesome is the fact that 88% of the platforms explicitly state that they can end user accounts without giving them any notice or the opportunity to challenge the decision. None of the analyzed platforms commit in their policies to notifying affected users if their accounts have been terminated for any reason.

**Most platforms offer clear mechanisms for reporting abusive content and requesting their removal**

Results show that most platforms (70%) comprise mechanisms for reporting abusive content and request their removal in their policies. None of the analyzed platforms explicitly state not having such mechanisms, one (2%) has contradictory clauses on the issue and 28% do not contain any information in this regard. These results can be considered positive, since they show that users are offered guarantees in case of third party violations of their rights. However, the fact that these mechanisms are not followed by a commitment to inform and communicate with the authors of the affected content, is a matter of concern. Moreover, it is noteworthy that in many cases, the existing mechanisms refer to the aforementioned *Digital Millennium Copyright Act* (DMCA), imposed on platforms by US law as a condition for the immunity of liability for third-party content in the case of copyright infringement. Mechanisms for reporting other types of abusive content are not always available.

**A limited number of platforms allow anonymity or the use of pseudonyms in their policies**

Contrary to the recommendations on freedom of expression by the United Nations special rapporteurs (see Methodology),

32% of the analyzed platforms do not allow anonymity or the use of pseudonyms in their policies. In addition, 8% of them have ambiguous policies on anonymity and 32% have no provisions on the subject.

### *2.2. Privacy*

Platform policies tend to be longer and more detailed with regard to privacy and the processing of personal data. This is not surprising in the privacy self-management model since the acceptance of these contracts represents users' consent and, therefore, legitimizes the processing of their data. Thus, it is somehow expected that Terms of Service provide enough information to users so they can make informed decisions.[64]

Providing more information through highlighted clauses, help and video pages, for example, may be important for users who want to better understand how their data will be processed if that is done in a clear and concise manner. These measures, however, do not solve the problem of consent in a context in which Terms of Service are rarely read.

In addition, the emergence and advancement of new processing technologies and businesses based on the intensive processing of personal data have brought new challenges to the model of consent. Solove (2013) comments on structural problems, including: (i) a problem of scale, due to the huge number of entities that process personal data, some of which are invisible to data

[64] In the words of Daniel Solove (2013): "Providing people with notice, access, and the ability to control their data is key to facilitating some autonomy in a world where decisions are increasingly being made about them with the use of personal data, automated processes, and clandestine rationales, and where people have minimal abilities to do anything about such decisions. A world without privacy self-management would clearly be troublesome, as people should have rights to know about how their data is being used and to make decisions about those uses".

subjects;[65] (ii) an aggregation problem, namely that it is nowadays possible to deduce sensitive information about a person from the combination of data, which otherwise would seem harmless, from different sources , and (iii) a problem of assessing harm, since the negative impacts of sharing certain data may only be evident a long period after processing, while benefits are usually immediate.[66]

In this context, it seems important that online services consider adopting more explicit and affirmative mechanisms for obtaining consent, instead of seeking the acceptance of a single and general contract. This type of approach has not yet been prioritized by the analyzed platforms. On the contrary, in general, their terms are drafted so as to be broad enough to ensure that companies can perform various operations using user data without the need to change the contract or to require a new consent. While this might be a more practical and, possibly, economic solution for platforms, it is not the most protective from a human rights perspective.

Given this situation, it is possible to identify some tendencies regarding the processing of personal data from the analysis of platform Terms of Service. They are detailed below:

**Policies usually anticipate tracking user activities on other websites and allow third party tracking by default**

The large number of platforms that request user consent to monitor their activities on other websites seems to indicate that this is

[65] In Solove's words (2013): "Not only will people struggle to manage privacy with the entities they know about, but there are also scores of entities that traffic in personal data without people ever being aware. People cannot manage their privacy with regard to these extensive "reservoirs" of data unless they know these reservoirs exist and can identify the various entities that maintain them".

[66] Cohen (2012) lists some of the immediate benefits of personalization, which are very appealing to consumers, regardless of the damages that may arise in the long term.
They include, for example, discounts, improved products and services, access to the most convenient resources and increased social status.

a common practice in the market: 66%, compared to only 4% that do not make provisions for this (30% do not have any information about it in their policies). Similarly, an even higher percentage of the sample (80%) states that they may allow third parties to monitor user activities while using their services. In both cases, requesting general consent prevails by default. Few are the cases in which users can opt-out of being monitored, with restricted possibilities of effectively managing their personal data. It is worth noting that, in general, terms do give enough information for users to identify which activities platforms or third parties are able to monitor as well, as though it only happens when users are logged onto the platforms or not. Similarly, in relation to third-party tracking, Terms of Service are usually unclear about the entities that can perform this type of monitoring.

**Data sharing with partners is significant**

When it comes to sharing user data with third parties for various purposes beyond legal requirements (commercial, technical, processing or others), most platforms state that they may do so by default (62%). Although the purposes are specified in some cases, usually such provisions are broad and generic, giving rise to situations in which platforms can share data.

**Requests for consent to aggregate data among different services is more common than from different devices**

While the policies of 52% of analyzed platforms have provisions for aggregating personal data collected in different services from the same company or affiliates, 38% do so to aggregate data collected on different devices.

**Scanning private content is mentioned in less than half of the analyzed platforms**

Consent for scanning users' private communications for various purposes is requested in 44% of the platforms. Most of the other platforms (46%) have no clauses in this regard.

**Policies tend to be complacent about data sharing requests from government and law enforcement agencies**

When it comes to sharing data with government or law enforcement authorities, policies do not usually provide sufficient guarantees to their users; despite the recommendations contained in the international human rights standards (see Methodology). In most cases (54%), platforms do no commit through their policies to a legitimate judicial process before providing user data to the authorities. In addition, 30% have contradictory clauses, offering little security to users. The fact that certain platforms (10%) explicitly commit to the observance of a specific legal process before providing data for government officials seems to show that the market could sustain the establishment of clear commitments in this regard.

**More platforms are committed to encrypting transmitted content in comparison to stored content**

Only half of the platforms are committed–at least as a matter of written policy—to the use encryption to protect users' personal data or content. The number of platforms committed to encrypting stored data is even lower: 38% of the total. Among the companies that mention encryption, there is a wide dissemination of the *Transport Layer Security* (TLS) and *Secure Sockets Layer* (SSL) protocols for transmitted data. The encryption of only certain personal data (such as credit cards, passwords and email addresses) is more common than of stored content and was considered sufficient to indicate that the platform adopts encryption.

### *2.3. Due Process*

With regard to due process, on the one hand, platform obligations are not clear and clauses that limit users' access to justice were observed. On the other hand, the analyzed policies have no provisions for alternative mechanisms of dispute resolution among users or between users and platforms.

**Users are not always informed about changes in Terms of Service and hardly have access to the original contracts accepted when joining the platform.**

Only 30% of the platforms explicitly commit to notifying users about changes in their terms, while 56% of them have contradictory clauses in this regard. In many of those cases, there is a partial commitment to notification, only if the changes are considered significant by the platforms. It should be noted, however, that even minor changes can have an impact on the rights of users, who, therefore, should be informed. The fact that 12% of the analyzed platforms claim that there will be no notification even for significant changes is even more worrying. When it comes to giving access to the contract originally accepted when creating an account, few platforms ensure this possibility (32%). Most of them (64%) do not commit to storing previous versions of their terms for possible consultation.

**Judicial disputes are usually subject to a number of limitations on the access of users to justice.**

Several platforms impose a limitation on users' access to justice: 26% require users to waive their right to initiate a class action; 34% impose arbitration as the only method for resolving disputes, and 86% have clauses establishing the platform's jurisdiction as the only alternative for dispute resolution. Although the number of platforms that determine a specific jurisdiction for possible disputes is significant, these clauses are quite common in many types of standardized contracts. The main difference in the case of online platforms is the fact that often user-platform relationships go beyond the jurisdiction of a particular country, encompassing two or more distinct legal systems. In this context, these clauses can make it prohibitively expensive for individuals to exercise their rights to access justice and prevent the effective accomplishment of a due process. Finally, 64% of the pla-

tforms impose other restrictions on accessing justice besides those mentioned above.

