Oñati Socio-Legal Series (ISSN: 2079-5971)
Oñati International Institute for the Sociology of Law
Avenida Universidad, 8 – Apdo. 28
20560 Oñati – Gipuzkoa – Spain
Tel. (+34) 943 783064 / opo@iisj.net / https://opo.iisj.net

Tackling online hate speech from a European perspective: Potentials and challenges of inter-legality

OÑATI SOCIO-LEGAL SERIES VOLUME 13, ISSUE 4 (2023), 1376–1411: ACCESS TO JUSTICE FROM A MULTI-DISCIPLINARY AND SOCIO-LEGAL PERSPECTIVE: BARRIERS AND FACILITATORS
DOI LINK: HTTPS://DOI.ORG/10.35295/OSLS.IISL/0000-0000-0000-1392
RECEIVED 28 NOVEMBER 2022, ACCEPTED 31 JANUARY 2023, FIRST-ONLINE PUBLISHED 3 FEBRUARY 2023, VERSION OF RECORD PUBLISHED 28 JULY 2023

BARBARA GIOVANNA BELLO*

Abstract

The contribution delves into some main implications of the current soft and hard legal framework related to the Internet governance for tackling online hate speech, from the perspective of legal and social actors based in the European Union (EU). Given the dynamic constellation characterised by centripetal trends towards UN-fostered international governance, Council of Europe and EU soft and hard legal instruments, co-existing with centrifugal forces of national legislations, the article explores areas where inter-legality may be fruitfully engaged to contribute tackling online hate speech in today's fast changing and complex legal scenario. Hence, due to the lack of a universally recognised definition of hate speech and a global regulation of online communication, inter-legality may be operationalised in still unexplored places – that is, not only by judges but by lawmakers, independent authorities on communication, and even platforms.

Key words

Internet governance; online hate speech; inter-legality; legal and non-legal actors

Resumen

La contribución profundiza en algunas de las principales implicaciones del actual marco jurídico vinculante y no vinculante relacionado con la gobernanza de Internet para hacer frente a la incitación al odio en línea, desde la perspectiva de los actores

This contribution complements my research on preventing and tackling online hate speech related to the substantive legislation (Bello 2021) initiated within the Center Information Society Law, University of Milano, Italy, the Officina informatica su Diritto, Etica, Tecnologie (DET), University of Modena and Reggio Emilia, Italy, and the Digital Equality Working Group" of the Berkeley Center on Comparative Equality & Anti-Discrimination Law. I wish to thank Marco Bassini, and the anonymous peer-reviewers for their suggestions to improve earlier versions of this article.
* Barbara Giovanna Bello, Università degli Studi della Tuscia, Viterbo, Italy, barbaragbello@gmail.com,

jurídicos y sociales con sede en la Unión Europea (UE). Dada la constelación dinámica caracterizada por las tendencias centrípetas hacia la gobernanza internacional promovida por la ONU, los instrumentos jurídicos blandos y duros del Consejo de Europa y de la UE, que coexisten con las fuerzas centrífugas de las legislaciones nacionales, el artículo explora las áreas en las que la interlegalidad puede ser fructífera para contribuir a hacer frente a la incitación al odio en línea en el cambiante y complejo escenario jurídico actual. Por lo tanto, debido a la falta de una definición universalmente reconocida de la incitación al odio y de una regulación global de la comunicación en línea, la interlegalidad puede ser operativa en lugares aún inexplorados, es decir, no sólo por los jueces, sino también por los legisladores, las autoridades independientes de comunicación e incluso las plataformas.

Palabras clave

Gobernanza de Internet; discurso de odio online; interlegalidad; actores jurídicos y no jurídicos

Table of contents

1. Legalities on the Internet

The contestation of the Westphalian State as the only source of law as well as legal and social order relies on a well-established and rich scholarly body of literature, developed from the anti-formalistic critique of law. If the issue has been widely discussed with regard to the offline world, cyberspace – a global and transnational space *par excellence* – has proved to particularly challenge States' sovereignty. The "boundless" nature of the Internet (or 'Web') would have suggested that States would promptly converge towards global agreements on the legal protection of online communication (including against hate speech), a step that still seems hard to take.

