INTERNET POLICY REVIEW
Journal on internet regulation

Volume 5 | Issue 4

Private ordering and the rise of terms of service as cyber-regulation

Luca Belli
Center for Technology and Society, Fundação Getulio Vargas Law School, Rio de Janeiro, Brazil

Jamila Venturini
Fundação Getulio Vargas Law School, Rio de Janeiro, Brazil, jamila.venturini@fgv.br

Published on 28 Dec 2016 | DOI: 10.14763/2016.4.441

Abstract: Online communications and activities require the intermediation of numerous private entities that unilaterally define and implement their terms of service (ToS). The substantive provisions set in the ToS regulate the relationships between intermediaries and users with a binding force that may be even stronger than the one exercised by the law. Notably, we stress that internet intermediaries privately enforce their contractual regulation by shaping the architecture of the networks and platforms under their control. Such regulation and implementation do not need to rely on "traditional" public law-enforcement mechanisms and may apply in a transnational fashion. This paper argues that internet governance is witnessing the increasing centralisation of power in the hands of internet intermediaries defining private orderings. While acknowledging that ToS are an efficient and well-suited instrument to regulate the online world, we claim that ToS unilaterally impose rules, despite being presented as voluntarily accepted by the involved parties through the expression of free and informed consent. Based on empirical research, we highlight that ToS and their private implementation affect internet users' capability to enjoy their human rights, with particular regard to freedom of expression (and innovation), the right to privacy and to due process. Lastly, we put forward some recommendations on internet intermediaries' compliance with human rights standards.

Keywords: Terms of Service (TOS), Human rights

Article information

Received: 27 Apr 2016 **Reviewed:** 17 Jun 2016 **Published:** 28 Dec 2016
Licence: Creative Commons Attribution 3.0 Germany
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/private-ordering-and-rise-terms-service-cyber-regulation

Citation: Belli, L. & Venturini, J. (2016). Private ordering and the rise of terms of service as cyber-regulation. *Internet Policy Review*, *5*(4). https://doi.org/10.14763/2016.4.441

With the potential to democratise access to information, knowledge and culture in a way that was never seen before, the internet was at first hailed as the place where the "Governments of

the Industrial World" were "not welcome" and had "no sovereignty" (Barlow 1996). Twenty years after Barlow's Declaration of the Independence of Cyberspace, it has become evident that the internet is not immune to sovereignty claims. On the contrary, the increasing reliance on a variety of intermediaries makes the internet a hyper-regulated environment where both national legislation elaborated by "traditional" sovereigns and private ordering defined by a new wave of private sovereigns (Lessig, 1999; MacKinnon, 2012; Belli, 2016c) shape the internet experience of the regular user. Particularly, the revelations of former NSA contractor Edward Snowden seem to have called the public's attention on two considerations that have always been at the core of internet governance studies. First, the fact that all communications and activities taking place online require the intermediation of a number of private entities that unilaterally regulate a myriad of components of the internet (Goldsmith & Wu, 2006; DeNardis, 2014; Bygrave, 2015). Second, that such regulation has direct impact on internet users' capability to enjoy their human rights, with particular regard to freedom of expression, privacy and due process (Korpf, 2014; MacKinnon et al., 2014; Belli & De Filippi, 2016; Venturini et al., 2016).

Private intermediaries play a key role in ensuring the well-functioning of the internet, providing an ample range of services spanning from the very access to the internet to a variety of online platforms as well as mobile applications. Firstly, intermediaries' representatives are the strong majority of the individuals participating in the very standardisation of the internet architecture,[1] thus having direct influence on the possibility to incorporate (or not) human rights principles and considerations into the internet infrastructure. Secondly, internet intermediaries unilaterally define the contractual terms that will regulate users' behaviour within a given electronic network or online platform, exactly as the law of the land regulates individuals' behaviour within the national territory (Belli & De Filippi, 2012). Indeed, contractual agreements may be considered as a kind of private law-making system, because the substantive provisions set in the agreements – which may apply transnationally – regulate the relationships between the parties with a binding force that may be analogue to or even stronger than the one exercised by the law (Shapiro, 1993). Conspicuously, the success of private ordering in the online environment is due to the concrete possibility to enforce terms of service's (ToS) provisions independently from "traditional" public law enforcement mechanisms.

Indeed, internet intermediaries' contractual regulation can be directly implemented through technical means such as algorithms, within online platforms, or internet traffic management techniques, within electronic networks. Notably, algorithm govern how data flows are directed across the internet and play a pivotal role in controlling "money and information" (Pasquale, 2015), determining crucial aspects of our lives such as "how a billion plus people get where they're going" (Barocas, Hood, & Ziewitz, 2013). Such technical implementation is particularly effective within digital environments, for it directly shapes the architecture of a given cyberspace thus not needing to rely on public enforcement mechanisms to implement contractual provisions. On the contrary, it is increasingly common to observe the reliance of law enforcement agencies on intermediaries in order to implement legislation within a given territorial jurisdiction (OECD, 2011; Edwards, 2011; MacKinnon et al., 2014). The double purpose of this paper is to provide evidence to emphasise the ToS function as a fundamental tool of cyber-regulation and, based on such evidence, elaborate some basic recommendations on how to foster the compatibility of private ordering with core values of international human rights law.