**There are no provisions for alternative mechanisms for conflict resolution.**

Most platforms do not provide their users with alternative mechanisms for conflict resolution. Only 4% include them in their policies for disputes involving only users and 18% when it comes to disputes between users and the platforms.

# Conclusion

The terms of service of online platforms influence the exercise of various human rights, including the right to freedom of expression, privacy and due process.

Since such documents are difficult to read and understand, there is no real impact for users.

This makes it difficult to understand how their rights are affected, undermines their right to determine whether or not to adhere to certain platforms and make it impossible to compare the degree of protection offered by competing platforms, which could create market incentives for an increased compliance of terms of service according to human rights protection standards present in international instruments.

The methodology for analyzing terms of service developed under the project "Terms of Service and Human Rights" has produced empirical data on the compliance of standardized contracts with human rights, as well as identified common policies. Hopefully, the results presented in this report will contribute to future research and policymaking in harmony with human rights by both private and public entities.

## References


Article 19. (2012). *Ameaças na rede: relatório de violações contar blogueiros, donos ou editores de sites e usuários de internet em 2012*. São Paulo.

Bakos, Y.; Marotta-Wurgler, F.; Trossen, D. R. (2014) *Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts*. Journal of Legal Studies, Vol. 43, No. 1, 2014; CELS 2009 4th Annual Conference on Empirical Legal Studies Paper; NYU Law and Economics Research Paper No. 09-40. Available at: <http://ssrn.com/abstract=1443256>.

Benedek, W. & Kettermann, M. C. (2013). *Freedom of Expression and the Internet*. Strasbourg: Council of Europe Publishing.

Benkler, Y. (2003) *Freedom in the Commons: Towards a Political Economy of Information*. Duke Law Journal. Available at: <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1191&context=dlj>.

Benkler, Y. (2000). "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access", *Federal Communications Law Journal*, vol. 52, 2000.

Bruno, F. (2013). *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. Porto Alegre: Sulina.

Belli, L. (2016). *De la gouvernance à la régulation de l'Internet*. Paris, Berger-Levrault.

Belli, L. & De Filippi, P. (2012). *Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation*. European Journal for Law and Technology, Vol. 3, Nº 2.

Bygrave, L. A. (2015). *Internet Governance by Contract*. Oxford.

Cohen, J. E. (2013). *What Privacy Is For*. Harvard Law Review, Vol. 126, 2013. Available at: <http://ssrn.com/abstract=2175406>.

Doneda, D. (2006) *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar.

European Commission. (2015). *A Digital Single Market Strategy for Europe - Analysis and Evidence*, COM(2015) 192, p. 52.

Internet Commissioner's Office, ICO (2011). *Data sharing code of practice*. Available at: <https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf>.

Jenkins, H. (2006). *Confronting the challenges of participatory culture: Media education for the 21st century.* White Paper. MacArthur Foundation.

Kim, N. S. (2012). *The Duty to Draft Reasonably and Online Contracts.* Cambridge University Press. Chapter 8, in Commercial contract law: a transatlantic perspective. Eds. Larry DiMatteo, Keith Rowley, Severine Saintier, and George Zhou. Cambridge University Press.

Lemley, M. A. (2006). *Terms of Use*, 91 MINN. L. REV. 459, 459. Available at: <http://www.kentlaw.edu/faculty/rwarner/classes/ecommerce/2008/contracts/consent/lemley%20tersm%20of%20use.pdf>.

Lessig, L. (1999). *Code and other laws of cyberspace.* Basic books.

Loren, Lydia Pallas. (2004). *Slaying the Leader-Winged Demons in the Night: Reforming Copyright Owning Contracting with Clickwrap Misuse*, 30 OHIO, N.U.L. REV. 495, 512-22.

Louzada, L. & Venturini, J. (2015). *A regulamentação da proteção de dados pessoais no Brasil e na Europa: uma análise comparativa*. Available at: <http://lavitsrio2015.medialabufrj.net/anais/#theme-1>.

MacKinnon, R. (2012). *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York, Basic Books.

MacKinnon et. al. (2015) *Fostering Freedom Online: the Role of Internet Intermediaries.* Paris: Unesco. Available at: <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>.

Magrani, E. (2014) *Democracia Conectada: a Internet como Ferramenta de Engajamento Político-Democrático*. Curitiba: JURUA. Available at: <http://bibliotecadigital.fgv.br/dspace/handle/10438/14106>.

McDonald, A. M., & Cranor, L. F. (2008). *The Cost of Reading Privacy Policies.* ISJLP, 4, 543. Available at: <http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf>.

Nery Junior, Nelson (2010). *Princípios do Processo na Constituição Federal*. 10th ed. São Paulo: Revista dos Tribunais.

OECD. (2010). *The Economic and Social Role of Internet Intermediaries*. Available at: <http://www.oecd.org/internet/ieconomy/44949023.pdf>.

OECD (2011) *The Role of Internet Intermediaries in Advancing Public Policy Objectives* DSTI/ICCP(2010)11/FINAL

Pasquale F.A. (2010). "*Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries"*. Northwestern University Law Review. Vol. 104, No. 1, p. 105. Available at: <www.law.northwestern.edu/lawreview/v104/n1/105/LR104n1Pasquale.pdf>.

Petit Jr, M. (1983), *Modern Unilateral Contracts*, 63, B.U.L. REV. 551, 551.

Randall, S (2004). *Judicial Attitudes Toward Arbitration and the Resurgence of Unconscionability*, 52 BUFF. L. REV. 185, 186.

Sarlet, I. W. (2006). *A eficácia dos direitos fundamentais*. 6. ed. Porto Alegre: Livraria do Advogado.

Sarmento, D. (2004*). Direitos fundamentais e relações privadas*. Rio de Janeiro: Lumen Juris.

Sarmento, D. & Gomes, F. R. (2011). *A Eficácia dos Direitos Fundamentais nas Relações entre particulares: o caso das relações de trabalho*. Rev. TST, Brasília, vol. 77, n° 4, Oct./Dec. Available at: <http://aplicacao.tst.jus.br/dspace/bitstream/handle/1939/28342/003_sarmento_gomes.pdf?sequence=3>.

Solove, D. (2013*) Introduction: Privacy self-management and the consent dilemma*. In Harvard law review. Vol. 126: p. 1884. Available at: <http://www.harvardlawreview.org/media/pdf/vol126_solove.pdf>.

Stylinou, K. (2010) *An Evolutionary Study of Cloud Services Privacy Terms*. In John Marshall Journal of Computer & Information Law, Vol. 27, No. 4. Available at: <http://ssrn.com/abstract=1764633>.

Sweeney, L., Abu, A. & Winn, J. (2013). *Identifying participants in the personal genome project by name*.

União Internacional das Telecomunicações. (2014). *ICT Facts and Figures.* Available at: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf>.

Zingales, N. (2013). *Accountability 2.0: Towards a special responsibility of Internet intermediaries*, Global Internet Governance Academic Network (GIGANET) Annual Conference proceedings 2013.

Zittrain. J. (2006). *"A History of Online Gatekeeping*". Harvard Journal of Law & Technology. Vol. 19, No. 2, pp. 253-98. Available at: <http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf>.

## News


Farivar, C. (2012) *How one law student is making Facebook get serious about privacy.* Arstechnica. Available at: <http://arstechnica.com/tech-policy/2012/11/how-one-law-student-is-making-facebook-get-serious-about-privacy/>.

Agência Lusa. (2012) *Facebook suspende ferramenta de reconhecimento facial*. EBC. Available at: <http://www.ebc.com.br/tecnologia/2012/09/facebook-suspende-ferramenta-de-reconhecimento-facial>.

Alsenoy, B.V. et al. (2015) *From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms.* v.1.3. Available at: <http://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf>.

Carr N. (2009). *Googler in the Middle.* Rough Type. Available at: <http://www.roughtype.com/?p=1249>.