The phenomenon of globalisation per se (even offline) though has posed new questions to law-makers since the law has not developed as a uniform and ordered legal space (Itzcovich 2012, Pastore 2017, Palombella 2019, Parolari 2020, 2021), despite the predictions of the proponents of legal globalism (Shapiro 1993, Parolari 2020, 2021). On the contrary, it blatantly appears that the law of the global word has taken a polycentric and interconnected shape, characterised by hybrid legal spaces, where multiple and heterogeneous legal orders and normativities – stemming from a variety of (international, supranational and national; public and private) actors – not only coexist but intersect (Fischer-Lescano and Teubner 2004, Palombella 2018).

The missed promise of global law particularly interests scholars and decision-makers about the possible ways to regulate many aspects of the Internet, including hate speech. In fact, today's legal scenario appears to be still fragmented and, at the same time, very dynamic: it may be observed that it is characterised by both centripetal trends (towards an international governance and supranational provisions) and centrifugal forces of national legislations. Besides them, private actors – e.g., big platforms such as Facebook, Twitter, Instagram, to mention a few – concur or even compete within these hybrid and polycentric legal spaces.

Instead of a global law, legal pluralism seems to become broadly (although not unanimously) accepted as the current and almost general configuration of the offline word, which has increasingly taken the form of a "new legal pluralism" (Berman 2009; cf. Cotterrell 2014) or a "global legal pluralism" (Berman 2014), no longer confined to collisions within one geographical context. This perspective goes well beyond both early elaborations of pluralism in the colonies (see Furnivall 1939, who is credited to have introduced the term) and its later or even updated versions,[1] such as those concerning plural societies, originated by the close encounters among different "cultures" and legal/social norms (Mancini 2015, Parolari 2020).

In international literature, the metaphor of the transition from the "pyramidal system" to that (horizontal and heterarchical) of the "net", pointedly explained by François Ost and Michel Van De Kerchove, is particularly relevant for both the offline and online spheres. This latter space is considered "the network of networks" because it is based on "the global interconnection of multiple local nodes" (Fiorinelli 2021, p. 405; cf. Kahn *et al.* 1997).

[1] In a non-Western perspective, see, at least, Chiba (1989); in the field of criminal law, see at least Delmas-Marty (1986, 2007).

Ost and Van De Kerchove delve into the implications of the transition mentioned above that entails a double shift: from "réglementation" to "régulation", the second consisting of a "weaker, fragmented, contextual, often negotiated" (Ost 2013, p. 42; cf. Ost and Van De Kerchove 2000, 2002) legislation which does not replace the former but overshadows it; from "government" (as institution) to governance (cf. Commaille and Jobert 1998, Scamardella 2021). The plurality of traditional legal actors is flanked by influential – public and private (exponents of the market and civil society), para-State or quasi-governmental – normative actors endowed with various authority and power.

In Italian literature, recently dear departed scholar Paolo Grossi wrote that:

> [t]he old image of the pyramid, mirroring the old regulatory system, is replaced by an image that does not necessarily evoke an unwelcome hierarchical one; and sociologists of law – but also more law scholars at the forefront of the new trenches – speak of a net (…), in the sense of replacing the arbitrary authoritarian pyramidal image by a system of rules that are not placed one above or below the other, but, on the same level, linked to one other by a relationship of reciprocal interconnection. Rules that don't will find their legitimacy in a single supreme source identified by who holds the supreme political power, but most often in a spontaneous motion of that varied and mobile reality represented by the market. (Grossi 2002, p. 160, my translation)

The interconnection between norms from multiple legal orders, all simultaneously applicable to concrete cases on the basis of the ordering principle of the impact on the very case under scrutiny, is at the core of a recent conceptualisation of *inter-legality* in legal philosophy (Palombella 2019, Chiti *et al.* 2021a) that departs from socio-legal scholar Boaventura de Sousa Santos' original elaboration (*interlegality*). It may be suggested that the hyphen (-) of the term 'inter-legality' marks a semantic shift from 'interlegality': therefore, in the following, I will use these words accordingly.