Over the past centuries, private regulatory determinations and enforcement mechanisms have emerged in the absence of the state in a variety of contexts (Cafaggi, 2004; Zumbasen, 2007 and 2013). The internet is not exempt from such private-ordering tendency. On the contrary,

although the focus of internet governance scholars has traditionally concentrated on the internet technical architecture and on internet governance processes and institutions, it seems important to note that much of the internet evolution and use is unilaterally defined by the private sector through contractual agreements. As eloquently exposed by Nobel laureates Oliver Hart and Bengt Holmstrom, one of the primary functions of contracts is to fashion power relationships (The Economist, 2016). Notably, contractual terms aim at shaping the behaviours of the parties in order to precisely define the articulation of power, thus playing a pivotal role for the well-functioning of a given system and of the economy at large. In this sense, private orderings enshrined by network operators within internet access policies can define the ways in which users can access and share content and applications online, while private orderings enshrined within platforms ToS regulate the extent to which users will be able to enjoy privacy or freedom of expression within a given platform. Hence, it can be said that the contractual regulations established by private actors, as well as their technical implementations, *de facto* fashion the ways in which the internet can be accessed and used, while strengthening or limiting individuals' enjoyment of their fundamental rights and their capability to access and share innovation without asking for permission.

The first part of this paper argues that internet governance is witnessing the increasing centralisation of power in the hands of internet intermediaries defining private orderings. In this sense, we highlight that online private ordering relies on the key role of ToS and their technical implementation as fundamental regulation and implementation tools for governing the internet ecosystem. While acknowledging that ToS are an efficient and well-suited instrument to regulate the online world, we stress that ToS represent a tool of unilateral imposition of rules, despite being presented as voluntarily accepted by the involved parties through the expression of free and informed consent. In the second part of this paper, we explore the repercussions that ToS may have on a wide range of stakeholders. Based on empirical research on how network operators and online platforms[2] define and implement their ToS, we draw conclusions and put forward some recommendations for internet intermediaries on how to foster the compliance of their governance practices with human rights standards.

We highlight that private orderings, crafted and implemented by internet intermediaries, have direct impact on internet users' capability to fully enjoy their fundamental human rights, while the entities at the origin of such regulation enjoy a true position of "Internet points of control" (Zittrain, 2003; DeNardis, 2013). However, it is essential to keep in mind that internet intermediaries, as any private entity, have the corporate responsibility to respect human rights, as it has been clarified by a variety of soft-law documents, providing guidance on the implementation of human rights norms with regard to business entities (ISO, 2010; Ruggie Principles, 2011; CoE, 2014; IGF, 2015b)[3].

Such responsibility concretely means that intermediaries should explicitly commit to respect human rights and act with due diligence to identify and avoid potential negative impact that their ToS and practices may determine on individuals' human rights, eventually addressing adverse impacts through the provision of effective remedies. In this perspective, the concluding part of this paper will focus on the formulation of concrete suggestions, based on existing norms and driven by empirical research, with the aim to avoid that ToS deploy a negative impact on internet users' capability to enjoy their fundamental rights.

I. EFFICIENCY OR *ANCIEN RÉGIME* RELOADED?

Modern legal systems are grounded on the separation of powers, theorised by Montesquieu in the Spirit of Laws, according to which the authority of the state is split between legislative, executive and judicial powers, which mutually check and balance each other (De Secondat, 1748). Such separation avoids the concentration of power, which characterised the totalitarian state of the *Ancien Régime*, while aiming at safeguarding liberty in an effective fashion. Although the original doctrine of the separation of powers has lost much of its original rigidity, it remains a cornerstone of modern democracies based on which fundamental rights and liberties can be safeguarded effectively.

In many ways, the online environment subverts such separation, re-concentrating the aforementioned powers in the hands of private entities, in a model that has been compared to the feudalism by some authors (Narayanan, 2013; Schneier; 2013; Belli, 2016a). In such perspective, intermediaries acquire a quasi-sovereignty of the cyber-spaces under their control. First, intermediaries enjoy a quasi-legislative power, having the capability not only to unilaterally define the contractual clauses that regulate the provision and use of their services, but also - as evidenced below - to modify them at their own discretion.[4] This basically means that intermediaries' contractual regulation undertakes a quasi-legislative function (Belli & De Filippi, 2012; Korff, 2014; Belli, 2016c) by the ability to define the range of behaviours that are allowed within a given network, platform or service and, consequently, fashion users' capacity to exercise their fundamental rights online. Second, intermediaries enjoy a quasi-executive power, having the possibility to autonomously implement their self-defined regulations via technical means, such as algorithms, thus making sure that the service is structurally conceived to impose the respect of the contractual provisions.

Network operators may contractually foresee and technically implement the blocking or throttling of specific applications within their internet access contracts (BEREC, 2012) regardless of the fact that such provisions may hinder users' freedom of expression or harm competition. Likewise, application providers may unilaterally - and discretionary - foresee, within their ToS, the conditions for the collection, processing and sharing of users' and non-users' personal data (Van Alsenoy et al., 2015). Such discretionary data-use regulation may have particularly worrisome consequences in the case of US-based intermediaries applying the "business record doctrine", more frequently denominated "third party doctrine". Indeed, according to such doctrine, personal information does not enjoy privacy protection awarded by the Fourth Amendment, as long as it is knowingly revealed to a third party, such as an intermediary, since disclosure is considered as relinquishing control over information.[5] Third, intermediaries may enjoy a quasi-judicial power, for they may define alternative dispute resolution systems, autonomously deciding how to implement the contractual provisions regulating the interactions within the cyberspaces on which they can exert control. Particularly, intermediaries may mandatorily impose such alternative dispute resolutions to their users through the ToS (Venturini et al., 2016).