Jeong, S. (2016) *The History of Twitter's Rules.* Motherboard. Available at: <http://motherboard.vice.com/read/the-history-of-twitters-rules>.

Micali, B. (2015) *O fim de uma era do compartilhamento: RapidShare acaba no dia 31 de março*. Tec Mundo. Available at: <http://www.tecmundo.com.br/compartilhador/74913-fim-compartilhamento-rapidshare-acaba-dia-31-marco.htm>.

Costa, C. (2013). *Brasileiros 'descobrem' mobilização em redes sociais durante protestos*. BBC Brasil. Available at: <http://www.bbc.co.uk/portuguese/noticias/2013/07/130628_protestos_redes_personagens_cc>.

Farivar, C (2012). *"How One Law Student is Making Facebook get Serious About Privacy"*. Available at: <http://arstechnica.com/tech-policy/2012/11/how-one-law-student-is-making-facebook-get-serious-about-privacy/>.

Muotri, A. (2013). *O Brasil descobriu o poder das redes sociais*. G1 Espiral. Available at: <http://g1.globo.com/platb/espiral/2013/06/21/o-brasil-descobriu-o-poder-das-redes-sociais/>.

Pinho, L. & Rodrigues, K. (2015). *Marco Civil da Internet: o diabo está no detalhe*. Available at: <https://www.eff.org/pt-br/deeplinks/2015/03/marco-civil-da-internet-o-diabo-esta-no-detalhe>.

## ANNEX I - RELATED PROJECTS AND CIVIL SOCIETY INITIATIVES

Below is a non-exhaustive list of projects, mapped during the research, which deal with the Terms of Service and regulation by intermediaries in the online environment:

| Name | Page | Description |
|---|---|---|
| Common Terms | http://commonterms.net/ | Project originating in Sweden, which seeks to develop a preview mechanism for Terms of Service, summarizing their main points with icons and short descriptions on these practices. It is based on the fact that few people read the Terms of Service and still claim to have them read just to access the services, which may have consequences for users and the market. |
| Customer Commons | http://customercommons.org | Non-profit organization based in California, United States, which seeks to "restore the balance of power, respect and trust between individuals and organizations that serve them." It develops an extension called "Web Pal" that blocks tracking attempts and ads during browsing. |
| Disconnect.Me | https://disconnect.me/ | Start-up based in California, United States, which provides extensions to block tracking by third parties during browsing. It has a tool called "Privacy Icons" showing icons summarizing the key practices related to privacy for each page visited or found in search engines. |

| | | |
|---|---|---|
| know Privacy | http://knowprivacy.org | Project that has mapped the common collection practices, sharing and analysis of personal data on the web and crossed them with users' expectations on privacy in order to make recommendations to the industry and regulators. |
| Legal Geek | http://www.legalgeek.it | Database of terms of use, currently brings together about 1900 terms for consultation. |
| Open Notice | http://opennotice.org | Its goal is to develop a standardized model of consent and authorization for privacy policies and Terms of Service. Seeks to join efforts of the various initiatives dealing on those issues in order to solve the problem of acceptance of terms without reading (the so called "the biggest lie on the web", already mentioned *the biggest lie)*. |
| Privacy Icons | http://www.azarask.in/blog/post/privacy-icons/ | It developed icons to describe a series of privacy parameters. |
| Privacy Labels | http://cups.cs.cmu.edu/privacyLabel/ | Initiative from the Carnegie Mellon University, United States, that proposes a standardized table, based on the model of the nutritional information table found in food packing, to present data privacy. |
| Ranking Digital Rights | https://rankingdigitalrights.org/ | The Ranking Digital Rights project seeks to develop a ranking of the largest companies in the information and communication technologies sector considering the degree of protection of the rights to freedom of expression and privacy offered to their users. The proposal is to encourage companies to develop and offer their products and services in alignment with human rights. Although it is a broader project, Terms of Service are not between the criteria considered in the construction of the ranking. |

| | | |
|---|---|---|
| Standard Information Sharing Label | http://standardlabel.org/ | Based on the table of nutritional information for food packing, the project aims to easily compile and display in a summarized way information about sharing personal information with online services. |
| Terminos y Condiciones | http://terminosycondiciones.es/ | It compiles commented versions of the terms of various online services and provides periodic updates on any changes. |
| ToS;DR | https://tosdr.org | It includes peer review and classification of Terms of Service according to companies' practices. It provides an extension that shows a summary and evaluation of the terms of the sites accessed during browsing. |
| ToS Back | https://tosback.org/ | A Beta version tracker for Terms of Service. A partnership between the Electronic Frontier Foundation (EFF) and the ToS;DR project. |

In addition to the projects mentioned above, some documents pushed by the civil society seek to develop additional parameters to international human rights standards in relation to relational matters on the liability of intermediaries and online contracts. Some examples are:

- **Principles on Freedom of Expression and Copyright in the Digital Age** (http://www.article19.org/data/files/medialibrary/3716/13-04-23-right-to-share-PO.pdf): The human rights organization Article 19 launched in 2013 a document on the "Right to Share: Principles on Freedom of Expression and Copyright in the Digital Age" in which - starting from standards and international jurisprudence - it gathers principles to guide legislators, judiciary and civil society on how to seek balance on freedom of expression and copyright.
- **International Principles on the Application of Human Rights in Communications Surveillance** (https://pt.necessaryandproportionate.org/text): The document was

developed by an alliance of civil society organizations that included Electronic Frontier Foundation, Privacy International, Access, and Article 19 and gathers the minimum standards for the protection of the rights to freedom of expression and privacy in mass surveillance contexts. The principles were endorsed by 400 international organizations and more than 300,000 individuals around the world.

- **The Manila Principles on Accountability for the Intermediaries** (https://www.manilaprinciples.org/): Also developed from a coalition of civil society organizations, the Manila Principles seek to provide a guide of good practices on intermediary liability policies on third-party content. The document is intended primarily for legislators and intermediaries, to policy developments. The proposal is to promote a harmonized and interoperable system of accountability that is aligned with international human rights.

## ANNEX II - ANALYZED PLATFORMS AND DOCUMENTS

Below is the complete list of analyzed platforms, as well as the documents used by each of the analysts and the dates of their last modification:

| Platform | Analyst 1 | Analyst 2 | Analyst 3 | Date of the analyzed document | Date of filing |
|---|---|---|---|---|---|
| 4shared | Terms of Service | Terms of Service | Terms of Service | 4/06/2012 | 2/25/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | - | 2/25/2015 |
| | DMCA Policy | DMCA Policy | DMCA Policy | - | 2/25/2015 |
| Academia.edu | Terms of Service | Terms of Service | Terms of Service | 3/13/2013 | 12/23/2014 |
| | Privacy Policy | Privacy Policy | Privacy Policy | - | 12/23/2014 |
| **AirBnb** | Terms of Service | Terms of Service | Terms of Service | 6/30/2014 | 11/6/2014 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 4/7/2014 | 11/6/2014 |
| **Ashley Madison** | Terms of Service | Terms of Service | Terms of Service | 11/21/2013 | 12/11/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 11/3/2011 | 12/11/2015 |
| **Ask.fm** | Terms of Service | Terms of Service | Terms of Service | 12/1/2014 | 12/29/2014 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 12/1/2014 | 12/29/2014 |
| | Cookies Policy | Cookies Policy | Cookies Policy | 12/1/2014 | 12/29/2014 |
| | FAQ for parents | | | - | 12/29/2014 |

| | | | | | |
|---|---|---|---|---|---|
| **Cartoon Network** | Terms of Service | Terms of Service | Terms of Service | 10/8/2014 | 1/6/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 8/8/2014 | 1/7/2015 |
| **Delicious** | Terms of Service | Terms of Service | Terms of Service | 1/10/2013 | 1/21/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 1/10/2013 | 1/21/2015 |
| | | Copyright Policy | | - | 9/25/2015 |
| **Docracy** | Terms of Service | Terms of Service | Terms of Service | 2/7/2013 | 1/22/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 2/7/2013 | 1/22/2015 |
| Doodle | Terms of Service | Terms of Service | Terms of Service | 6/25/2012 | 1/26/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 9/24/2014 | 1/26/2015 |
| **Dropbox** | Terms of Service | Terms of Service | Terms of Service | 1/22/2015 | 2/23/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 2/13/2015 | 2/23/2015 |
| | Acceptable Service Policy | Acceptable Service Policy | Acceptable Service Policy | - | 2/23/2015 |
| | Government Data Requests Principles | Government Data Requests Principles | Government Data Requests Principles | - | 2/23/2015 |
| | | How does Dropbox use cookies and similar technologies? | How does Dropbox use cookies and similar technologies? | - | 9/27/2015 |