In light of the above, the hypothesis guiding my reflection is that, in the lack of global binding regulation of online communication and Internet governance[2] (Raustiala 2016, Radu 2019), inter-legality may provide (at least) tools and (even) a method to judicial and non-judicial actors in handling hate speech-related "cases" in a loose sense. My suggestion is that inter-legality may have a strong impact if it is operationalised in still unexplored places – that is, not only by judges but by lawmakers (Chiti *et al.* 2021b, 21–23), independent authorities on communication, and even platforms. In fact, currently, judges both bear the burden and have the opportunity to consider all and often conflicting legislations applicable to the concrete judicial case. This occurs when trying to find a balance between, on the one side, the protection of internet users' dignity and non-discrimination and, on the other side, freedom of speech within a complex inter-legal framework. They are not the only actors, though, faced with this challenge and creative space. The very characteristics of online hate speech (*infra*, para. 3) lend it to being considered as a "paradigmatic case" to be analysed from this perspective, given the unavoidable overlap among provisions from international, supranational, national

[2] At the substantive level, the lack of a universally recognised definition of (offline/online) hate speech further complicates preventing and tackling this phenomenon (Ziccardi 2016, 2019), which also engages inter-legality. From the outset, States' prevailing trend has been to ensure the same level of legal protection to online hate speech that was guaranteed for offline assaults (Council 2021, European Commission 2022b).

and private actors (e.g., providers and platforms) that concur within hybrid and polycentric legal spaces.

In the following, I will first discuss inter-legality (para. 2) and the main approaches taken towards online hate speech (para. 3). I will then focus on the role of the major big platforms (para. 4) and on the primary hard and soft law on the Internet governance-related issues, an area that is now experiencing a fervent historical moment of change, witnessing States' growing interest in common rules for regulating the Internet, which may have implications for preventing and tackling hate speech too (para. 5, sub-paras. 5.1-5.2.2). While delving into the developments occurred at different decision-making levels, I'll explore viable paths to integrate inter-legality with the purpose to contribute to tackling online hate speech in today's fast-changing and complex legal scenario. I will also provide some suggestions on the first examples of EU Member States' legislations on the topic (sub-para. 5.3). Lastly, I will dedicate the final remarks to reflect on how inter-legality may be furthered in the future.

2. Inter-legality and its potentials for tackling online hate speech

In the theoretical debate on legal pluralism, interlegality was first introduced by Santos in 1987 as the "phenomenological counterpart of legal pluralism" (Santos 1987, p. 298) where different and separate legal orders coexist rather than intersect. On the contrary, by embracing a postmodern conception of law (Santos 1987, pp. 297–299), the scholar conceives "interlegality" (and, consequently, "interlaw") as describing situations of "porous legality or of legal porosity, of multiple networks of legal orders forcing us to constant transitions and trespassings" (Santos 1987, p. 298, Palombella 2019, p. 374; in an anthropological perspective, see Moore 1973).[3] Since individuals are socialised within national legal orders, they may "refuse to recognise as legal those normative orders that use different scales, projections, and symbolisations", which may be perceived as too far away from them (Santos 1987, p. 298). Far from stopping at the descriptive level, the Portuguese scholar suggests developments in two directions. Firstly, sociologists of law should change their priorities and "uncover the latent or suppressed forms of legality in which more insidious and damaging forms of social and personal oppression frequently occur" (Santos 1987, p. 230); secondly, interlegality provides individuals and groups with the opportunity of exploiting the interstices, divergences and contradictions of different orders to counter oppressions "from below" (Santos 2005, p. 29, 2016; cf. Palombella 2019, p. 374).

Italian legal philosopher Gianluigi Palombella departs from Santos's insightful socio-legal elaboration by shifting the focus from legal systems' perspective to that of law, namely "composite law" (Palombella 2019, p. 375), made up of the contents of a plurality of provisions stemming from different sources. In this way, the crucial aspect becomes the relevant law "from the vantage point of the issues under consideration" (Palombella 2019, p. 378; Palombella and Scoditti 2021) in the concrete case (di Martino 2021).

[3] From a legal anthropology perspective, in 1973 Sally Falk Moore introduced the concept of "semi-autonomous social fields" and the lack of autonomy and isolation among them (Moore 1973, p. 722), by examining their capacity to produce rules and persuade or even constrain individuals to conform to them vis a vis other orders' sourced normativity, including State law.

This elaboration involves both a *descriptive* and a *normative* dimension.

