

2 Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police

Luca Belli, Pedro Augusto Francisco and Nicolo Zingales

Abstract

This chapter argues that digital platforms are increasingly undertaking regulatory and police functions, which are traditionally considered a matter of public law. The authors emphasise that such functions have been growingly delegated to platforms by public authorities, while at the same time platforms are self-attributing such functions to avoid liability, de facto becoming private cyber-regulators and cyber-police.

After highlighting the tendency towards delegation of public functions to private platforms, we provide concrete examples of such phenomenon. For example, the chapter illustrates three types of delegations of public power: the imposition of open-ended injunctions against innocent intermediaries, typically for content removal or website blocking; the implementation of the right to content delisting against search engines, also known as the “right to be forgotten”; and the enlisting of numerous IT companies into a voluntary scheme to counter “illegal hate speech”. We show in all these cases that the amount of discretion conferred on platforms is problematic from the standpoint of the protection of individual rights.

Furthermore, the paper scrutinises the case of the parallel copyright regime developed by YouTube, to emphasise another collateral effect of the privatisation of regulation and police functions: the extraterritorial application of a national legislation – US copyright, in this case – which de facto turns the platform into a private proxy for global application of national regulation. We conclude highlighting some of the challenges and viable solutions for the protection of individual rights in an era of increasing privatisation of regulation and police.

2.1 Introduction

Our analysis departs from the observation that digital platforms²⁸ are increasingly undertaking regulation and police functions, which have traditionally been considered a matter of public law. In particular, such functions have been growingly delegated to platforms by public regulation²⁹, while at the same time platforms are self-attributing such functions in order to avoid liability, *de facto* becoming private cyber-regulators and cyber-police. This tendency is exemplified tellingly by a series of cases we discuss in sections 2 and 3, focusing on different kinds of intermediaries, and illustrating their growing role as Internet points of control.

First, we scrutinise three types of delegations of public power: the imposition of open-ended injunctions against innocent intermediaries, typically for content removal; the implementation of the right to content delisting against search engines, also known as the “right to be forgotten”; and the enlisting of a number of intermediaries into a voluntary scheme to counter “illegal hate speech”. We show in all these cases that the amount of discretion conferred on platforms is problematic from the standpoint of the protection of individual rights. Second, we review the parallel copyright regime developed by YouTube, which can be deemed as the most utilised content distribution platform. This latter example is particularly useful to emphasise another collateral effect of the privatisation of regulation and police functions, which is the extraterritorial application of a national regulatory regime – in this case, US copyright legislation – *de facto* turning the platform into a private proxy for global application of national regulation.

Lastly, we draw some conclusions, based on the presented case studies, highlighting challenges and possible solutions for the protection of individual rights in an era of increasing privatisation of regulation and police.

28 For purposes of this article, we rely on the definition of “platform” laid out in the DCPR Recommendations on Terms of Service and Human Rights, which refers to “any application[] allowing users to seek, impart and receive information or ideas according to the rules defined into a contractual agreement”. See Belli, De Filippi and Zingales (2015), Annex 1 (n).

29 Here, the term “regulation” should be considered as encompassing both the activity of issuing rules (rulemaking) and the activity of adjudicating disputes and taking decision (ruling).

2.2 The Rise of Platforms as Points of Control

Public law and international relations are grounded on the assumption the states and international organisation are the only actors having legitimacy to elaborate and implement binding norms. In this sense, Max Weber critically influenced the evolution of domestic public law, arguing that states are the “political enterprises”³⁰ characterised by “the monopoly of the legitimate use of physical force within a given territory”³¹ while Hans Kelsen affirmed the essential unity between state and legal order, thus considering state and law as synonyms³². However, these assumptions take a different flavour at the international level, where no entity may claim the monopoly of force or the legitimacy to unilaterally establish binding rules. In this context, private actors have long taken the lead and bridged the gap left by the lack of international public authority, through the institution of private ordering systems. Such systems structure³³ in a very effective fashion a wide range of variegated sectors, spanning from global finance to organised crime³⁴ and, of course, the online environment.

By nature, the Internet environment and particularly its application layer – which is composed of privately developed and run platforms – lends itself very well to the surge of private authority to provide law and order while avoiding conflicts of jurisdiction. Indeed, the very commercialisation of the Internet was driven by the belief that “the private sector should lead”³⁵ the expansion of electronic commerce over the Internet on a global basis.

Considering the above, it is not a surprise that the digital platforms that populate cyberspace have long established private mechanisms, which represent a much more efficient and reliable

30 Weber (1919).

31 *Ibid.*

32 Kelsen (1967).

33 Susan Strange’s concept of “structural power” (Strange,1988) is useful to describe very well the capability of private entities to shape frameworks within which (natural or legal) persons relate to each other. For a discussion of how such concept can be applied to internet intermediaries, see Horten (2016).

34 Hall and Biersteker (2002).

35 See W J Clinton and Al Gore Jr (1997).

alternative to conflicting and ineffective public institutions in the online world. As such, the ineffectiveness of state coercion – which in the offline world confers public actors a certain degree of authority and leads citizens to respect legislation – has prompted private players to replace it with the contractual rules and technical architecture that establish what behaviours are allowed in the offline world. In this perspective, digital platforms may be considered as cyberspaces in the sense of true virtual territories whose frontiers are defined by their technical architecture³⁶. Notably, platform providers concentrate the capacity to unilaterally establish the law of the (cyber)land, enforce it and utilise their self-established rules to adjudicate conflicts between platform users.