| | | | | | |
|---|---|---|---|---|---|
| **Ello** | Privacy Policy | Privacy Policy | Privacy Policy | 10/3/2014 | 1/26/2015 |
| **Facebook** | Terms of Service | Terms of Service | Terms of Service | 1/30/2015 | 3/3/2015 |
| | Data Use Policy | Data Use Policy | Data Use Policy | 1/30/2015 | 3/3/2015 |
| | Community Standards | Community Standards | Community Standards | - | 2/17/2016 |
| | Principles | Principles | Principles | - | 10/13/2014 |
| | | Page Terms | | 1/16/2015 | 9/27/2015 |
| | Cookies, Pixels & Similar Technologies | | Cookies, Pixels & Similar Technologies | - | 3/3/2015 |
| **Flickr** | Terms of Service | Terms of Service | Terms of Service | 3/16/2012 | 12/23/2014 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 9/25/2014 | 12/23/2014 |
| | Content Upload Additional Terms | Content Upload Additional Terms | Content Upload Additional Terms | - | 12/23/2014 |
| | Universal Anti-Spam Policy | Universal Anti-Spam Policy | Universal Anti-Spam Policy | - | 12/23/2014 |
| **Freenode** | Policies | Policies | Policies | - | 12/30/2014 |
| **GitHub** | Terms of Service | Terms of Service | Terms of Service | - | 1/7/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | - | 1/7/2015 |

| | | | | | |
|---|---|---|---|---|---|
| **Gmail** | Terms of Service | Terms of Service | Terms of Service | 4/14/2014 | 2/19/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 12/19/2014 | 2/19/2015 |
| | Gmail Program Policies | Gmail Program Policies | Gmail Program Policies | - | 2/26/2015 |
| **Google Groups** | Terms of Service | Terms of Service | Terms of Service | 4/14/2014 | 2/19/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 12/19/2014 | 2/19/2015 |
| | Content Policies | Content Policies | Content Policies | - | 2/26/2015 |
| Google Drive | Terms of Service | Terms of Service | Terms of Service | 4/14/2014 | 2/19/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 12/19/2014 | 2/19/2015 |
| **Google Plus** | Terms of Service | Terms of Service | Terms of Service | 4/14/2014 | 2/19/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 12/19/2014 | 2/19/2015 |
| | User Conduct and Content Policy | User Conduct and Content Policy | User Conduct and Content Policy | - | 3/3/2015 |
| | G+ Pages Additional Terms of Service | G+ Pages Additional Terms of Service | G+ Pages Additional Terms of Service | - | 3/3/2015 |
| | Embedded Content Policy | Embedded Content Policy | Embedded Content Policy | - | 3/3/2015 |
| **Gruveo** | Privacy Policy | Privacy Policy | Privacy Policy | - | 1/23/2015 |

| | | | | | |
|---|---|---|---|---|---|
| **Hotmail** | Services Agreement | Services Agreement | Services Agreement | 7/31/2014 | 12/12/2014 |
| | Privacy Statement | Privacy Statement | Privacy Statement | 10.2014 | 12/12/2014 |
| | Privacy Statement for Online Advertising | Privacy Statement for Online Advertising | Privacy Statement for Online Advertising | 09.2014 | 12/16/2014 |
| **Indiegogo** | Terms of Service | Terms of Service | Terms of Service | 12/15/2014 | 1/23/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 6/16/2014 | 1/23/2015 |
| | Cookies Policy | Cookies Policy | Cookies Policy | 2/26/2013 | 1/23/2015 |
| **Jamendo** | Terms of Service | Terms of Service | Terms of Service | 2/21/2013 | 1/6/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 12/13/2013 | 1/6/2015 |
| **Kickstarter** | Terms of Service | Terms of Service | Terms of Service | 10/19/2014 | 1/27/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 8/10/2014 | 1/27/2015 |
| | Cookies Policy | Cookies Policy | Cookies Policy | - | 9/25/2015 |
| | | Copyright Policy | | - | 9/25/2015 |
| **Kidsworld** | Privacy Policy | Privacy Policy | Privacy Policy | - | 1/8/2015 |
| | Security Guidelines | | | - | 1/8/2015 |
| **LinkedIn** | Privacy Policy | Privacy Policy | Privacy Policy | 10/23/2014 | 3/5/2015 |
| | Cookies Policy | Cookies Policy | Cookies Policy | 9/18/2014 | 3/5/2015 |
| | User Agreement | User Agreement | User Agreement | 10/23/2014 | 3/5/2015 |
| | | Copyright Policy | | 3/26/2014 | 9/22/2015 |

| | | | | | |
|---|---|---|---|---|---|
| **Mega** | Terms of Service | Terms of Service | Terms of Service | – | 1/13/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | – | 1/13/2015 |
| | Content Removal Policy | | Content Removal Policy | 8/21/2013 | 1/13/2015 |
| | Affiliates Terms of Service | | Affiliates Terms of Service | – | 1/13/2015 |
| **MyHeritage** | Terms of Service | Terms of Service | Terms of Service | – | 1/27/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 8/8/2012 | 1/27/2015 |
| **MyKolab** | Terms of Service | Terms of Service | Terms of Service | 7/25/2013 | 1/5/2015 |
| | Privacy Statement | Privacy Statement | Privacy Statement | 6/1/2014 | 1/5/2015 |
| **MySpace** | Agreement of Terms of Service | Agreement of Terms of Service | Agreement of Terms of Service | 6/10/2013 | 1/9/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 6/24/2014 | 1/9/2015 |
| | Cookies Policy | Cookies Policy | Cookies Policy | 6/10/2013 | 1/9/2015 |
| | Videos Privacy Policy | Videos Privacy Policy | Videos Privacy Policy | 6/24/2014 | 1/9/2015 |
| | Police Authorities Guidelines | Police Authorities Guidelines | Police Authorities Guidelines | 6/10/2013 | 1/9/2015 |
| **One Drive** | Services Agreement | Services Agreement | Services Agreement | 7/31/2014 | 12/12/2014 |
| | Privacy Statement | Privacy Statement | Privacy Statement | 10.2014 | 12/12/2014 |
| | Privacy Statement for Online Advertising | Privacy Statement for Online Advertising | Privacy Statement for Online Advertising | 09.2014 | 12/16/2014 |

| | | | | | |
|---|---|---|---|---|---|
| **Oovoo** | Terms of Service | Terms of Service | Terms of Service | - | 1/5/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | - | 1/5/2015 |
| **Pinterest** | Terms of Service | Terms of Service | Terms of Service | - | 1/5/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 10/19/2014 | 1/5/2015 |
| | Copyright Policy | Copyright Policy | Copyright Policy | - | 1/5/2015 |
| | Acceptable Service Policy | | | - | 1/5/2015 |
| **Rapidshare** | Terms of Service | Terms of Service | Terms of Service | - | 1/15/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | - | 1/15/2015 |
| **Reddit** | User Agreement | User Agreement | User Agreement | 5/15/2014 | 1/7/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 7/18/2014 | 1/7/2015 |
| **RiseUp** | Terms of Service | Terms of Service | Terms of Service | 4/15/2015 | 1/6/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | - | 1/6/2015 |
| | DMCA Policy | DMCA Policy | DMCA Policy | - | 1/6/2015 |
| **Skype** | Terms of Service | Terms of Service | Terms of Service | 06.2014 | 12/18/2014 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 04.2014 | 12/18/2014 |
| **Slideshare** | Privacy Policy | Privacy Policy | Privacy Policy | 10/23/2014 | 3/5/2015 |
| | Cookies Policy | Cookies Policy | Cookies Policy | 9/18/2014 | 3/5/2015 |
| | User Agreement | User Agreement | User Agreement | 10/23/2014 | 3/5/2015 |
| | | Copyright Policy | | 3/26/2014 | 9/22/2015 |
| | Community Guidelines | | | - | 2/17/2016 |