At the descriptive level, inter-legality encapsulates in a realistic way, the interconnectedness among international, supranational, national and other legalities, the interference occurring among systems when two or more of them may be simultaneously applied to the same case and suggests viewing "the composite functioning of legality" (Palombella 2019, p. 368) as inter-legality.

At the normative level, this perspective reverses the "top-down" approach characterising Kelsenian theories (Parolari 2021, p. 132) and opts for a "bottom-up" approach by starting from the *concrete case* being reviewed and the relevant (national, supranational, international) legislations it attracts. In doing so, it considers all overlapping and competing legalities that define the law of the concrete case. In this sense, inter-legality promotes a "cultural message" (di Martino 2021, p. 89) of *inclusiveness*.

Also, it has a very pragmatic aim, i.e. the attempt to suggest "a *method* of handling the case" (Chiti *et al.* 2021b, p. 21, my italics) to courts in their interpretation of current intertwined legal provisions. Starting from the concrete case, the law emerges "as the composite legal nature of the issue under scrutiny" (Palombella 2019, p. 379) through an "empirical (…) reconnaissance, in both senses of the term (exploration as well as recognition)" (Palombella 2019, p. 382), rather than an aprioristic and abstract planning. This change of paradigm – from abstract to concrete, from "top-down" to "bottom-up"; from deductive to inductive-empirical – requires a (not easy) change in judges' reasonings too.

They should first recognise the inter-legal situation and, secondly, let it unveil all relevant competing legislations produced by autonomous decision-making powers, which may be applied to the case. As a consequence, such actors – conceived as "interlegality hubs" (Parolari 2021, p. 124, cf. Shany 2019) – should also recognise and consider/include these provisions on an equal footing.

The significance of acknowledging the inter-legality raised by online hate speech lies not only in the current intertwining legalities related to this matter and numerous legal and social actors involved in these spheres but also in the possible *continuum* between online and offline hateful assaults (Ziccardi 2016, Bello 2021) in our "onlife" (Floridi 2015) world.

3. Current approaches to online hate speech

Given the well-known features of online communication (including hate speech) – i.e., transnationality, permanence/persistence and the unpredictable return of content, as well as the perceived Internet users' anonymity (UNESCO 2015, 13–15) – States would need to reach an agreement to prevent and tackle hate speech. Still, this process is problematic because it does not only call into question the traditional understanding of national jurisdiction but also of different perspectives on content (substantively) amounting to legally relevant "hate speech", the extension of "free speech", and the control that needs to be exerted on online contents in order to make the Internet a safe place for all users. These issues are deeply context-related, depending on culture, including legal ones.

National lawmakers and judges have long been struggling to identify a balance between fundamental principles such as dignity and non-discrimination, on the one hand, and freedom of expression, on the other one, in the offline sphere and the challenge now increasingly concerns the online sphere.

With this purpose, scholars tend to contrast the American and European approaches to hate speech (among many others, Post 2009, Kahn 2013, Ziccardi 2016). In the American legal order, a well-established case-law orientation about the First Amendment of the Constitution by the Supreme Court extensively interprets the protection of freedom of religion, speech, press, assembly, and petition in the light of the liberal "Marketplace of ideas" theory sustained by such scholars as John Stuart Mill (1859/1977; cf. Gordon 1997, Lee 2010) and Jeremy Bentham (1821, cf. Cutler 1999). In analogy to the free market for goods and services, this jurisprudence – starting with Judge Oliver Wendell Holmes Jr.'s dissenting opinion in *Abrams v United States* of 1919[4] – affirms the principle that "the best test of truth is the power of the thought to get itself accepted in the competition of the market" and not the opinion of a censor, be it a government or other authority.

This approach is well explained by Elon Musk's statements during the long process of buying and taking over Twitter, ultimately completed in Autumn 2022. During the negotiations to acquire Twitter, the billionaire entrepreneur, who turned from being a highly-followed Twitter user to its owner, announced that he planned to allow for maximum freedom of expression in the platform (Musk 25 April 2022). His statement sparked a variety of reactions, spanning from concerns about the possible increase of hate speech to open support for unlimited free speech (Curwen 2022, Newitz 2022). However, on May 10, 2022, he declared that the forthcoming EU Digital Services Act (EU DSA by European Commission 2022b; *infra*, para. 5.2.2.) was "exactly aligned with [his] thinking" (Musk 10 May 2022; see also Frosio 2022).