First, platforms enjoy the capacity to regulate the behaviour of their users via their Terms of Service (ToS), which unilaterally establish what content users are authorised to access and share, what activities they are allowed to perform, as well as what data will be collected about users and how such data will be processed.³⁷ One of the salient features of platforms' ToS is that parties do not negotiate them but, on the contrary, the platform provider defines the conditions in a standard fashion – as it happens in all adhesion or boilerplate contracts – and the platform users can only decide to adhere or not to the pre-established terms.³⁸ In this context, the platform user is an adhering party, whose bargaining power is limited to the choice between “take it or leave it” thus giving to the ToS the force of a “law of the platform,” which is established and modifiable uniquely by the platform provider. Furthermore, such quasi-regulatory power may not only be exercised with regard to the definition of substantive provisions enshrined in the platform's ToS but also with regard to the criteria according to which decisions will be taken by the platform when implementing its ToS as well as the procedural and technical tools to be utilised to put into effect the platform's ToS and decisions.

Secondly, differently from legislation and, more generally, from

³⁶ Belli (2016:202, 219).

³⁷ See Belli & Venturini (2016).

³⁸ See Belli & De Filippi (2012); Radin (2012); Kim (2013).

any type of public regulation, platforms' private ordering does not need to be implemented by public executive organs. By contrast, digital platforms can directly implement their self-defined private regulation by designing the platform's technical structure according to the ToS, in a way that only allows users to perform the actions that are permitted by the platform's rules of engagement. Regulation by architecture³⁹ is also possible in the off-line but the level and scale of control achieved by the digital architectures of online platforms is extremely difficult to achieve even in the most authoritarian regimes of the offline world. Moreover, the algorithms that enable the platform's functionalities – for instance, establishing the order according to which information will be displayed on the platform's timeline – do not need implementation, for they are self-executing norms⁴⁰. Platforms may also independently establish and run alternative dispute resolution and other private remedy mechanisms, as we stress in section 2.b, including by employing individuals who actively monitor users' compliance with the private regulation.⁴¹

Thirdly, platforms usually include – and frequently impose⁴² – alternative dispute resolution mechanisms to solve conflicts amongst users based on the law of the platform. As such, these intermediaries do not simply enjoy a quasi-normative power to establish the ToS and the quasi-executive power to enforce them but they also enjoy the quasi-judicial power to take decision based on the ToS provisions, for instance deliberating what constitutes “obscene” or “harmful” content. However, such private decision-making may frequently lead to erroneous decisions and over-restriction, as has been stressed by Urban, Karaganis and Schofield (2017), with regard to takedowns of

39 In this sense, Lawrence Lessig argues that regulation of real spaces can define the constraints that real space creates and, likewise, the regulation of the cyberspaces' architecture defines constraints on cyberspaces. See Lessig (2006:127-128).

40 Belli (2016:140-144).

41 As an example, Facebook currently employs a team of more than 7,500 “community operators” dedicated to the review “millions of reports” of abusive content that Facebook receives weekly. See Mark Zuckerberg officially announcing the hiring of 3,000 extra operators to cope with the increasing reports of “abuse”, on 3 May 2017, *supra* n. 3.

42 In this regard, a recent study conducted by the Center for Technology and Society at Fundação Getulio Vargas analysed the ToS of 50 digital platforms, demonstrating that 34% of the analysed ToS imposed arbitration as the only method for dispute resolution. See Center for Technology and Society at Fundação Getulio Vargas (2016).

supposedly illicit content.

Although the expansion of private regulation over individuals should not be considered necessarily as a negative phenomenon, the ways in which business actors exercise their “private sovereignty” should be subject to public scrutiny, in order to avoid the emergence of abusive conducts. As pointed out by Chenou and Radu (2017), the rise of private authority in the online context does not necessarily result in a loss of sovereignty and decision-making power for the state, but it rather stimulates a hybridisation of governance. Indeed, it seems that the supposed efficiency of digital platforms’ private enforcement is leading public actors to increasingly delegate regulatory functions to private actors. In this perspective, the OECD already stressed in 2011 the pivotal role that Internet intermediaries, such as digital platforms, play in advancing public policy objectives.⁴³ This consideration is leading an ample range of governments to utilise digital platforms – and Internet intermediaries in general – as proxies in order to reaffirm their national sovereignty online.

However, it should be emphasised that, in their pursuit of efficiency or compliance with national regulation, platforms end up focusing on cost minimisation and avoidance of their potential liability rather than individual rights maximisation. Moreover, the entrustment of platforms with regulatory functions tends to increase their power *vis a vis* market participants which depend on the platform’s services, and often entrench already powerful market positions by imposing regulatory burdens on a whole category, to the disadvantage of smaller competitors. Finally, it should not be underestimated that platforms may choose to simply implement domestic legislation at the global level, rather than designing a framework better suited to meet multicultural needs and exceptions, thereby leading to the extraterritorial implementation of a discretionarily chosen regime. In the following sections, we offer some concrete examples, corroborating what we have argued above with evidence and illustrating the rise of platforms as *de facto* private regulators and police of cyberspace.