| | | | | | |
|---|---|---|---|---|---|
| **Sound Cloud** | Terms of Service | Terms of Service | Terms of Service | 3/12/2013 | 1/8/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 8/21/2014 | 1/8/2015 |
| | Cookies Policy | Cookies Policy | Cookies Policy | 7/17/2014 | 1/8/2015 |
| | Community Standards | Community Standards | Community Standards | - | 1/8/2015 |
| **Spotify** | Terms of Service | Terms of Service | Terms of Service | 3/5/2014 | 1/8/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 4/29/2014 | 1/8/2015 |
| | Copyright Policy | Copyright Policy | | 10/17/2012 | 1/8/2015 |
| **Trello** | Terms of Service | Terms of Service | Terms of Service | 5/13/2014 | 1/13/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 2/15/2014 | 1/13/2015 |
| TripAdvisor | Terms of Service | Terms of Service | Terms of Service | 4/28/2014 | 1/9/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 4/28/2014 | 1/9/2015 |
| **Tumblr** | Terms of Service | Terms of Service | Terms of Service | 1/27/2014 | 12/17/2014 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 1/27/2014 | 12/17/2014 |
| | Community Standards | Community Standards | Community Standards | 10/28/2014 | 12/17/2014 |
| **Twitch** | Terms of Service | Terms of Service | Terms of Service | 3/24/2014 | 1/15/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 10/13/2014 | 1/15/2015 |
| | | Sales Terms | Sales Terms | 8/6/2014 | 8/21/2015 |
| | Code of Conduct | Code of Conduct | Code of Conduct | 10/27/2014 | 1/15/2015 |
| | Cookies Policy | Cookies Policy | Cookies Policy | 9/12/2013 | 1/15/2015 |

| | | | | | |
|---|---|---|---|---|---|
| **Twitter:** | Terms of Service | Terms of Service | Terms of Service | 9/8/2014 | 12/18/2014 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 9/8/2014 | 12/18/2014 |
| | Use of Cookies and Similar Technologies | Use of Cookies and Similar Technologies | Use of Cookies and Similar Technologies | - | 12/18/2014 |
| | The Twitter Rules | The Twitter Rules | The Twitter Rules | - | 12/18/2014 |
| **Viber** | End-User License Agreement | End-User License Agreement | End-User License Agreement | - | 1/13/2015 |
| | DMCA Policy | DMCA Policy | DMCA Policy | - | 1/13/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 6/11/2014 | 1/13/2015 |
| | Public Chats Content Policy | Public Chats Content Policy | Public Chats Content Policy | - | 1/13/2015 |
| **Vimeo** | Terms of Service | Terms of Service | Terms of Service | 12/8/2014 | 1/12/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 12/8/2014 | 1/12/2015 |
| | Copyright and DMCA Policy | Copyright and DMCA Policy | Copyright and DMCA Policy | 08.2014 | 1/12/2015 |
| | Cookies Policy | Cookies Policy | Cookies Policy | 01.2013 | 1/12/2015 |
| | Community Standards | Community Standards | Community Standards | - | 1/12/2015 |

| | | | | | |
|---|---|---|---|---|---|
| **Wikipedia** | Terms of Service | Terms of Service | Terms of Service | 6/16/2014 | 3/3/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 4/25/2014 | 3/3/2015 |
| **Yahoo Mail** | Terms of Service | Terms of Service | Terms of Service | 3/16/2012 | 12/29/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 9/25/2014 | 12/29/2015 |
| | Yahoo Mail Terms and Guidelines | | | - | 12/29/2015 |
| | | Content Upload Additional Terms | | - | 12/29/2015 |
| | Universal Anti-Spam Policy | Universal Anti-Spam Policy | | - | 12/29/2015 |
| | POP Access and Forwarding Emails Terms of Service | | POP Access and Forwarding Emails Terms of Service | - | 12/29/2015 |
| | Premium Email Box Terms of Service | | | - | |
| | Communication Terms | | Communication Terms | - | 12/29/2015 |
| **Youtube** | Terms of Service | Terms of Service | Terms of Service | 6/9/2010 | 2/26/2015 |
| | Privacy Policy | Privacy Policy | Privacy Policy | 12/19/2014 | 2/19/2015 |
| | Community Standards | Community Standards | Community Standards | - | 2/26/2015 |

## ANNEX III - RECOMMENDATIONS ON TERMS OF SERVICE & HUMAN RIGHTS[67]

*Edited by Luca Belli, Primavera de Filippi and Nicolo Zingales*

### Introduction

The following recommendations aim at fostering online platforms' responsibility to respect human rights, in accordance with the UN Guiding Principles on Business and Human Rights, by providing guidance for "responsible" terms of service. For the purpose of these recommendations, the term "responsible" should be understood as respectful of internationally agreed human rights standards. Besides identifying minimum standards for the respect of human rights by platform operators (standards that "**shall**" be met), these recommendations suggest best practices (which are "**recommended**", or "**should**" be followed) for the most "responsible" adherence to human rights principles in the drafting of terms of service.

### Background

The digital environment is characterized by ubiquitous intermediation: most of the actions we take on the web are enabled, controlled or otherwise regulated through the operation of online platforms (see: definition n). Online platforms are essential instruments for individuals to educate themselves, communicate information, store and share data (see definition d). Increasingly, the operation of these platforms affects individuals' ability to develop their own personality and engage in a substantial amount of social interactions. The online world might thus challenge the system of human rights protection traditionally used in the offline world,

[67] These recommendations were developed by the Dynamic Coalition on Platform Responsibility (DCPR) of the United Nations' Internet Governance Forum and do not necessarily represent the views of the Center for Technology and Society at Fundação Getulio Vargas Rio de Janeiro Law School.

which relies predominantly on a public infrastructure. While private actors are traditionally not considered as duty-bearers in international human rights law, they are indirectly subject to international law through the laws of the countries in which they operate. However, since national laws do not always adequately implement internationally-agreed human rights, there is a need to define minimum standards and develop voluntary best practices at the international level to ensure protection of human rights by transnational corporations.

Respect of human rights undoubtedly represents an important factor in assessing the conduct of corporations from the perspective of a variety of stakeholders, including governments, investors and increasingly, consumers. This is especially relevant in the context of online platforms designed to serve the needs of a global community, and forced to satisfy different, often conflicting legal requirements across the various jurisdictions where they operate. In light of the key role that online platforms are playing in shaping a global information society and the significant impact they have on the exercise of the rights of Internet users (see definition k), an expectation exists that such entities behave "responsibly", thus refraining from the violation of internationally recognised human rights standards and offering effective remedies aimed at repairing the negative consequences that their activities may have on users' rights.[68]

The existence of a responsibility of private sector actors to respect human rights, which was affirmed in the UN Guiding Principles on Business and Human Rights[69] and unanimously endorsed by the UN Human Rights Council, is grounded upon the tripartite framework developed by the UN Special Rapporteur

[68] See Council of Europe, Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media.

[69] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, UN Human Rights Council Document A/HRC/17/31, 21 March 2011 ("Guiding Principles"), p. 1.

for Business and Human Rights, according to which States are the primary duty bearers in securing the protection of human rights, corporations have the responsibility to respect human rights, and both entities are joint duty holders in providing effective remedies against human rights violations.

As part of this responsibility, corporations should:

1. make a policy commitment to the respect of human rights
2. adopt a human rights due-diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights; and
3. have in place processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute.[70]

These recommendations focus on one of the most concrete and tangible means for online platforms to bring that responsibility to bear: the contractual agreement which Internet users are required to adhere to in order to utilise their services (usually called "Terms of Service", see definition s in). Specifically, the recommendations constitute an attempt to define "due diligence" standards for online platforms with regard to **three essential components: privacy, freedom of expression and due process**. In doing so, they aim to provide a benchmark for respect of human rights, both in the relation of a platform's own conduct as well as with regard to the scrutiny of governmental requests that they receive. As recently stressed by the Council of Europe's Commissioner for Human Rights,[71] guidance on these matters is particularly important due to the current lack of clear standards.