In the European context, lawmakers and judges are more prone to admit possible (justified) limitations to hate expressions in consideration of the social consequences that can derive from them, albeit with significant differences between legal systems (Waldron 2012; cf. Ziccardi 2016, 2019, Bello 2021, Bello and Scudieri 2022).

Limiting the analysis to the regulation of the Internet for the purpose of contrasting online hate speech, two orientations can be distinguished. First, the Web is considered as a neutral means of transmitting messages, the contents of which appear simply translated from the real world to the virtual one. Consequently, from a legal point of view, it would not be necessary or useful to intensify the regulation of the Web in order to combat hate speech (Ziccardi 2016, 15–18). This perspective is in line with the general (i.e., not limited to online hate speech) "unexceptionalist" approach to the Internet (Post 2008, p. 889; see, extensively, Fiorinelli 2021). The paradoxical effect produced by an unexceptionalist logic is that "(just about) everything you do on the Web may be subject to (just about) everybody's law" (Post 2008, p. 891) in the world.

On the contrary, according to the second orientation, the Internet can help to facilitate hate speech to favour both new ways of interaction and the spread of the phenomenon;

[4] On the debate about the "clear-and-present danger test", introduced by Judge Holmes in *Schenck v United States* (1919) and reiterated in *Abrams v United States* (1919), see, among many others, and Redish 1982 and Blasi 2020.

therefore, it would be necessary to intervene to control and sanction the contents. This view is consistent with the general "exceptionalist" approach to the Web (Post 2008, 889–891), supporting the opinion that jurisdictional principles developed for the offline space may not be applied to border-crossing interactions.

At their extremes, these two poles can lead to the maximum protection of freedom of expression without prejudice to the protection against only serious forms of hate speech and, alternatively, to the hyper-control and hyper-regulation from which it derives the risk of arbitrary forms of censorship (Ziccardi 2016, 15–18).

Other scholars suggested that private actors should be entitled to regulatory powers adopting "a sort of *lex electronica* (…) regardless of any traditional apparatus" (Fiorinelli 2021, p. 412; cf. Johnson and Post 1996; on the *lex informatica*, which policy-makers should consider to formulate information policy rules, see Reidenberg 1997; on the *lex numerica*, regulating transactions in the cyberspace, see Ost and Van De Kerchove 2002, p. 34).

At the moment, human beings are wrapped in a boundless net of legal relations while simultaneously affiliated with various regulatory systems concerning both the definitions and sanctioning of hate speech as well as the regulation of the Internet in order to prevent and tackle it. In both cases, a fragmented set of binding and non-binding provisions produced by a plethora of decision-making powers – spanning from law-makers to platform owners – intersect in Internet users' lives, including "haters", "targets of hate", and other people who are neither "haters" nor directly targeted by online hate speech but can read, comment on the contents (words or images, like memes), and take stance for one side or the other one.

Given the above-mentioned four features of online hate speech – particularly, the intrinsic "ubiquitous" (Pollicino and Bassini 2014) nature of online communication and the quick spread of contents – this phenomenon urges prompt responses to remove hateful contents, which judges may not warrant. Even though these legal operators remain important "inter-legal hubs" in applying "composite law" to concrete cases of hate speech, their overload of work, and the length and costs of legal proceedings may prevent them from providing such quick responses. As I'll explain, Internet intermediaries play a key role in handling the massive quantity of online content urgently, and they carry various degrees of liability; this may lead to overblocking and collateral censorship that infringes the right to free speech (Wu 2013).

Therefore, it may be suggested that inter-legality as a method may support more and more other legal and even non-legal actors too, spanning from law-makers in elaborating adequate legislation, communications regulatory authorities and even private actors as provider's operators (especially with "first responders"), who are in charge of identifying "hateful contents" rapidly. Obviously, this path needs caution because it requires a thorough legal knowledge of the issue at stake that these "responders" may not rely on. It would be ambitious, at least currently, to envision inter-law (composite law) competences in their case in a short-term perspective, but there might be room to engage them in a long-term perspective. I will elaborate more on these aspects below.