43 See OECD (2011).

2.3 The Delegation of Regulatory and Police Functions to Private Intermediaries

In recent years, the above-mentioned type of delegation of public functions to online platforms has increased exponentially. As discussed, such transfer of responsibilities is grounded upon the recognition of the instrumentality of Internet intermediaries in advancing public policy objectives. This can be explained by digital platforms' essential role with regard to the circulation of information online, as well as by the inescapable need for any regulatory framework to involve platform in the implementation process, in order to be effective. However, as illustrated below, the varying mechanisms by which such involvement is established are typically lacking in the definition of limits to the platforms' discretion, thus failing to secure due respect for the fundamental rights of the individuals who bear the consequences.

Three prominent examples of this tendency are: (i) the use of injunctions against (innocent) intermediaries to remove illegal content from their properties; (ii) the entrustment of data controllers with the delisting of specific information, implementing the so called "right to be forgotten"; and (iii) the enlisting of a selected number of ICT companies for the countering of "illegal hate speech". These examples vividly illustrate that the tasks assigned to digital platforms as private executors of regulatory objectives can morph into private law-making and adjudication, where platforms not only choose the means of implementation of the delegated functions, but also substantially take part in the definition and interpretation of the rights and obligations of their users.

2.3.1 Injunctions against Innocent Third Parties

The first example concerns a possibility that the European Union has explicitly established in its legislation concerning intellectual property enforcement⁴⁴. Indeed, according to Article 11 of the Intellectual Property Enforcement Directive of 2004, "Member States shall [...] ensure that rightholders are in a position to apply

44 See Husovec (2017).

for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right” (IPR). The interpretation of this provision as sufficient legal basis to trigger the intermediary’s duty to assist rightholders, even in the absence of liability, was confirmed in *L’Oreal v Ebay*⁴⁵. In this trademark-related case, which involved the online marketplace eBay, the European Court of Justice also clarified that such injunctions may entail the prevention of future infringements of the same kind⁴⁶. Worryingly, the Court did not specify what would constitute an infringement of that “kind”; nor did it indicate what specific types of measures that can be imposed through such injunctions⁴⁷. However, it provided an admonition to EU Member States that such measures must strike a “fair balance” between on the one hand, the right to intellectual property and the right to an effective remedy for the IPR holder, and on the other hand, the intermediary’s freedom to conduct business and the end users’ right to personal data protection, privacy and freedom of expression⁴⁸.

In a later case, the Court provided further details on the meaning of this admonition with regard to injunctions imposing website blocking. Conspicuously, such measures shall “at least partially prevent and seriously discourage the access to a targeted website”⁴⁹ but without leading to unbearable sacrifices for the intermediary in question⁵⁰ and without “unnecessarily depriv[ing] Internet users of the possibility of lawfully accessing the information available”⁵¹. It also established that any such measures must give the court dealing with enforcement proceedings a possibility to assess their degree of reasonableness; and must provide a possibility for Internet users to assert their rights before a court once the implementing measures taken by the Internet

45 Case C-324/09, *L’Oreal v. eBay*, ECLI:EU:C:2011:474, paras. 137-144.

46 Para. 144.

47 The Court only provided two examples: the suspension of the infringer, and measures that make it easier to identify customers who are operating in the course of trade. See paras. 141- 142.

48 Para. 143.

49 Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH*, ECLI:EU:C:2014:192. Para. 57.

50 Para. 62.

51 Para. 63.

service provider are known⁵². Despite these important caveats, it cannot be neglected that the answers to a number of crucial questions for the effectiveness of fundamental rights protection remain subject to the discretion of the platform – or any other intermediary – implementing the measure.

This is especially problematic considering that the CJEU admitted⁵³ the possibility for courts to issue injunctions imposing an “obligation of result”, as opposed to an obligation to adhere to a prescribed course of conduct (“obligation of conduct⁵⁴”). In practice, such injunctions to obtain a particular result entail a choice between an ample range of measures with different relative impact on fundamental rights. Letting aside doubts about the suitability of such cost-benefit analysis to determining the scope of protection of fundamental rights, it is evident that economic incentives directly impact the effectiveness of protection afforded to individuals. Intermediaries are naturally inclined to err in favour of more restrictive measures, rather than to try and devise more elaborate and costly solutions that accurately balance conflicting rights: restricting access to content exhaust the demands of copyright holders, while affected subjects would need to file a separate claim in order to mitigate its adverse effects.

The trend of granting injunctive relief against innocent third party should not be considered as a European specialty and can also be noticed in other jurisdictions, notably the United States, where a number of orders have been issued requiring domain name registries, Internet service providers, payment intermediaries, search engines and social media to prevent the accessibility of infringing websites.⁵⁵ More recently, the trend was also embraced for the first time by the Canadian Supreme Court in *Google v Equustek*⁵⁶. Affirming the lower court’s opinion that imposed

52 Para. 57.

53 *Id.*

54 See Conde (1999:102).

55 See, e.g., *Hermes v. Doe*, (SDNY April 30, 2012); *Chanel Inc. v. Does* (D. Nev., Nov. 14, 2011); *ABS-CBN Corporation v Ashby*, Case (Dist. Or. Aug. 8, 2014); *Richemont International SA v Chen*, Case (SDNY Jan. 4, 2013); *Arista Records LLC v. Tkach*, 122 F.Supp.3d 32 at 33-38 (SDNY 2015).

56 *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34.

Google to delist certain trademark-infringing websites on a worldwide level, the Canadian Supreme Court found it justified to do so on the basis of its equitable jurisdiction, which among other things allows the issuing of orders against non-parties that facilitate the commission of wrongdoing⁵⁷. Crucially, the Court found “unpersuasive” Google’s argument that the order clashes with the right to freedom of expression recognised in other countries, requiring it instead to prove in separate proceedings that any such conflict has actually arisen.