As noted by DeNardis, private entities have always played a crucial role in the design and administration of the internet, elaborating internet protocols and coordinating critical internet resources through private ordering (DeNardis, 2010). In this regard, it is important to stress the regulatory function of private intermediaries. The private ordering defined by internet intermediaries has indeed filled the institutional and regulatory gaps left by sovereign nation states, incapable to effectively regulate and control online flows of information. In this

perspective, private entities have been indubitably more successful than public actors, acquiring the capability of *de facto* regulating expression online by defining the architecture and contractual provisions according to which users can seek, impart and receive information and ideas – or, more appropriately, search, access and share content, applications and services. Notably, ToS are standard contracts enshrining unilaterally-drafted restrictions whose enforceability exclusively depends on the intermediary's actions. As prominently argued by Niva Elkin-Koren (1997), such unilateral definition and implementation of contractual rules may carry undesirable consequences. Indeed, freedom of contract assumes that users are informed and rational individuals, only entering into the transactions from which they will have a benefit, thus being the best guardians of their own interests.

The aforementioned conclusion, however, "holds true only in the absence of any market failure that would undermine the fundamental propositions on which the freedom of contract rests" (Elkin-Koren, 1997) such as the free formation of all contracting parties' will, the full information of all parties and the consequent inexistence of information asymmetries. To this end, the expression of consent to intermediaries ToS becomes a fundamental instrument allowing the intermediaries to deploy their private ordering, based on a contractual relation into which the individual is assumed to enter freely and after having been fully informed. Such contractual relation does not merely allow intermediaries to efficiently control their cyber-spaces, exercising quasi-legislative, quasi-executive and quasi-judicial powers. It may also give rise to a phenomenon of "governance by proxy" (Elkin-Koren & Haber, 2016), where state actors may establish public private partnerships with intermediaries to bypass constitutional limits regarding fundamental values such as privacy, freedom of expression and due process, as eloquently argued by former NSA contractor Edward Snowden.

It is important to note, however, that being subject to fewer procedural safeguards, private institutions can operate more efficiently than governments. This was the premise under which the Clinton administration established a Framework for Global Electronic Commerce, in the 1990s, promoting contractually based self-regulatory regimes.[6] Nonetheless, it must also be noted that the goal of commercial regulation - embedded in private orderings - is economic efficiency. As such, it seems important to question the extent to which such commercial regulations may be able to protect users' fundamental rights and the public interest in the absence of public scrutiny.

A multistakeholder approach including public oversight seems therefore essential to evaluate the range of externalities that private regulations may produce on other components of the internet ecosystem (Belli, 2016c), rather than delegating the elaboration of regulation to private entities whose natural behaviour is maximisation of their private interest rather than the promotion of public welfare. In such perspective, we argue in the next section that network operators may be keen to regulate internet traffic management in a way that privileges their interests – for instance blocking competing services and prioritising their commercial partners – rather than promoting users' freedom to impart and receive information. Likewise, online platforms may be tempted to censor to avoid liability or to maximise data collection and processing rather than minimise it to fair and specific purposes.[7]

II. PRIVATE ORDERING LAYERS

It is no secret that the development and evolution of the internet is influenced by the decisions and actions taken by a multiplicity of different stakeholders. In this context, intermediaries are

at the origin of the private orderings that regulate some essential components of the internet, be it at the infrastructure, application or content layers. The private ordering spectrum goes from rules independently defined and implemented by private entities to rules that are defined in accordance with national legislation and subsequently implemented by intermediaries. Contractual agreements and their subsequent implementation are the legal mortar and bricks for much of the internet environment (Bygrave, 2011), going from the organisation of the internet's DNS to the provision of internet access and online services. As such, operators' capability to contractually regulate internet access through their electronic networks – for instance defining what content or applications can be blocked, throttled, prioritised or sponsored (Belli & De Filippi, 2016) – is consecrated by the operators' definition and implementation of their internet access policies. These contractual agreements must be in accordance with net neutrality regulation and legislation, as long as such norms exist (Marco Civil, 2014; FCC, 2015; EU, 2015). Likewise, platform providers may have ample contractual autonomy to define, for instance, what kind of information can be accessed or shared by users or how their personal data are collected and processed within their ToS.

The regulatory function of the ToS, is limited by the existence of laws and regulation striking a balance between the protection of users' rights and the contractual autonomy of the intermediaries. In the absence of comprehensive fundamental rights protection and consumer protections, private actors providing any kind of internet service may contractually regulate such service in the most economically efficient way, which may not be the most user-interest-oriented.[8] Indeed, this latter approach includes the utilisation of jurisdiction clauses as well as class-action-waiver clauses that can obviously help saving the costs of entering into legal disputes around the globe but can also severely diminish the protection of users' rights. It is evident, from the analysis of the Terms of Service of 50 online platforms, conducted by the Center for Technology and Society at FGV Law School (CTS/FGV) and presented in Subsection (b), that avoiding liability is a key factor taken into account in the ToS provisions regarding due process and freedom of expression. Despite the legitimate interest of internet companies to regulate their businesses, the results of the aforementioned analysis show an imbalance of power between companies and users' rights, demonstrating that the most efficient choices may frequently neglect the full protection of users' rights.