4. Main orientations of large platforms

The providers of large platforms are influential actors in the market and their understanding of free speech – inspired by the US liberal legal culture – does intersect plural legal orders.

As their activities increasingly crossed transnational borders, though, they faced different and even opposed social and legal cultures informed by national constitutional principles. Various national governments and the European Union (EU) have started to pose or impose new obligations upon them, driven by a European approach to the issue (Pollicino and De Gregorio 2019). Each platform's responses towards hateful content differ from one other but, looking diachronically, some phases may be distinguished (Ziccardi 2016).

In the beginning, these large US platforms adopted a non-interventionist approach (Kosseff 2019). At a later stage, they were more prone to remove the most harmful content, draw up guidelines on hate speech aimed at the user community and provided their staff ("first responders") with manuals. These measures soon proved to be too abstract with respect to both the plurality of instances gradually emerging from the "diversity" (including national, cultural and religious) of context in the digital environment and the difficulties met by first responders to handle growing complaints that expressed very different sensitiveness.

The providers then started to adopt policies aimed at combating hate speech towards individuals or groups on the basis of a series of identity categories but not of institutions or countries: for instance, it was not allowed to express "strong" content towards inhabitants of a given country, but it was still possible to do so against the country itself. Facebook launched a further measure to combat online hate speech around 2013, which consisted of a system for identifying the discourse that could cause violence based on four objective standards for determining if a threat is credible: time, place, method and target. If three of these four criteria were met, the company removed "hateful" posts or videos. Google began a similar campaign, while Twitter still decided to remove only content that expressed "direct and specific" threats to individuals or groups (extensively on the evolution of the platforms' approaches, Ziccardi 2016, 90–94).

Platforms' Community Standards have evolved over time to find their own way to balance the contrasting ideas of the freedom of expression and online hate speech in the face of a European approach that was taking shape in a very different way from that American liberal approach (Adler 2011, Rosen 2012, 2016). For instance, Meta established the Oversight Board (Transparency Center n.d.), an external and semi-independent body that handles cases of people who disagree with Meta's content enforcement decisions on Facebook or Instagram.

In the EU context, the European Commission's "soft" initiative to introduce a Code of Conduct to counter the incitement to illegal online hate speech (*infra*, para. 5.2.2.) in 2016 has mediated this process to a certain extent. However, the adoption of the EU DSA in October 2022 will presumably elicit new platforms' orientations. In the current landscape, it will be particularly interesting to observe how Musk's lead of Twitter will cope with forthcoming challenges.

5. International, supranational and national constellations

Tackling online hate speech raises delicate political, legal, regulatory and technological issues concerning the modalities and intensity of Internet governance (Bassini 2019, Ziccardi and Perri 2022). It involves powers and liabilities of various actors, including service providers, in ensuring the protection of fundamental rights of Internet users. The intersecting provisions adopted by different bodies worldwide within the scope of their relative competencies, including States, supranational and international organisations, as well as private actors, shape the complexity of the online space and the unavoidable inter-legality it generates (Kettemann 2020, Fiorinelli 2021).

In this regard, Jack M. Balkin (2018) describes the shift from the dyadic structure of freedom of expression, based on the State-citizen relation, to the triadic one by using the metaphor of the triangle. In one corner of the triangle are Nation-States together with infra-state and supra-state legal orders, while in the second corner are internet-infrastructure (most frequently private) companies. Actors in these corners usually regulate communication on the Internet. In the third corner, at the very bottom, Balkin locates "speakers and legacy media, including mass-media organizations, protesters, civil-society organizations, hackers, and trolls" (Balkin 2018), which may act as agents of change and influence states and infrastructure owners through social activism and protest (Isin and Ruppert 2020, p. 149 ff.).

By looking at the current legal scenario from the perspective of legal and social actors based in the EU countries, it appears to be a dynamic constellation characterised by centripetal trends towards UN-fostered international governance, Council of Europe (CoE) and EU soft and hard legal instruments, co-existing with centrifugal forces of national legislations. However, as for the EU countries, the adoption of the EU DSA is likely to invert the national directions from centrifugal to centripetal and to create a uniform EU legality crossing those deriving from other law-making centres.