2.3.2 The Right to Be Forgotten and the Rise of Private Remedy Mechanisms

A second example of delegation concerns the implementation of the so called “right to be forgotten” defined by the CJEU in the *Google Spain* case⁵⁸. In that case, the Court affirmed the existence of the right of all individuals to obtain erasure of their personal data from the results of search engines prompted by a search for their name, whenever such information is “inadequate, irrelevant or no longer relevant, or excessive.” While the judgment has been primarily criticised for its insufficient consideration of freedom of expression, the most striking implication for our purposes is that it leaves the responsibility of implementing the aforementioned right in the hands of a private entity. Although the result of the private pondering between the accessibility and the elimination of the from the search results under an individual’s name may be subsequently appealed by that data subject to the relevant data protection authority, we should stress that this mechanism creates not only one, but potentially multiple regimes of private governance running in parallel to (and possibly afoul of) the domestic legal systems.

Shortly after the ruling, all three major search engines in Europe (Google, Microsoft Bing and Yahoo) acted as *de facto* regulators creating a specific web form that enables users to provide the

57 Para. 31.

58 Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, ECLI:EU:C:2014:317. For a more in-depth analysis, see Zingales and Janczuck (2017).

relevant information that should be delisted⁵⁹, each with their own different requirements. For example, while Google and Yahoo provide a blank space in the form for individuals to explain how the page relates to the data subject and why its content is “unlawful, inaccurate, or outdated”,⁶⁰ while Microsoft Bing poses a number of additional questions.⁶¹

Furthermore, although these companies have not yet released any criteria they use to adjudicate conflicting rights, it is likely that significant divergence arises as a result of the open-ended character of the guidelines provided by the Article 29 Working Party⁶². The lack of prescriptions detailing the implementation of those guidelines in accordance with national freedom of expression standards, granting these entities wide discretion in the implementation of the right, is problematic for at least two reasons. First, search engines are not public courts, and thus employees tasked with making these determinations will not have the same competence and standards of professional ethics and independence that bind members of the judiciary⁶³. The fact that the relevant DPA and a court may be asked to review such determinations is not sufficient to overcome this concern, as such requests are unlikely to be systematic, and can only be made by the affected data subject (not by the individual or entity who has produced the content whose accessibility is in question). Second,

59 According to press coverage, Google made its form available in June 2014, and Microsoft in July of the same year. It is less clear when the form first appeared on Yahoo!, although it was reported to be already in place on December 1st, 2014. See Schechner (2014); and Griffin (2014).

60 For Google, see <https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636297647133257433-1626206613&rd=1> [accessed 31 October 2017]; for Yahoo, see <goo.gl/3qUdTe> [accessed 31 October 2017].

61 See <<https://www.bing.com/webmaster/tools/eu-privacy-request>> [accessed 31 October 2017]. Specifically, claimants must indicate (1) whether they (and presumably anyone on behalf of whom the application is made) are public figures; and (2) whether they have or expect to have a role in the local community or more broadly that involves leadership, trust or safety. Furthermore, claimants are asked to qualify the information that Bing is requested to “block” as (a) inaccurate or false; (b) incomplete or inadequate; (c) out-of-date or no longer relevant; or (d) excessive or otherwise inappropriate. They are also invited to indicate why their “privacy interest” should outweigh the public’s interest in free expression and the free availability of information. Last, but not least, they are given the opportunity to upload supporting documentation.

62 Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union Judgment on ‘Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales’ C-131/12., 14/EN WP 225 (26 November 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf> [accessed 1 November 2017].

63 Haber (2016).

the nature and depth of balancing users' fundamental rights may be affected by the economic incentives and the interest of those entities to conduct their business in the most efficient and lucrative fashion. For instance, it is clear that a very probing inquiry into the circumstances of each case would impose serious costs on the search engine. Similarly, it runs against the incentives of search engines operators to publish a detailed list of their criteria for decision-making, as the availability of such criteria would make users' claims more sophisticated and more complex to decide. Under these conditions, as a result of the concerns for transparency of the criteria and fairness over their substantive standards, the role of online platforms in giving effect to individual rights becomes at least questionable.

2.3.3 Countering of Illegal Hate Speech

Our third example of public functions delegation relates to the agreement defined by the European Commission in conjunction with Facebook, Microsoft, Twitter and YouTube, with the aim of adopting a specific code of conduct on “countering the spread of illegal hate speech online.”⁶⁴ Above all, the code of conduct requires such companies to have in place “Rules or Community Guidelines clarifying that they prohibit the promotion of incitement to violence and hateful conduct,” and “clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content”, in the majority of cases in less than 24 hours since the reception of a valid notification. It also demands companies to “raise awareness” about their rules and procedures with users and Member States' designated national contact points, and encourages the provision of notice and flagging mechanisms to tackle hate speech with the help of experts from civil society organisations through the creation of a group of “trusted reporters”. On its part, the European Commission commits, in coordination with Member States, to promote adherence to the Code to other relevant platforms and social media companies, thereby setting the conditions for this

⁶⁴ The text of the “Code of Conduct” agreement can be found at <http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf> [accessed 31 October 2017].

to serve as a basis for promoting greater protection against hate speech in the sector.