---

[70] Guiding Principles, Part II, B, para. 15.

[71] Council of Europe, "The Rule of Law on the Internet and in the Wider Digital World", footnotes 181-187 and corresponding text.

## I. Privacy & Data Protection (see definition q)

The first section of these recommendations provides guidance over the rules that online platform operators (see definition o) can adopt in order to guarantee that their users are not subject to unnecessary or unreasonable collection, use and disclosure of their personal data (see definition m).

### 1. Data Collection

Platform operators **should** limit the collection of personal information (see definition m) from Internet users to what is directly relevant and necessary to accomplish a specific, clearly defined and explicitly communicated purpose.[72] The platform's terms of service (ToS) **shall** also specify every type or category of information collected, rather than requiring a general-purpose consent (see definition c).[73] If consent is withdrawn, the platform

[72] See Principle I.3 of the OECD Privacy Principles ("The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."); Principle III of the APEC Privacy Framework which " limits collection of information by reference to the purposes for which it is collected. The collection of the information should be relevant to such purposes, and proportionality to the fulfilment of such purposes may be a factor in determining what is relevant"; and Principle 3 of the UN Data Protection Principles and Rights, according to which "The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that: (a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified; (b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified? (c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.

[73] See Principle III of the OECD Privacy Principles; and Principle 5 of the APEC Privacy Framework.

is no longer entitled to process such data for the related purpose. Although withdrawal is not retroactive, *i.e.* it cannot invalidate the data processing that took place in the period during which the data was collected and retained legitimately, it **shall** prevent any further processing of the individual's data by the controller and should imply deletion unless further use is permitted and regulated by a legitimate law (see definition l).[74]

Platform operators **shall** also refrain from collecting data by automatically scanning content (see definition b) privately shared by their users, in the absence of platform-users' consent. Admissible derogations to this principle include the need to fight against unsolicited communications (spam), maintain network security (e.g. preventing the diffusion of malware) or give force to court order or provisions defined by a legitimate law.

Platform operators **shall** always obtain user consent before tracking their behaviour (both within the platform and outside, *e.g.* through social plugins on third-party sites). Even after consent has been given, they **shall** always provide a way for users to opt-out at a later stage by the platform within other services. In order to facilitate user oversight on the application of these principles, platform operators **shall** allow their users to view, copy, modify and delete the personal information they have made available to the platform, both within its own services or by other services within the platform, and are encouraged to do so enabling download of a copy of their personal data (see definition m) in interoperable format.[75] Platform operators **shall** also allow their

[74] See Principle UN Data Protection Principle and Rights ("Everyone [...] has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees") and Art. 8e of the modernized version of Convention 108 ("Any person shall be entitled: [...] to obtain, upon request, as the case may be, rectification or erasure of such data"). See also Opinion 15/2011 of the Article 29 Working Party on the definition of consent, p. 9.

[75] See article 15 of the proposed EU data protection regulation.

users to view, modify and delete the personal information that platform operators have shared with third parties for marketing purposes.

### 2. Data Retention

Platform operators **should** clearly communicate in their terms of service whether and for how long they are storing any personal data. As a general rule, any retention beyond the period necessary to accomplish the purpose (not exceeding 180 days)[76] **should** be specifically foreseen by a "legitimate law".[77]

### 3. Data aggregation

As a best practice, aggregation of platform users' data **should** only be done subject to express consent (see definition g). Aggregation of data across multiple services or devices requires extra diligence from the part of the data controller (see definition e), since it might result in data being processed beyond the original purpose for which it was collected and the generation of new data, whose nature, volume and significance may nor be known or knowable by the platform user (see definition p). The purpose of the data aggregation and the nature of the new data resulting from the aggregation **should** be clearly stated, in order to allow the platform users to properly understand the scope of the given consent. Although this does not prevent the implementation of cross-

[76] Given the importance of data about past platform user behaviour for the provision of personalised search results, it appears unnecessary, as a matter of principle, to apply data retention periods exceeding those foreseen for search engines. Thus, the criterion of 180 days is based on the recognition by the Article 29 Working Party that search engines do not need, in principle, to store data for longer than 6 months- beyond which period, retention should be "comprehensively" justified on "strict necessity" grounds. See Art. 29 WP Opinion 1/2008 on data protection issues related to search engines, p. 19

[77] See definition p): "Legitimate Law".

device functionalities,[78] it is necessary to ensure that platform users understand the reason, scope and outputs of the data aggregation.

## 4. Data Use

Platforms **shall** obtain consent in order to use personal data (including platform users' contacts and recipients) for the legitimate purpose and duration as specified within the Terms of Service. Additional use of platform user's personal data does not require the platform user' consent when such use is necessary: (a) for compliance with a legal obligation to which the platform operator is subject; or (b) in order to protect the vital interests or the physical integrity of the platform user or of a third person; (c) for the performance of a task carried out in the public interest or in the exercise of official authority as specified by a legitimate law. (d) for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.[79] However, express consent **should** be required for making personal data available to the public. Platform users **should** have the possibility to redefine the extent to which their personal data are available to the public.

A broad and open-ended permission on the use of platform users' personal data for "future services"[80] can be in conflict with

---

[78] One example of such functionality is the recently added cross-device tracking feature of Google Analytics. See: <https://support.google.com/analytics/answer/3234673?hl=en>.

[79] See e.g. art 7, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[80] See e.g. Google's Terms of Services <http://www.google.com/intl/en/policies/terms> stating that "The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop *new* ones" (as of 15 January 2015).

the right of users to informational self-determination.[81] For this reason, it **is recommended** that platforms specify in their ToS that the processing of personal data is limited to the scope of existing services, or explicitly state that the data can be used for specified additional services. The enrolment of platform users into any new service shall require the acceptance of new ToS.

Platform operators shall also give users the possibility to demand the rectification of inaccurate data and to object to the use of their personal data on legitimate grounds, unless such use is mandated by a legitimate law.[82] Furthermore, platform users **shall** always be able to obtain information about any predictive or probabilistic techniques that have been used to profile them and the underlying rationale of such profiling.[83]

Lastly, platform operators **shall** always permit their users to delete their account in a permanent fashion.[84] Likewise, if there is no other legal reason justifying the further storage of the data, the data processor shall proceed with the permanent deletion of all or portions of the relevant data associated with the platform user's account,[85] in a time that is reasonable for its technical implementation. While anonymous data (see definition a) can be kept and processed without consent, pseudonymous data (see definition r) should not be subject to different treatment in that regard.

### 5. **Data protection** *vis-à-vis* **third parties**

Platform operators **shall** provide effective remedies against the violation of internationally recognised human rights. For this

[81] For the development of this principle, see the decision by the German Constitutional Court in the so called "census" decision. BVerfGe 65, 1. Available at: <http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm>.

[82] See Principle VII d) of the OECD Privacy Principles, Principle II of the UN Data Protection Principles & Rights, and art. 8 d) of Convention 108.

[83] See Convention 108, art. 8 c).

[84] This is a corollary of the right to one's own identity, which forms integral part of the right to privacy.

[85] See Opinion 15/2011 of the Article 29 Working Party on the definition of consent, p.33.

reason, they **should** establish clear mechanisms for platform users to gain access to all of their personal data held by a third party to whom their data have been transferred, as well as to be informed of the actual usage thereof.[86] Platform operators **should** also enable their users to report privacy-offending content and to submit takedown requests.[87] When such requests are submitted, a balance of the relevant rights and interests should be made and the outcome may depend on the nature and sensitivity of the privacy-offending content and on the interest of the public in having access to that particular information.[88] They **should** also implement a system to prevent the impersonation of platform users by third parties, although exceptions can be made with regard to public figures where pertinent to contribute to the public debate in a democratic society.[89]

A second set of concerns pertains to the possibility to preempt any interference with platform users' personal data, by preventing third parties' access to platform user's content and metadata. Firstly, platform operators **should** allow users

[86] See article 8 b) of Convention 108.