Many scholars also point to the proliferation of Internet Bills/Charter of Rights that prove to have few effects, if any (Rodotà 2010, Bassini and Pollicino 2015, Redeker *et al.* 2018, Abba and Alù 2020, Isin and Ruppert 2020). The same criticisms are raised about the Internet Governance Forum (IGF) of the United Nations (UN), which I will discuss shortly.

The process is in the making and may unfold new challenges and opportunities for applying an inter-legal approach to tackling hate speech, which it is worth closely observing in the years to come.

5.1. United Nations: Towards a transnational governance?

Since the beginning of the 2000s, the United Nations has undertaken attempts to call upon States to converge towards "global" rules on matters of Internet governance.

For instance, a two-phased process on the digitally-oriented Information Society[5] was sponsored by the UN between 2003 and 2005. The first World Summit on the Information

[5] "Information Society" commonly refers to the post-industrial society, where information plays a crucial role and has five characterizations: technological, economic, occupational (or sociological, Nath 2009), spatial, and cultural (Webster 2000/2014; cf. Nath 2009; cf. Steinfield and Salvaggio 1989 and Castells 2010).

Society (WSIS),[6] which took place in Geneva on 10–12 December 2003, led to the Declaration of Principles and Action Plan (Geneva Declaration) and the creation of a multi-stakeholders Working Group on Internet governance (WGIG) (WSIS 2003, para. 50), ultimately established by the then Secretary-General Kofi Annan in 2004.[7] The second Summit on the Information Society, organised in Tunis on 16–18 November 2005, led to the Tunis Commitment, the Tunis Agenda for the Information Society (Tunis Agenda; WSIS-UN World Summit on the Information Society 2005a, 2005b) and the creation of the IGF.

The main task of the WGIG was "to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005" (*ibidem*) and deliver the outcomes at the forthcoming WSIS Phase II Summit meeting in 2005.

Apart from developing a working definition of "Internet governance" and pinpointing relevant public policy issues concerning it, the WGIG had to examine the roles and responsibilities of governments, international organisations and other actors, including the private sector and civil society around the world.

The report issued by the WGIG (2005, para. 10) defined the Internet governance as "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet". In doing so, it aimed to strengthen the inclusiveness of all actors in the functioning of Internet governance and to acknowledge their "different interests, roles and participation, which in some cases will overlap" (WGIG 2005, para. 11). This document acknowledges the existence and plausibly conflicting instances of various actors involved in such global governance. At the descriptive level, these intertwining interests may stem from a plurality of legalities/normativities that interplay in a hypothetical concrete case. Given the lack of the converge towards binding global and uniforms rules at the time and, as we'll see, currently, this a place where an inter-legal approach (in its normative dimension) could be applied.

While tackling cybercrimes is addressed by the report, hate speech is not directly mentioned: this may be explained by the general aims of this document and the (still ongoing) disagreement on considering hateful communication as a "crime". Although, the risk of violations of freedom of expression due to security or fighting crime on the Web is considered among public policy issues (WGIG 2005, para. 24). With this idea, the report recalls the Universal Declaration of Human Rights and the aforementioned WSIS Declaration of Principles, which contains several hints to freedom and explicitly addresses the "ethical dimensions of the Information Society" (WSIS 2003, para. 56 ff; on data ethics, see Floridi and Taddeo 2016, Floridi 2018). The Information Society, *inter alia*, should respect the fundamental values of freedom, equality, solidarity and tolerance (*ibidem*) and "foster justice, and the dignity and worth of the human person" (WSIS 2003,

[6] The WSIS United Nations-sponsored summit on Information Society, articulated into two phases, marked respectively by the Geneva Summit in 2003 and the Tunis Summit in 2005, see UN Sustainable Development 2016.

[7] The two-day UN Global Forum on Internet Governance, organised by the UN Information and Communication Technologies Task Force (ICTF) in March 2004, aimed to contributing to create the Working Group on Internet Governance, see UN News 2004.

para. 57). The attempt to balance the protection against hateful content and free speech emerges by, on the one hand, the attention paid to the respect human rights and fundamental freedoms, as well as the right to freedom of thought, conscience, and religion in conformity with relevant international instruments (WSIS 2003, para. 58) and, on the other hand, the preventive measures that all actors in the Information Society should take, under the law, against "illegal and other acts motivated by racism, racial discrimination, xenophobia, and related intolerance, hatred, violence" (WSIS 2003, para 59).