As pointed out by Article 19, there are significant problems of overbreadth with the definition of “hate speech” provided by the Code, which derives from the Commission’s Framework Decision on Combating Certain Forms and Expressions of Racism and Xenophobia by Means of Criminal Law.⁶⁵ Notably, the code of conducts presents an overbroad focus on “incitement to hatred” (as opposed to the ICCPR’s “incitement to discrimination, hostility and violence”), a lack of reference to the intent of the speaker and an unspecified threshold of seriousness for the forms of racism and xenophobia to be considered as illegal⁶⁶. Furthermore, as noted by EDRI, the Code effectively creates a framework for privatised law-enforcement by enabling the above-mentioned companies to come up with an own definition of “hate speech” in their rules and to community guidelines, and review removal requests against those rules and guidelines⁶⁷. Finally, there are concrete problems of oversight in the application of the Code, given that there is no direct reporting from the companies adhering to the code, but only “testing” of the reactions received by organisations that volunteered to submit notices in different Member States⁶⁸. As a result of these tests, the review of the practices of these companies one year after the enactment of the Code revealed deficiencies in feedback provided to users submitting notification, corroborating the picture that companies enjoy a large amount of discretion both in the definition of offenses and in enforcement of those prohibitions.⁶⁹

Interestingly, the Commission has also of recent facilitated the adoption of a Common Position of national authorities within the Consumer Protection Cooperation network concerning the

65 Article 19 (2016).

66 *Id.*, pp. 7-8.

67 McNamee (2016).

68 European Commission, ‘Code of Conduct on countering illegal hate speech online: First results on implementation’ (December 2016), Factsheet, <http://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf> [accessed 31 October 2017].

69 European Commission, ‘Code of Conduct on countering illegal online hate speech 2nd monitoring’, Press Release IP/17/1471, <http://europa.eu/rapid/press-release_MEMO-17-1472_en.htm> [accessed 31 October 2017], at 1 and 5.

protection of consumers on social networks, which seemingly takes issues with the framework created by the Commission through the Code of Conduct⁷⁰. Lamenting the “general and unspecified” nature of the criteria used by social networking platforms to refuse to display or remove content, the Position explains that contract clauses granting “unlimited and discretionary power” without identifying sufficient criteria for the suitability of user-generated content are illegal under consumer law, as they create a significant imbalance *vis à vis* consumers. In addition, the Position proposes the establishment of a standardised communication format between social media and consumer protection authorities including, in the case of requests for removal, information of the action taken and, if no action is taken, the legal and factual reasons for that. While this Position constitutes a significant step towards greater accountability of social networking platforms for their removals and a model exportable to other types of digital platforms, it still does little to fix the problems originated by the vaguely worded delegation that we have described in this Section.

24 YouTube and iRegulate

In this Section, we consider a more specific example with regard to content regulation. Specifically, we analyse how YouTube shapes copyright through its own ToS, which are based on US copyright law, thus creating a hybrid public-private regime that is entirely privately implemented. The case of the content industry is particularly interesting, because few are the relations that are not intermediated by a third party and therefore, there is ample margin for platform action. To reach a user, the work created by an author must be fixed in some media – be it physical or digital – and subsequently distributed. In the content industry of the 20th century, these activities were typically performed by intermediaries such as big record companies, publishers and producers. These actors have been remarkably impacted by the popularisation of ICTs and by the digitisation of information. However, although digital technologies have completely changed

70 European Commission, ‘The European Commission and Member States consumer authorities ask social media companies to comply with EU consumer rules’, Press Release IP/17/631, <http://europa.eu/rapid/press-release_IP-17-631_en.htm> [accessed 31 October 2017].

the industry settings, such impact has not resulted in the extinction of the aforementioned intermediaries, as many thought at the end of the last century.⁷¹ Indeed, differently from what was originally expected, the mid-2000s witnessed the emergence of streaming platforms, shifting intermediation towards the offering of content as a service, rather than as a product.

The historical reality of content industries shows that several actors who were relevant in the past still retain their importance. Although the configurations have changed, the power relations have been maintained as old intermediaries have adapted to the current scenario and big copyright holders continue to influence how copyrighted works can be reproduced and distributed. What is different now is the emergence of a new breed of actors in the content industries: the digital distribution platforms. These platforms can be characterised by their private governance, consisting in privately defined rules along with the provision of an infrastructure designed to allow only the authorised interactions between the involved actors⁷². Their business models depends on the use of information and communication technologies to connect people, organisations and resources, inside ecosystems where value is generated and goods and services are exchanged. Ultimately, the goal of digital distribution platforms is to foster the establishment of agreements between their users and facilitate any type of exchange that can generate value from the distributed material.

Among these digital platforms, one of the most notable is certainly YouTube. Created in 2005 and acquired by Google just over a year later, YouTube is by far the biggest online video streaming platform in the world, with – according to its own website⁷³ – over a billion users, which would mean almost one-third of all Internet users. The website also states that, In the US, the platform reaches more people between 18 and 49 years old than any cable TV. YouTube has been influencing content consumption in such

71 In this sense, see Parker, Alstyne & Choudary (2016); Evans and Schmalensee (2016); Moazed & Johnson (2016).

72 Rochet & Tirole (2003).

73 See 'YouTube in numbers' <<https://www.youtube.com/intl/en-GB/yt/about/press/>> [accessed 31 October 2017].

a way that it cannot be perceived as a mere channel between creators and consumers. As a cultural-industry intermediary, Youtube implements its own content governance technologies and imposes on its users the US Digital Millennium Copyright Act (DMCA), a legal regime that should only apply to US users – not users in any country in which a video is watched or uploaded.