INTERNET TRAFFIC REGULATION

In order to access the internet, users – be they individuals or Content and application providers (CAPs) – enter into contracts with Internet access providers (IAPs), defining the terms according to which the service will be provided. Internet access agreements may offer performance-specific plans to users, thus allowing operators to diversify their offerings, applying differentiated pricing, while letting the user choose the most appropriate subscription. Access contracts usually define elements such as quality levels with regard to specific performance indicators and may include conditions describing the provision of IP services, known as specialised services, such as IPTV, or sponsored applications commonly referred as zero rated services, (Belli, 2016b) to be bundled with internet access. However, internet access ToS may include provisions that limit end-users capability to enjoy their fundamental human rights while maximising IAPs capability to manage internet traffic (BEREC, 2012; Belli & van Bergen, 2013; Belli & De Filippi, 2016). These contractual limitations are defined in so called "fair use policies" that, in the absence of net neutrality regulation, may allow operators to have ample discretion with regard to the criteria according to which content and applications can be blocked, throttled, prioritised or sponsored.

Indeed, fair use policies may include an ample range of restrictions implemented through traffic

management practices. Due to their contractual autonomy, internet access providers enjoy a level of discretion with regard to access restrictions that is inversely proportional to the limits set by national net neutrality frameworks. Both contractual and technical restrictions are usually considered admissible as long as they are necessary and proportionate to the achievement of a legitimate aim.[9] On the other hand, discriminatory traffic management – be it foreseen by the internet access ToS or not – is considered as unreasonable when it is used for anticompetitive purposes or when it can jeopardise end-users' fundamental rights such as freedom of expression or privacy.[10] Without entering in the details of the net neutrality debate, it is important to stress that the blocking of legitimate content or applications as well as the degradation of competing services are consensually considered as anti-competitive behaviour that may also limit the full enjoyment of end-users fundamental rights (FCC, 2015; IGF, 2015; CoE, 2016). It is important to note that in the absence of net neutrality policies, contractual provisions allowing for discriminatory traffic management may be surprisingly widespread even in competitive markets, thus exercising a restrictive regulatory function. As an instance, a study led by the Body of European regulators of Electronic Communications in 2012, clearly demonstrated that blocking and throttling of P2P traffic was remarkably frequent in internet access contracts throughout the European Union.[11]

In spite of their reasonably competitive environments, in countries such as France, the UK, Italy or Germany, contractual restrictions within mobile networks were quite widespread until early 2013 (BEREC, 2012; VON Europe, 2014). In this sense, the European Telecommunications Network Operators' Association (ETNO) explicitly considered contractual restrictions on peer-to-peer (P2P) or Voice over IP (VoIP) application as "appropriate [a]s long as the relevant transparency obligations are met and the market provides end-users with a variety of offers providing access to Internet content and applications of their choice, this [limitation] is also appropriate".[12] However, in the absence of legislation or regulation limiting operators' leeway to contractually discriminate specific types of internet traffic, it seems likely that vertically integrated operators can have an incentive to disfavour competing CAPs, thus limiting users' rights and freedom to choose (FCC, 2015; Belli & De Filippi 2016).

Furthermore, internet access contracts usually establish the operator's right to filter internet traffic using a variety of – usually vaguely defined – techniques, including Deep packet inspection (DPI), for purposes ranging from network security and stability to compliance with domestic legislation and other supposedly "reasonable" purposes. In this regard, for instance, the Vodafone Group provides information regarding the "principles, policies and processes" that it follows to implement "network censorship, content blocking and the restriction of services" as well as to comply with "intercept and communications data demands" in the various countries where it operates in order to "assist [nation authorities] with their law enforcement and intelligence-gathering activities".[13] However, it should be noted that filtering techniques – notably, the widely deployed DPI – are also frequently used for traffic shaping purposes, inspecting the content of packets travelling over an IP network to identify what application or protocol is in use and subsequently apply a differentiated treatment. It must be reiterated that, in the absence of proper net neutrality policies, operators have ample discretion regarding the definition and the technical implementation of contractual restrictions, as well as the exclusion of effective remedies aimed at challenging such contractual restrictions. As an instance, it seems sufficient to consider that the use of DPI to identify, block or throttle perfectly legal applications, such as Skype or BitTorrent was considered as a "reasonable" restriction by a wide number of operators until the beginning of 2013 (Renals & Jacoby, 2009; BEREC, 2012).

Despite the emerging consensus on the nullity and voidness of contractual clauses that

contradict human rights law (CoE, 2014; Korff, 2014), it seems important to stress that undue restrictions, targeting legal applications and services have been allowed by internet access contracts, as long as net neutrality regulations were absent. At the same time, in countries where such regulation is still missing, operators retain the power to autonomously establish the private ordering of their own networks, which may lead to massive restriction of perfectly legal applications, as it has been recently documented in South Korea (Nam, 2016). Therefore, it is also important to note that operators' ToS-defined and technically implemented private ordering may jeopardise internet users' rights, particularly when IAPs are vertically integrated with CAPs and enjoy significant market power. In such perspective, although operators' ToS may be an effective way of regulating internet traffic management, the total delegation of such regulatory power to private entities has the potential to limit users' capability to fully enjoy their fundamental rights.