[87] See article 8 f) of Convention 108, and Part IV of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[88] See Article 29 WP Opinion (WP225/14) on the implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez", C-131/12. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf>.

[89] This is, once again, in respect of the individual's right to identity, see supra note 15. The exception for public interest purposes is intrinsic to the notion of right to informational self-determination. In part, it refers to the notion of "public figures" which was specified in Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the Right to Privacy; it is also specifically addressed through the relevant human rights jurisprudence (see e.g. Von Hannover v. Germany (no.2), 2012) and most recently, through the Art. 29 Working Party's Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González " C- 131/12.

to preserve their anonymity *vis-à-vis* third parties to the extent permitted by legitimate laws. Secondly, it is **recommended** that platforms enable end-to-end encryption of communications and other personal information, in the context of both storage and transmission.[90] In that respect, **best practice** is when the decryption key is retained by the platform user, except where the provider needs to hold the decryption key in order to provide the service and the platform user has provided informed consent.

As regards the handing over of platform users' data upon governmental request, platform operators **should** specify that they execute such request only in the presence of a valid form of legal process, and release a periodic transparency report providing, per each jurisdiction in which they operate, the amount and type of such requests, and the platforms' response (in aggregate numbers).[91]

## II. Due Process

Due process (see definition f) is a fundamental requirement for any legal system based on the rule of law. "Due" process refers to the non-derogability of certain procedures in situations which may adversely affect individuals within the legal system. These procedures are grounded upon essential principles such as the clarity and predictability of the substantive law, the right to an effective remedy against any human rights violations and the right to be heard before any potentially adverse decision is taken regarding oneself. In particular, while a law must be clear and accessible to the platform user, the latter principles translate into the need for an appeal system and the respect of the core minimum of the right to be heard, including: (1) a form of legal process which respects the guarantees of independence and impartiality; (2) the right to receive notice of the allegations and the basic

90 *Ibidem*.

91 See Guiding Principles, Part II, section B, para. 21. The Google transparency report is a role model in this field. Available at: <http://www.google.com/transparencyreport/>.

evidence in support, and comment upon them, to the extent that not doing so may prejudice the outcome of the dispute; and (3) the right to a reasoned decision.

Due process has significant implications with regards to potential amendment and termination of contractual agreements, as well as the adjudication of potential disputes.

## 1. Amendment and termination of contracts

Terms of Service **should** be written in plain language that is easy to understand. The platform operators should provide an accessible summary of the key provisions of the terms of service. The platform operators **should** give their users meaningful notice of any amendment of the ToS affecting the rights and obligation of the users. Meaningful notice **should** be provided in a way, format and timing that enable platform users to see, process and understand the changes without unreasonable effort. Contractual clauses that permit termination by platforms without clear and meaningful notice **shall** not be used.

In addition, platform operators **should** consider giving notice even of less significant changes, and enabling their users to access previous versions of the terms of service. Ideally, platforms operators **should** enable their users to continue using the platform without having to accept the new terms of service related to the additional functionalities. Additional functionalities should never be imposed to the user when it is possible to provide the original service without implementing the additional functionalities. The platform user should have the possibility to opt in in for new functionalities. Meaningful notice **should** also be given prior to termination of the contract or services. Besides, to reduce the imbalance between platform users and platforms owners when it comes to litigation, it is **recommendable** that the ToS be negotiated beforehand with consumer associations or other organisations representing Internet users. In order to prevent

wrongful decisions, it is **also recommended** that platforms make termination of accounts of particular platform users possible only upon repeated violation of ToS or on the basis of a court order.

### 2. Adjudication

Disputes can arise both between platform users and between a particular platform user and the platform operator. In both cases, platform operators **should** provide alternative dispute resolutions systems to allow for quicker and potentially more granular solutions than litigation for the settling of disputes. However, in view of the fundamental importance of the right of access to court, alternative dispute resolution systems **should** not be presented as a replacement of regular court proceedings, but only as an additional remedy. In particular, platform operators **should** not impose waiver of class action rights or other hindrances to the right of an effective access to justice, such as mandatory jurisdiction outside the place of residence of Internet users. Any dispute settlement mechanism **should** be clearly explained and offer the possibility of appealing against the final decision.

## III. Freedom of Expression

Freedom of expression (see definition h) is a fundamental right consisting of the freedom to hold opinions without interference and Freedom of expression may be subject to certain restrictions that shall be explicitly defined by a legitimate law. In the online platform context, the effectiveness of this right can be seriously undermined by disproportionate monitoring of online speech and repeated government blocking and takedown. The following section provides guidance as to how platforms should handle such matters through their terms of service.

- **Degree of monitoring**

Although there are no rules to determine, in general terms, what kind of speech should or should not be allowed in private online platforms, certain platforms **should** be seen more as "public spaces" to the extent that occupy an important role in the public sphere.[92] These actors have assumed functions in the production and distribution process of media services which, until recently, had been performed only (or mostly) by traditional media organisations.[93] As a matter of fact, online platforms increasingly play an essential role of *speech enablers* and pathfinders to information, becoming instrumental for media's outreach as well as for Internet users' access to them.[94]

As a general rule, any restriction on the kind of content permitted on a particular platform should be clearly stated and communicated within the ToS. In addition, platforms **should** provide effective mechanisms aimed at signalling and requesting the removal of content that is forbidden under the applicable legitimate laws (e.g. illegal content such as child pornography as well as other kinds of undesirable content, such as hate speech, spam or malware). However, such mechanisms shall be necessary and proportionate to their purpose.[95] It is of utmost importance that the rules and procedures imposing such restrictions are not formulated in a way that might affect potentially legitimate content, as they would otherwise constitute a basis for censorship. To this end, content restriction requests pertaining to unlawful content shall specify the legal basis for the assertion that

[92] In Sweden, for example, journalistic products such as newspapers, even if privately owned, abide by specially designed laws that grant them a special legal status because of their potential for free speech.

[93] See Council of Europe, Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media, para. 6.

[94] *Ibidem*.

[95] On that regard, the Johannesburg Principles on National Security, Freedom of Expression and Access to Information provide further guidance on how and when restrictions to freedom of expression may be exercised.

the content is unlawful; the Internet identifier and description of the allegedly unlawful content; and the procedure to be followed in order to challenge the removal of the content.[96]

Similarly, although platforms can legitimately remove content that is not allowed by their terms of service, either on their own motion or upon complaint, such terms of service **should** be clear and transparent in their definition of the content that will be restricted within the platform. However, when platforms offer services which have become essential for the enjoyment of fundamental rights in a given country, they should not restrict content beyond the limits defined by the legitimate law. Lastly, **platforms may** legitimately prohibit the use of the name, trademark or likeness of others, when such use would constitute an infringement of the rights of third parties. However, platforms operator **should** always provide clear mechanisms to notify those platform users whose content has been removed or prohibited and provide them with an opportunity to challenge and override illegitimate restrictions.

## 2. Government blocking and takedowns

Transparent procedures should be adopted for the handling and reporting of governmental requests for blocking and takedown in a way that is consistent with internationally recognised laws and standards.[97] Firstly, platform operators **should** execute such requests only when these are grounded on legitimate law. The content should be permanently removed only when such operation is justified by a judicial order, or the takedown request has not been appealed or countered in due course. Secondly, platforms operators **should** notify their users of such requests, ideally giving them an opportunity to reply and challenge their

[96] See Manila Principles on Intermediary Liability, 3.b. Available at: <https://www.manilaprinciples.org/>.

[97] See the Global Network Initiative Principles on Freedom of Expression and Privacy. Available at: <https://globalnetworkinitiative.org/principles/index.php>.

validity, unless specifically prohibited by a legitimate law. Finally, as already mentioned in the context of government requests for data, platform operators **should** adopt law enforcement guidelines and release periodic transparency reports.