YouTube’s private copyright protection is enforced through two mechanisms: copyright takedowns and the Content ID system. The copyright takedown mechanism works in accordance with the DMCA. US copyright law determines that online hosting providers shall not be liable for copyright infringement if they do not have actual knowledge of the infringing material on its system, and have designated a DMCA agent to receive notifications of allegedly illegal content. Once received a notice, the online service provider wishing to escape potential liability must expeditiously take that content down. Only subsequently can the content uploader file a counter-notice, in which case Youtube shall make that content available after 10 to 14 days, unless the original claimant demonstrates to have filed an order in court against the alleged infringer.

As is well known, YouTube is a video-sharing platform which also offers users the ability to create their own channels, where they can stream or simply share with followers their own videos. Any person who believes their copyright-protected work was posted in a channel without authorisation may submit an infringement notice through a dedicated web form.⁷⁴ YouTube will remove the allegedly infringing video and the owner of the channel that uploaded it will receive a “copyright strike”. According to YouTube’s privately established procedure, if a channel receives three copyright strikes, its owner’s account will be terminated, all their videos will be removed – importantly, even the ones that were *not* infringing any rights – and the user will not be able to create new accounts. After being notified that the infringing video has been struck, the owner has three possible courses of

⁷⁴ See ‘Submit a Copyright takedown notice’ <https://support.google.com/youtube/answer/2807622?hl=en&ref_topic=2778544> [accessed 31 October 2017].

action.⁷⁵ First, the notified user can decide to wait for the strike to be removed after 90 days, subject to the condition that the user attends YouTube's "Copyright School." This means that the owner must watch an animated video explaining the functioning of copyright and answer 4 true-or-false questions about the topic to verify the content has been understood correctly.

Despite its friendliness and humour – the Copyright School video consist in a Happy Tree Friends short animation – the video has a strong message about the dangers of using copyright protected materials without authorisation, alerting the audience that infringing copyright can result in economic loss. Even though there is a short mention to the existence of fair use⁷⁶ and similar provisions in the US and other countries jurisdictions, the video is emphatic in saying that any misuse or false allegations can result in a court case.⁷⁷ The underlying message is to always use original content, despite the fact that the use of third-party content may be legally legitimate in several cases. The second possible action is to contact directly the person who triggered the strike and ask this person to retract the claim, while the third option for the recipient of a strike is to submit a counter-notice through an ad hoc web form.⁷⁸ YouTube then forwards the counter-notice to the original claimant, who has 10 days to show proof that he or she has initiated a court action aimed at keeping the content down. Failing that, the platform will put the video back online.

The Content ID System is a more sophisticated tool. Since 2007, in order to legitimise itself as a reliable and law-abiding platform and to consolidate its position as a mainstream distribution medium, YouTube created a new system of digital identification, which can

75 See UN Human Rights Committee Act or the dissemination of EU and national law. See 'Copyright Strike Basics' <https://support.google.com/youtube/answer/2814000?hl=en&ref_topic=2778545> [accessed 31 October 2017].

76 The US Copyright Office defines fair use as the legal doctrine that promotes freedom of expression by permitting the unlicensed use of copyright-protected works in certain circumstances. Section 107 of the US Copyright Act provides the statutory framework for determining whether something is a fair use and identifies certain types of uses—such as criticism, comment, news reporting, teaching, scholarship, and research—as examples of activities that may qualify as fair use. See more at <<https://www.copyright.gov/fair-use/more-info.html>> [accessed 31 October 2017].

77 See YouTube's 'Copyright School' <https://www.youtube.com/copyright_school> [accessed 31 October 2017].

78 See Youtube's 'Counter Notification Basics' <https://support.google.com/youtube/answer/2807684?hl=en&ref_topic=2778545> [accessed 31 October 2017].

identify copyright protected materials. The system is based on the premise that any video has unique attributes that allows identification of the material even from within a short clip.⁷⁹ In this system, any copyright holder can establish a partnership with YouTube, where it uploads its protected material and allows it to become part of a reference database. YouTube can then automatically detect the use of that material in other videos. When the copyright holder establishes this type of partnership, three different actions become available to manage any further material that matches with the uploaded one. The copyright holder can decide to block a whole video from being viewed; to mute a video that contains the copyright protected music; to monetise the video by running ads against it – potentially opting for sharing the revenue with the user that uploaded the material –; and to simply track the video’s statistics.⁸⁰ This gives record companies the ability to automatically monetise a mashup video that uses even a fraction of one of their owned material, or simply block that content.

In fact, much like in the case of the notice and takedown procedure implemented by YouTube, the biggest problem with the Content ID system is that it does not require the consideration of fair use provisions by copyright holders submitting a claim⁸¹. Even though the system allows for a Content ID claim dispute, the rights holder may disagree with the uploader’s reasoning and request the removal of their video– which means that the potentially “fair” user will end up receiving a copyright strike. Recently, YouTube changed its Content ID policy in order to assuage at least part of these concerns. The main innovation is it will hold advertisement revenues associated with any video in a Content ID dispute, to then disburse the funds to the winning party only once the claim is resolved.⁸² However, this is far from solving the problem of overbroad takedowns documented by Urban, Karagnis, Schoefield (2017).