PLATFORM REGULATION

The use of standard contracts for the regulation of online services goes back to the origin of internet itself and their popularity is largely due to the fact that they are not only easy to edit and share (Bygrave, 2015) and they also represent a very effective regulatory tool. However, in spite of their effectiveness, standard contracts are almost never read (Obar & Oeldorf-Hirsch, 2016) and, if they are, they are considered hard to understand (Bakos, Marotta-Wurgler, & Trossen, 2013) due to their length, density, fine-print format and legal jargon. This scenario is even more troublesome in the online environment, either because these contracts "offer fine print in an environment where colourful images dominate over text" (Kim, 2012) or because the amount of time necessary to merely read ToS is increasingly overwhelming.[14]

The development of technical solutions for the report of abusive content by users in online platforms, for instance, responds to the advance of content takedown policies in the past years and allows some sort of "editorial" control[15] by the platform. The opposite is also true: the lack of technical implementation in some cases prevent the development of alternative solutions, particularly, regarding meaningful notice for users about the processing of their personal data.

In the case of online platforms, ToS can often establish rules for the publication and sharing of user-generated content and the modalities of collection and processing of personal data. Hence, such contractual agreements can have concrete impacts on users' ability to exercise their human rights online (CoE, 2014). An analysis of the ToS of 50 platforms, conducted by CTS/FGV,[16] assessed the degree to which such documents may be deemed as respectful of the human rights to freedom of expression, privacy, and due process[17] by implementing an analysis methodology derived from international human rights standards. The project methodology was based on the fundamental rights enshrined in international human rights documents: which have been decomposed in various elements that could fit into yes-or-no questions. The methodology was refined and three independent analysts applied the human-rights-based questions to assess the ToS of 50 online platforms. The preliminary research results were discussed in several national and international events to stimulate feedback from various stakeholders and, finally, the data generated by three analyses have been crossed utilising a conflict resolution methodology and applying statistical treatment to evaluate the level of agreement for each question.

An initial difficulty identified in the analysis was to determine which contractual agreement may be considered as effectively binding the users[18] due to (i) the amount of documents to which the main policies make reference to or (ii) the fact that not all of the binding documents are shown in a prominent way to the user, when the account is created. The study identified an average of three binding documents per platform, which may be complemented by a series of auxiliary

pages, providing explanatory videos and frequently asked questions (FAQ), amongst other informative materials.[19] These documents can detail, complement or even contradict the main ToS (Jeong, 2016), leaving users in a situation of juridical uncertainty, as regards their rights and responsibilities.

The CTS/FGV study has notably revealed that the analysed platforms offer limited guarantees with regard to the protection of freedom of expression, lacking clear and specific information about which content is allowed or not and avoiding any commitments to provide justification, notification or guarantee of the right to be heard, in case of content removal[20] (Venturini et al., 2016). In this regard, it is interesting to note that 26 of the analysed ToS foresee that if user-generated content is removed, the affected user may not receive any notification or have the opportunity to challenge the removal. Other 18 ToS, do not present any guarantee of notification and the right to be heard in case of content removal, evidencing the lack of clear commitment to notification in 44 (or 88%) of the analysed platforms.[21]

Even more troublesome is the fact that 44 (88%) of the examined ToS explicitly foresee that platform providers may terminate a specific user account without previous notice or the possibility to challenge the decision.[22] Moreover, none of the analysed platforms commit to notifying users before proceeding with the termination of their account. Unsurprisingly, more attention seems to be given to offering mechanisms to report abusive content. Indeed, the need to mitigate risks of facing legal action related to defamation or the copyright violation may be the reason for this apparent imbalance between the protection of freedom of expression and the rights of potential victims of supposedly abusive behaviour. The intention to avoid risk of liability for copyright violation or defamation may also explain the platforms' focus on efficient and expeditious removal mechanisms and the absence of procedure to challenge inappropriate removals.

The regulatory effects deployed by ToS are also particularly evident as regards users' possibility to be anonymous as well as their privacy protections. Contrary to the recommendations of the UN Special Rapporteur on Freedom of Opinion and Expression,[23] 16 (32%) of the analysed platforms do not allow anonymity or the use of pseudonyms by users in their policies, while other 16 do not include provisions on this matter. With regards to the right to privacy,[24] it should be stressed that online platforms' policies are generally detailed, which is not surprising considering that the "privacy self-management model" traditionally adopted by many data protection frameworks (Solove, 2013) is based on the expression of informed consent, thus making - at least apparently - detailed information essential to characterise the consent as informed. Indeed, the acceptance of privacy policies usually signifies the user agreement to the processing of his personal data, which is usually essential for the platform provider's business model. For this reason, ToS language regarding privacy and data protection is usually broad enough to ensure that platform providers are allowed to use users' data in new ways without having to update the contractual agreement or require a new consent. Even though this may be a practical and economic solution for platforms, as well as an effective regulatory tool, it seems patent that the protection of users' human rights is not the uppermost concern of the private regulator.

A further element that has been highlighted by the CTS/FGV study is the extra-platform reach of the platforms' private ordering. Indeed, while 33 (66%) of the analysed ToS explicitly state that users will be tracked in other websites and 40 (80%) explicit that they may allow third parties to monitor users' activities when using third parties' services,[25] only in few cases users have the concrete choice not to be tracked (i.e. via opt-out). As a consequence, effective personal data

management by users is significantly curtailed. It is important to notice that, in general, the analysed ToS do not specify which activities can be monitored by the platform or by third parties, nor who are the third parties, while letting unclear if monitoring only happens when users are logged in to the platform. Such a situation makes it particularly challenging, if not impossible, for the users to understand the actual reach of the platform regulation and the concrete impact that ToS have on their rights, thus transforming the expression of the informed consent into an evident juridical fiction.