## IV. Protection of Children and Young People

A special category of concerns arises in the case of children and young people, towards which platform operators **should** exercise a higher level of care. Platform operators **should** adopt particular arrangements, beyond warning for inappropriate content and age verification that can be imposed by legitimate law for certain types of content.

First, parental consent **should** be required for the processing of personal data of minors, in accordance with the applicable legislation. Secondly, although terms of service **should** generally be drafted in an intelligible fashion, those regulating platforms open to children and young people **should** consider including facilitated language or an educational video-clip and, ideally, a set of standardised badges[98] to make their basic rules comprehensible by all users regardless of their age and willingness to read the actual terms of use.[99] Secondly, **it is recommended** that platforms provide measures that can be taken by children and young people in order to protect themselves while using the platform,[100] such as utilising a "safer navigation" mode. Thirdly, platform operators **shall** offer specific mechanisms to report inappropriate content, and **should** providing a mechanism to ensure removal or

[98] See for instance, those provided by CommonTerms (see www.Commonterms.org) and Aza Raskin. Available at: <http://www.azarask.in/blog/post/privacy-icons/>.

[99] Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum, para. 90.

[100] Council of Europe Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum, para. 95.

erasure of content created by children and young people.[101]

As an element of media literacy, all platform users **should** be informed about their right to remove incorrect or excessive personal data.[102]

**Definitions**

**a) Anonymous data:**
Anonymous data means personal data processed in such a way that it can no longer be used to identify a natural person by using all the available means likely to be used" by either the controller or a third party.

**b) Content:**
Text, image, audio or video provided to particular platform user within the platform, even on a transient basis. This includes content produced and/or published by the platform operator, by another platform user or by a third party having a contractual relationship with the platform operator.

**c) Consent:**
Consent means any freely given, specific, and informed indication of the data subject's wishes by which s/he signifies her/his agreement to personal data relating to her/himself being processed.[103] To that end, every user shall be able to exercise a real choice with no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.

**d) Data:**
Content and/or personal information. Data can belong to both categories simultaneously.

---

101 See Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet. Decl-20.02.2008/2E.

102 See Council of Europe Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, para. II.8.

103 See EU Directive 95/46/EC, Article 2(h).

**e) Data controller:**

Data controller is the institution or body that determines the purposes and means of the processing of personal data.

**f) Due Process:**

Due process is a concept referring to procedural rights which are essential for the respect of the rule of law, comprising: (1) a form of legal process which respects the guarantees of independence and impartiality; (2) the right to receive notice of the allegations and the basic evidence in support, and comment upon them, to the extent that not doing so may prejudice the outcome of the dispute; and (3) the right to a reasoned decision.

**g) Express Consent:**

Express consent is a type of consent which (in contrast with "implicit" or "implied" consent) requires an affirmative step in addition to the acceptance of the general ToS, such as clicking or ticking a specific box or acceptance of the terms and conditions of a separate document.

**h) Freedom of Expression:**

The right to freedom of expression, enshrined in article 19 of the International Covenant on Civil and Political Rights consist of the freedom to hold opinions without interference and include freedom to seek, receive and impart information and ideas, regardless of frontiers. Freedom of expression may be subject to certain restrictions that shall be explicitly defined by a legitimate law. The right to freedom of opinion and expression is as much a fundamental right on its own accord as it is an "enabler" of other rights, including economic, social and cultural rights.[104]

---

[104] See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27.

**i) Function of the Platform:**
Function that the community has attributed to the platform on the basis of the legal, commercial and social expectations that it has generated. This should not be confused with a platform's functionalities, which constitute merely one (albeit important) element to identify the overall function(s).

**j) Hate Speech:**
Although there is no universally accepted definition of "hate speech", the term shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination on any grounds such as race, ethnicity, colour, sex, language, religion, political or other opinion, national or social origin, property, disability, birth, sexual orientation or other status.[105] In this sense, "hate speech" covers comments which are necessarily directed against a person or a particular group of persons.[106]

**k) Internet User:**
An individual who is using Internet access service, and in that capacity has the freedom to impart and receive information. The Internet user may be the subscriber, or any person to whom the subscriber has granted the right to use the Internet access service s/he receives.

**l) Legitimate Law:**
Laws and regulations are procedurally legitimate when they are enacted on the basis of a democratic process. In order to be regarded also as substantively legitimate, they must respond to a pressing social need and, having regard to their impact, they can be considered as proportional to the aim pursued.[107]

---

105 See e.g. Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms.

106 See Council of Europe, Committee of Ministers" Recommendation 97(20) on "hate speech".

107 In the case of restriction to freedom of expression, the legitimate purpose

(a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);
(b) It must pursue a legitimate purpose (principle of legitimacy);[108] and
(c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).

If it is manifest that the measure would not pass this three-pronged test, the platform operator should deny the request and, to the extent possible, challenge it before the relevant court.

**m) Personal Data & Personal Information:**

Personal data is any information about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, etc.[109] This is not intended to cover identification which can be accomplished via very

---

shall be one of those set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals. While no specific legitimate objectives have been identified by the Special Rapporteur to evaluate restrictions to privacy, the test devised in the Report is roughly equivalent, requiring that measures encroaching upon privacy be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others. See 2011 Report, para. 59. See Explanatory Report of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), para. 28.

108 See e.g. Council of Europe, Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum.

109 See the Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, according to which "a person is identifiable if, on the basis of any means likely reasonably to be used either by the data controller or by any other person, he or she can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

sophisticated methods.[110] This notion of personal data is sometimes also referred to as Personally Identifiable Information (PII), defined as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[111]

**n) Platform:**

For the purpose of these recommendations, platforms are understood as any applications allowing users to seek, impart and receive information or ideas according to the rules defined into a contractual agreement.

**o) Platform Operator:**

Natural or legal person defining and having the possibility to amend the platform's terms of service.

---

[110] See U.S. National Institute of Standards and Technology (NIST), NIST's Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Available at: <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>. See also the Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, according to which "a person is identifiable if, on the basis of any means likely reasonably to be used either by the data controller or by any other person, he or she can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

[111] In the case of restriction to freedom of expression, the legitimate purpose shall be one of those set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals. While no specific legitimate objectives have been identified by the Special Rapporteur to evaluate restrictions to privacy, the test devised in the Report is roughly equivalent, requiring that measures encroaching upon privacy be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others. See 2011 Report, para. 59.

**p) Platform User:**
Natural or legal person entering into a contractual relationship defined by the platform's terms of service.

**q) Privacy & Data Protection:**
Privacy is an inalienable human right enshrined in Article 12 of the Universal Declaration of Human Rights, which establishes the right of everyone to be protected against arbitrary interference with their privacy, family, home or correspondence, and against attacks upon his honour and reputation. In the context of online platforms, this encompasses the ability for data subjects to determine the extent to which and the purpose for which their personal data is used by data controllers, including the conditions upon which such data can be processed by the holder of data (the platform) and/or made available to third parties (right to informational self-determination).

**r) Pseudonymous Data:**
Pseudonymous data means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution.

**s) Terms of Service:**
The concept of "terms of service" utilised here covers not only the contractual document available under the traditional heading of "terms of service" or "terms of use", but also any other platform's policy document (*e.g.* privacy policy, community guidelines, *etc.*) that is linked or referred to therein.

**THE READER**

If, in a bookstore, you're told that a title published by Revan is exhausted, or Revan didn't consignment, or given any background similar to not having to sell the title sought, please communicate with us. The Revan systematically Reprints catalog titles and offers to bookstores. Phone, which we will be happy to serve you. Or buy directly on our website (see below).

**PUBLISHER REVAN**
Paulo de Frontin Avenue, 163
Rio de Janeiro – RJ – Brazil
CEP.: 20260-010
Tel: (21) 2502-7495

Our emails:
Administration: *administracao@revan.com.br*
Edition: *editorial@revan.com.br*
Graphic production: *grafica@revan.com.br*
Sales: *vendas@revan.com.br*
Disclosure: *divulg@revan.com.br*

Visit the Revan on the Internet:
*www.revan.com.br*
*www.facebook.com/editorarevan*