79 See Kevin J. Delaney, ‘YouTube to Test Software To Ease Licensing Fights’, *Wall Street Journal* (12 June 2007) <<https://www.wsj.com/articles/SB118161295626932114>> [accessed 31 October 2017].

80 See Youtube’s ‘How Content ID Works’ <https://support.google.com/youtube/answer/2797370?hl=en&ref_topic=2778544> [accessed 31 October 2017].

81 Note that this is in direct conflict with the Ninth Circuit’s ruling in *Lenz v Universal*, which held that §512(c)(3)(A) (v) requires the consideration of fair use before the issuing of takedown requests. See *Lenz v. Universal Music Corp.*, 801 F.3d 1126 (2015).

82 See Goodmann (2016).

Systems like Content ID and copyright strikes are implementations of a private right-management regime embodying a “DMCA-plus” approach – i.e., voluntary, above-and-beyond enforcement measures that are undertaken by intermediaries whose compliance obligations are defined by DMCA safe harbours clauses⁸³. Such regimes should not be valid outside of the US but are privately implemented by globally accessible digital platforms. This observation serves to relativise the idea that YouTube is a “global” platform, for in fact its private regulation is based on a very specific American law. Indeed, YouTube’s private regulation rarely ensures respect of exceptions and limitations recognized in international copyright regimes and implemented in legislation other than US law. As discussed, although YouTube provides the possibility of a dispute between users – allowing the user that had its content blocked to defend him or herself – the mode of resolution of the conflict and the continue availability of the disputed content are at the mercy of the copyright holder.⁸⁴ In the end, through its architecture and ToS, the platform takes a clear choice of reinforcing the imbalance of power between big copyright holders and those small independent creators who depend on YouTube to make and distribute their content.

2.4 Conclusions

The examples discussed above seem to corroborate our initial hypothesis, *i.e.* that the advent of the Internet environment has prompted parallel consolidation of power in the hands of private intermediaries, demonstrating an increasing tendency towards the privatisation of traditionally public functions. In some instances, this tendency is the result of a specific choice taken by policymakers or courts, obliging platforms to implement appropriate responses and mechanisms to avoid liability or to give force to a decision (as in the cases of injunctions against innocent third parties and the implementation of *Google Spain*). In another scenario, the choice to define specific rules or to utilise specific national frameworks globally is “voluntarily”

⁸³ See Bridy (2015).

⁸⁴ Francisco & Valente (2016).

made (with different degrees of regulatory influence) by the specific platform, as shown in the implementation of the code of conduct on hate speech and in YouTube's approach to copyright exceptions and limitations. These examples illustrate that the lack of adequate constraints to platform power generates collateral damages, such as insufficient commitment to fundamental rights protection and distortion of competition in the market.

Digital platforms have become essential to allow individuals fully enjoy many of their fundamental rights, such as the right to educate themselves, their right to privacy and their freedom of communication and of information. In this sense, in light of the fact that social interactions increasingly depend on digital platforms, it is simply unacceptable for States to throw their hands up and let platform define the content, scope and limitations of fundamental rights without adequate constraints. More specifically, States cannot escape liability for violations of such rights occurring as a result of platform rules created in response to the incentives set up by the legal framework⁸⁵, be it for insufficient safeguards or for lack of regulatory intervention. International human rights law is quite clear in this respect, affirming not only "the positive obligations on States Parties to ensure human rights [and protect] individuals against acts committed by private persons or entities"⁸⁶ but also that "the obligations of States to respect, protect and promote human rights include the oversight of private companies."⁸⁷

There is a spectrum of responses that States can take to ensure appropriate protection of fundamental rights, ranging from "command and control" regulation to secondary liability regimes, co-regulation, and ultimately self-regulation: thus, the encouragement of platform responsibility through commitment and transparency mechanisms constitutes the least intrusive type of regulatory intervention. Choosing this end of the scale may be preferable in the absence of evident market failures, but can

85 Zingales (2014).

86 See UN Human Rights Committee (2004).

87 See CoE Recommendation CM/Rec (2014)6.

only be effective in conjunction with adequate State supervision designed to ensure the detection and remedy of such failures. Additionally, targeted efforts of promotion of a culture of human rights compliance in the corporate environment may be necessary to ensure that the impacts of platforms on individuals are taken into account at the level of management as well as by shareholders, highlighting the significance of monetary consequences of human rights violations, such as reputational losses and liability under domestically implemented human rights law.

This focus on platforms' self-awareness and acceptance of their own responsibility to respect human rights is in line with the increased recognition of corporations as responsible entities for the upholding of the values of International human rights law, and should imply at a minimum that platforms do not merely devise the most cost-efficient solutions to conflicts between users, but rather strive to ensure effective protection of fundamental rights. States should remain vigilant that this does not remain an aspiration of principle, ensuring that it be given concrete effect through platforms' policies and ToS.

2.5 Bibliography

Article 19 (2016). 'EU: European Commission's Code of Conduct for Countering Illegal Hate Speech Online and the Framework Decision' (Article 19, June 2016) <<https://www.article19.org/data/files/medialibrary/38430/EU-Code-of-conduct-analysis-FINAL.pdf>> [accessed 31 October 2017].

Article 29 Working Party, 'Guidelines on the implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales' C-131/12', 14/EN WP 225 (26 November 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf> [accessed 1 November 2017].

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

Belli L, De Filippi P and Zingales N (eds.) (2015). 'Recommendations on terms of service & human rights. Outcome Document n°1; <<https://tinyurl.com/toshr2015>> [accessed 31 October 2017].