Lastly, the analysis of the ToS compliance with the right to due process[26] reveals the widespread presence of unclear provisions regarding platforms' restrictions of users' access to justice. Notably, 13 (26%) of the analysed ToS foresee that users waive their right to initiate class actions; 17 (34%) impose arbitration as the only method for dispute resolution; and 43 (86%) establish a particular jurisdiction for dispute resolution (generally the Californian one) which may create an excessive burden for individuals to exercise their right to access to justice. Moreover, users are not always informed about ToS modifications and can hardly access the version of the contract that they originally accepted. Indeed, only 15 (30%) platforms explicitly commit to notifying users about changes in their contracts, while 28 (56%) have contradictory clauses on this. In many cases ToS foresee the need to notify only if the changes are considered as "significant" by the platform, while 6 platforms state that there will be no notification in the event of contractual changes regardless of their relevance.

In the light of the aforementioned considerations, it seems clear that ToS are a very pervasive regulatory tool, allowing platform providers to regulate not only their users' behaviour within the platform but, frequently, the users' possibility to enjoy their fundamental rights when browsing the internet without having accessed the platform.

III. CONCLUSION

The analysis of the ToS regulatory function at the network as well as the platform level shows that these contractual agreements have the potential to concretely affect internet users' human rights. However, it must be noted that international bodies have already attempted to develop parameters providing both procedural (ISO 26000) as well as substantial guidance (IGF, 2015a; IGF, 2015b) that may be followed by private intermediaries in drafting ToS so that users' rights and interests are both considered and incorporated into the final result. Furthermore, domestic legislation and overview mechanisms - especially on consumer protection, net neutrality and data protection - should be designed to guarantee the respect of human rights principles, involving a variety of stakeholders, such as users, NGOs and academic institutions in monitoring and reporting potential abusive contractual behaviours at both network and platform level.

One of the main challenges seems to be how to enforce shared norms in a transnational environment. While international human rights standards offer general principles that should be observed in terms of freedom of expression, privacy (including data protection) and due process, usually they lack procedural orientations on how to implement such principles when national legislations are lacking. International standards like ISO 26000 could be useful in this sense. In fact, besides specific rules and procedures, ISO 26000 offers guidance for businesses on how to involve affected stakeholders in the policy elaboration as well as on how to implement social responsibility, including through transparency, accountability and human rights obligations. According to the description offered by ISO itself, the norm "helps clarify what social responsibility is" and allows "businesses and organizations [to] translate principles into

effective actions and shares best practices relating to social responsibility, globally". ISO 26000 itself was the result of a long process of consultation with an ample spectrum of stakeholders and can be applied to different types of organisations, including internet companies regardless of their size or location.

Lastly, the above analyses have also pointed out that some specific measures could be implemented by internet companies in order to strengthen their corporate social responsibility. First, intermediaries should explicitly declare their commitment to the full respect of users' fundamental rights. Second, intermediaries should undertake a due diligence process, aimed at assessing the impact that their ToS as well as their algorithmic implementation may have on users' rights. Third, they should state in a clear and transparent fashion what kind of restrictions they intend to apply in their networks or platforms, so that all stakeholders may have a concrete possibility to assess whether such restrictions are in full compliance with existing human rights standard and eventually challenge any undue restrictions. Fourth, national regulators should have the right to review, at any time, the ToS as well as any technical means utilised to implement them in order to assess the conformity of the intermediaries' private orderings to the national law and international human rights standards. Lastly, intermediaries should play an active role in the promotion of due process, notifying users if any ToS changes occur, particularly when such changes affect users' rights and obligations, facilitating access to justice and complementing access to traditional court systems with alternative dispute resolution mechanisms.

To conclude, it is important to highlight that, although private intermediaries have a responsibility to respect human rights, public actors have a duty to actively protect such rights. Concretely, this duty entails a positive obligation on states to "ensure human rights [and protect] individuals against acts committed by private persons or entities, which includes" (UN HRC, 2004) this exercising appropriate oversight of private companies. Ultimately a multistakeholder approach would be beneficial in order to let private actors the freedom to autonomously enshrine human rights protections within their private orderings, while regulators and courts should be the ultimate guardians of individuals' interests, making sure that users rights prevail over the general terms and conditions.

REFERENCES

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. Retrieved from http://ssrn.com/abstract=1443256.

Barocas, S., Hood, S. and Ziewitz, M. (29 March 2013). Governing Algorithms: A Provocation Piece. http://dx.doi.org/10.2139/ssrn.2245322

Belli, L. (28 October 2016a). Collaborative Policymaking: from Technical to Legal Interoperability. Presented at the XIX International Congress of Constitutional Law. Brasilia. Panel 7. https://www.youtube.com/watch?v=KyQ5f--Yw44&t=236s

Belli, L. (October 2016b). Net neutrality, zero rating and the Minitelisation of the internet. Journal of Cyber Policy. Routledge. http://dx.doi.org/10.1080/23738871.2016.1238954

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

Belli, L. (2015). A heterostakeholder cooperation for sustainable internet policymaking. Internet Policy Review, 4(2). DOI: 10.14763/2015.2.364

Belli, L. and De Filippi, P. (2012). Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation, in European Journal of Law and Technology, Vol. 3, n°2.

Belli, L. and De Filippi, P. (Eds.) (2016) Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet. Springer.

BEREC. (2012). A view of traffic management and other practices resulting in restrictions to the open Internet in Europe. BoR (12) 30. https://ec.europa.eu/digital-agenda/sites/digitalagenda/files/Traffi c%20Management%20Investigation%20BEREC_2.pdf

Bygrave, L. A. Contract versus statute in Internet governance. In Ian Brown (ed.) (2012) Research Handbook on Governance of the Internet. Cheltenham: Edward Elgar.