- Belli L & Venturini J (2016). 'Private ordering and the rise of terms of service as cyber-regulation' (2016) 5 (4) *Internet Policy Review*.
- Bridy A (2015). 'Copyright's Digital Deputies: DMCA-Plus Enforcement by Internet Intermediaries'. J A Rothchild (ed.), *Research Handbook on Electronic Commerce Law* (Edward Elgar, 2016).
- Center for Technology and Society at Fundação Getulio Vargas (2016). 'Terms of Service and Human Rights: An Analysis of Platform Contracts' (Recavan Press, 2016) <<http://tinyurl.com/tosh>> [accessed 31 October 2017].
- Chenou J M and Radu R (2017). 'The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union' *Business & Society*.
- Evans D and Schmalensee R (2016). *Matchmakers: The New Economics of Multisided Platforms*. (Harvard Business Review Press, 2016).
- European Commission, 'Code of Conduct on countering illegal hate speech online: First results on implementation' (December 2016), Factsheet, <http://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf> [accessed 31 October 2017].
- European Commission, 'Code of Conduct on countering illegal online hate speech 2nd monitoring', Press Release IP/17/1471 <http://europa.eu/rapid/press-release_MEMO-17-1472_en.htm> [accessed 31 October 2017].
- European Commission, 'The European Commission and Member States consumer authorities ask social media companies to comply with EU consumer rules', Press Release IP/17/631 <http://europa.eu/rapid/press-release_IP-17-631_en.htm> [accessed 31 October 2017].
- Francisco P and Valente M (2016). *Da Rádio ao Streaming: ECAD, Direito Autoral e Música no Brasil*. (Azougue, 2016).
- Griffin A (2014). 'Microsoft's Bing and Yahoo search engines have started to fulfill the controversial requests', *The Independent* (London, 1 December 2014) <<http://www.independent.co.uk/life-style/gadgets-and-tech/news/microsoft-and-yahoo-join-google-in-deleting-search-results-under-right-to-be-forgotten-ruling-9896100.html>> [accessed 31 October 2017].
- Goodmann D (2016). 'YouTube's Content ID Policy Change Now Saves Lost Monetization for Fair Use Videos' (*Washington Journal of Law, Technology and Law Blog*, 1 December 2016) <<https://wjlt.com/2016/12/01/youtubes-content-id-policy-change-now-saves-lost-monetization-for-fair-use-videos/>> [accessed 31 October 2017].
- Haber E (2016). 'Privatization of the Judiciary' (2016), 40 *Seattle University Law Review* 115.

- Hall RB, and Biersteker TJ (Eds.) (2002). *The emergence of private authority in global governance*. (Cambridge University Press, 2002).
- Horten M (2016). *Closing of the Net* (Polity Press, 2016).
- Husovec M (2017). *Injunctions against Intermediaries in the European Union*. (Cambridge University Press, 2017).
- Kelsen H (1967). *Pure Theory of Law. Translation from the Second German Edition by Max Knight*. (University of California Press, 1967).
- Kim NS (2013). *Wrap Contracts: Foundations and Ramifications* (Oxford University Press, 2013).
- OECD (2011). *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (OECD Publishing, 2011). <<http://dx.doi.org/10.1787/9789264115644-en>> [accessed 31 October 2017].
- McNamee J (2016). 'Guide to the Code of Conduct on Hate Speech' (EDRI, June 2016) <<https://edri.org/guide-code-conduct-hate-speech/>> [accessed 31 October 2017].
- Moazed A and Johnson N (2016). *Modern Monopolies: What it Takes to Dominate the 21st Century Economy* (St. Martin's Press, 2016).
- Parker G, Alstynne M and Choudary S (2016). *Platform Revolution - How Networked Markets Are Transforming the Economy - and How to Make Them Work for You* (W. W. Norton & Company, 2016).
- Radin M J (2012). *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press, 2012).
- Rochet J C and Tirole J (2003). 'Platform Competition in Two-Sided Markets' (2003) 1 (4) *Journal of the European Economic Association* 990.
- Schechner S (2014). 'Google Starts Removing Search Results Under Europe's 'Right to be Forgotten'', *Wall Street Journal* (New York, 26 June 2014) <<https://www.wsj.com/articles/google-starts-removing-search-results-under-europes-right-to-be-forgotten-1403774023>> accessed 31 October 2017].
- Strange S (1988). *States and markets* (Continuum, 1988).
- 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>
- Urban JM, Karaganis J and Schofield BL (2017). 'Notice and Takedown in Everyday Practice' UC Berkeley Public Law Research Paper No. 2755628. <<https://ssrn.com/abstract=2755628>> [accessed 31 October 2017].

Weber M (1919). 'Politics as a Vocation'. in H H Gerth and C Wright Mills (eds.) *From Max Weber: Essays in Sociology* (Routledge & Kegan Paul, 1948).

Zingales N (2014). 'Virtues and perils of anonymity: should intermediaries bear the burden?' (2014) 5 (3) *Journal of Intellectual Property, Information Technology and E-commerce* 155.

Zingales N and Janczuck A (2017). 'Implementing the Right To Be Forgotten: towards a co-regulatory solution?' e-conférence on the Right to Be Forgotten in Europe and Beyond, May 2017, Blogdroiteuropeen. <<http://wp.me/p6OBGR-22t>.> [accessed 31 October 2017].