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

Cafaggi F. (2004). Le rôle des acteurs privés dans les processus de régulation : participation, autorégulation et régulation privée. Revue Française d'Administration Publique 2004/1 (no109)

Clinton B. and Gore, A. (1st July 1997). *A Framework for Global Electronic Commerce*. Retrieved from http://www.w3.org/TR/NOTE-framework-970706

CoE. (January 2016). Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality.

CoE (April 2014). Recommendation CM/Rec (2014)6 of the Committee of Ministers to member states on a guide to human rights for Internet users.

DeNardis, L. (September 17, 2010). The Emerging Field of Internet Governance. Yale Information Society Project Working Paper Series. Available at https://ssrn.com/abstract=1678343

DeNardis, L. (August 2013). Internet Points of Control as Global Governance. CIGI Internet Governance Papers n° 2. Available at https://www.cigionline.org/sites/default/files/no2_3.pdf

DeNardis, L. (2014). The Global War for Internet Governance. Yale University Press.

Elkin-Koren, (1997). Copyright Policy and the Limits of Freedom of Contract, 12 Berkeley Tech. L.J. 93. Available at http://scholarship.law.berkeley.edu/btlj/vol12/iss1/4

Elkin-Koren, N. and Haber, E. (2016). Governance by Proxy: Cyber Challenges to Civil Liberties (February 28, 2016). 82 Brooklyn Law Review. Available at https://ssrn.com/abstract=2765447

ETNO. (October 2012). ETNO response to the Commission Public Consultation on specific aspects of transparency, traffic management and switching in an open Internet. https://www.etno.eu/datas/positions-papers/2012/rd385-cma-open-internet.pdf.

EU Regulation (EU) 2015/2120 laying down measures concerning open internet access. http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015R2120

FCC. (2015). Report and Order on Remand, Declaratory Ruling, and Order on the Matter of Protecting and Promoting the Open Internet . GN Docket No. 14-28

IGF (2015a). Policy Statement on Network Neutrality. Presented at the 10th United Nations Internet Governance Forum. http://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/833-dcnn-2015-output-document/file

IGF (2015b). Recommendations on Terms of Service and Human Rights. Presented at the 10th United Nations Internet Governance Forum. http://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/830-dcpr-2015-output-document-1/file

Nam, H. (December 2015). Killing Network Neutrality – Massive Blocking P2P Traffic by KT Corporation. Retrieved from http://opennetkorea.org/en/wp/1529

Goldsmith, J. and Wu, T. (2006) Who Controls the Internet? Illusions of a Borderless World. Oxford University Press.

ISO (2010) ISO 26000:2010. Guidance on social responsibility.

Korff, D. (December 2014). The rule of law on the Internet and in the wider digital world. Issue paper published by the Council of Europe Commissioner for Human Rights Council.

Marco Civil. (2014). Lei N° 12.965, de 23 de abril de 2014, also known as Marco Civil da Internet no Brasil. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

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

Narayanan A., *Digital feudalism is upon us. How do we respond?*, Stanford Law School, 22 janvier, 2013, disponible sur http://cyberlaw.stanford.edu/events/digital-feudalism-upon-us-how-do-we-respond

Obar J. A. and Oeldorf-Hirsch A. (July 2016). The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. Retrieved from http://ssrn.com/abstract=2757465

Pasquale, F. (2015). The Black Box Society. The Secret Algorithms That Control Money and Information. Harvard University Press. Cambridge, Mass.

Schneier B., "Power in the Age of the Feudal Internet", in MIND, *Co:llaboratory discussion paper #6 Internet & Security*, 2013.

Shapiro, M. The Globalization of Law. Indiana Journal of Global Legal Studies, vol. 1, no 1, 1993.

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

UN Human Rights Committee. (2004). General Comment 31/2004. Nature of the General Legal Obligation on States Parties to the Covenant. CCPR/C/21/Rev.1/Add.13. http://www.unhcr.org/4963237716.pdf

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

Venturini, J. et al. (2016). Terms of service and human rights: an analysis of online platform contracts. Editora Revan. Rio de Janeiro, Brazil.

VON Europe. (April 2014) Comments on the BEREC's Consultation on the Draft Report on Monitoring Quality of Internet Access Services in the Context of Net Neutrality by the Voice on the Net Coalition Europe.

Weller, D. and B. Woodcock. (2013). "Internet Traffic Exchange: Market Developments and Policy Challenges", OECD Digital Economy Papers, No. 207, OECD Publishing. dot:10.1787/5k918gpt130q-en

Zumbansen, P. (2007). "The Law of Society: Governance Through Contract," Indiana Journal of Global Legal Studies : Vol. 14: I, Article 2. http://www.repository.law.indiana.edu/ijgls/vol14/iss2/2

Zumbansen, P. (2013). Transnational Private Regulatory Governance Ambiguities of Public Authority and Private Power. Law and Contemporary Problems, vol. 76:1

FOOTNOTES

1. The analysis of a random meeting of the Internet Engineering Task Force (IETF), which is the most relevant Internet standardisation body, reveals that that "80.8% of participants were affiliated to private sector entities; 6.4% affiliated to the academic community; 12.4 did not provide affiliation; and less than 1% declared to be affiliated to a (sic) (inter)governmental entities." (Belli, 2015) This seems to be a fundamental element to consider when assessing the "*demos*" that de facto composes the standardisation bodies shaping the Internet architecture (Belli 2016a and 2016c).

2. With particular regard to online platforms, section II.b will discuss the findings of the Terms of Service and Human Rights project, developed by CTS/FGV in partnership with the Council of Europe. The project aimed at analysing the compatibility of the ToS of 50 online platforms with human rights standards on freedom of expression, privacy, and due process. The initial phase of project defined a ToS analysis methodology, based on the fundamental rights enshrined in international human rights documents. Subsequently three independent analysts applied the methodology to examine the ToS of 50 online platforms and the three sets of results were crossed using statistical treatment. The evidence obtained have been used to elaborate conclusions and recommendations. See Venturini et al., 2016.

3. Although soft-law international norms may be criticised for their non-binding nature that situates them "in the twilight between law and politics" (Thürer, 2000), it is important to stress that such norms may turn out to be more effective than the development of "hard law" in order to achieve a specific goal. First, soft law documents can be developed through less formal and more open processes, concretely allowing a variety of stakeholders to provide their inputs and subsequently accept and support the outcome. Second, due to the lack of international institutions able to enforce supposedly "hard" agreements, in the majority of fields, observers agree that "most international law is 'soft' in distinctive ways" especially as compared to most domestic law. Third, soft law documents have the merit of providing a common understanding of a given issue and can be easily utilised – by both public and private actors – as a shared conceptual basis to elaborate hard law documents that, being based on shared principles, will foster legal interoperability (Belli, 2016c).

4. Projects like Terminos y Condiciones provide useful insight on the ToS changes of a variety of intermediaries. See Términos y Condiciones, visited on 31 October 2016.

5. According to *Smith v Maryland*, 442 U.S. 735 (1979) and *United States v Miller*, 425 U.S. 435 (1976): "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

6. The Framework for Global Electronic Commerce is also renown for having led to the creation of the Internet Corporation for Assigned Names and Numbers that is, itself, at the top of a private ordering system in the internet logical layer, regulating the Internet Domain Name System through a chain of contractual agreements. (Clinton & Gore, 1997; Belli, 2016c).

7. Data minimisation is a fundamental data protection principle, grounded on the principles of purpose limitation and data quality. At the European level, these latter principles have constitutional value, granted by article 8 of the EU Charter of Fundamental Rights, according to which personal data 'must be processed fairly for specific purposes.'

8. Concerns with unbalance between intermediaries' interest and users' interest within standard contracts are not an exclusivity of the online environment. The possibility for business actors to unilaterally define standard contracts is considered to incentivise such actors to commit to no more than the minimum required by law, defining "antisocial" standards (Bygrave 2015, p. 31), that may be frequently biased against users (Bakos, Marotta-Wurgler, & Trossen, 2013). This is primarily due to the information asymmetry and bargaining power imbalance that characterise the relationship between customers and business actors, which is considered as a solid justification for the development of regulations to protect consumer rights in several jurisdictions.

9. This conclusion has been reached by a variety of stakeholders in different policy and regulatory contexts. See, for instance, Marco Civil, 2014; FCC, 2015; EU, 2015; IGF, 2015.

10. Ibid.

11. As the study reported, "at least 36 % of mobile internet access users [were] affected by P2P-related restrictions" while, on fixed networks, "at least 21 % of internet access users [were] affected by P2P-related restrictions." See BEREC (2012).

12. See ETNO (2012).

13. Vodafone Group Plc. (2015). Law Enforcement Disclosure Report., accessed on 30 October 2016.

14. Studies have shown that users would have to spend eight hours a day for 76 days only to read the Privacy Policies of an average of 1.462 webpages visited in one year (McDonald & Cranor, 2008).

15. This control is not similar to the one exercised by traditional media agents in the sense that content shared by third parties in these platforms is not subject to review by the service provider, meaning that the responsibility over the content is on the author and not on the platform. However, once content guidelines are incorporated in the ToS, there is an ex-post control exercised by their enforcement through notice and takedown mechanisms.

16. The "Terms of Service and Human Rights" project was developed as a partnership between CTS/FGV and the Council of Europe Department on Information Society. The methodology of the project is grounded on various human rights standards, most notably the Guide to Human Rights for Internet Users of the Council of Europe.

17. The project "Terms of Service and Human Rights" was developed between September 2014 and March 2016 and its goals were to (i) prompt an 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 (Venturini et al., 2016).

18. While Terms of Service themselves usually inform which are the documents users are bound to by accepting them (e.g., ToS, Privacy Policy, Cookies Policy, etc.), a large number of auxiliary documents can be found, notably when the platform provider is a large enterprise. The auxiliary documents are either directly linked to the main documents or, sometimes, can be found by browsing the platform.

19. 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.

20. The fundamental right to freedom of expression is most notably guaranteed article 19 of the International Covenant on Civil and Political Rights, amongst other human rights standards. The Guide to Human Rights for Internet Users (CoE, 2014) reaffirms the right to freedom of

expression 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 users' demands and offer effective remedies to their complaints.

21. Recommendations on the notification about the removal of user generated content can also be found in the report of 2011 by the UN Special Rapporteur on Freedom of Opinion and Expression. See: 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.

22. 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.

23. See: 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.

24. The right to privacy is guaranteed by the Universal Declaration of Human Rights (art. 12), the International Covenant on Civil and Political Rights (art. 17), among others, like the American Convention on Human Rights and the European Convention on Human Rights.

25. For recommendations and considerations regarding the human rights impact of third-party tracking, see: La Rue, F. (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; 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.

26. 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).