The criteria to combine global cooperation and national interventions were not suggested, nor were they among the WGIG's tasks. The lack of an inter-legal approach in the report surfaces above all about the part dedicated to "Developing a common understanding of the respective roles and responsibilities of all stakeholders from both developed and developing countries" of the WGIG report. In fact, from a global perspective, governments should foster international and regional cooperation and contribute to coordination at the regional and international levels and Treaty-making. At the same time, they should also, among others, develop and adopt laws, regulations and standards; combat cybercrime (which, as said, may include hate speech in some countries, while in others not); and address dispute resolution and arbitration (WGIG 2005, para. 30 ff.).

However, the possible consequences of this gap in terms of – to use the lexicon of inter-legality – paving the way to concrete cases falling under different legal orders were not overlooked by this expert group's line. Thus, the report out-points the "vacuum within the context of existing structures, since there is no global multi-stakeholder forum to address Internet-related public policy issues" (WGIG 2005, para. 40). Consequently, it suggests creating a forum, conceived as a space for multi-stakeholder dialogue on "cross-cutting and multidimensional [issues] and that either affect more than one institution, are not dealt with by any institution or are not addressed in a coordinated manner" (*ibidem*).

Kofi Annan convened the IGF on 18 July 2006, a few months before the end of his last mandate, as one of the results of the Tunis Summit in 2005.

The Tunis Commitment reaffirms "the principle of freedom of expression and the free flow of information, ideas, and knowledge" (para. 3) to be essential for the Information Society, in the same way as the Tunis Agenda, which simultaneously upholds the Ethical Dimensions of the Information Society of the Geneva Declaration.

Regarding the mechanisms and roles of Internet governance, from an inter-legal perspective, it is worth recalling here that States are considered to have the *sovereign right* on and responsibilities for international Web-related public policy issues (para. 35), while intergovernmental and international organisations should remain a "facilitating role in the coordination" (*ibidem*) in this domain and develop "Internet-related technical standards and relevant policies" (*ibidem*). Furthermore, the private sector should continue to be key-actors in the development of the Internet, "both in the technical and economic fields" (*ibidem*). At the same time, civil society is encouraged to keep up its contribution to Internet matters, "especially at community level" (*ibidem*).

Since 2006 the IGF has been the *offline/online space* where the multi-stakeholder dialogue has been developing. Sadly, it has been without remarkable steps towards standard rules or, at least, criteria to coordinate a set of normativities stemming from the polycentric regulatory arena. For a long time, governments have proved reluctant to international regulation and preferred to maintain their decision-making autonomy. This hesitancy could be because they did not consider the Web so dangerous to need such measures or because they believed they were ensuring online market opportunities for national companies in the global market, including the owners of big platforms. As for free speech, possible litigation costs and sanctions for these latter important economic actors, oriented by the "Marketplace of ideas" thought, and the fear of unjustified censorship on the grounds of tackling hateful assaults, have prevented governments from any agreement. Tellingly, a few weeks before the delivery of the WGIG report in 2003, the US claimed the Internet Corporation for Assigned Names and Numbers (ICANN)[8] maintained "its historic role in authori[s]ing changes or modifications to the authoritative root zone file" (McCarthy 2005).

On this point, the WGIG report stressed that Internet governance does not encompass just Web name and address issues (ICANN's tasks); rather, it concerns relevant public policy issues, such as security and safety of the Internet, to mention a few (para. 12). On the contrary, the EU proposed to create a new governing body for the Internet in 2005, which also prompted reactions by the US.

However, over time the fragmentation of regulations at the national level, often conflicting with each other, proved to be an obstacle to business activities even for corporations, including platforms' owners. Moreover, States' awareness of the manifold effects of transnational online communication in relation to hate speech and free speech has increased meanwhile.

This might explain why in 2021, the UN's resumed activities towards a soft governance have managed to convey many States' upsurging interest for this solution, which has implications for tackling hate speech as well.

On 27 April 2021, the High-Level Thematic Debate on Digital Cooperation and Connectivity, organised by the President of the 75th session of the United Nations General Assembly, attempted to identify global governance rules. On this occasion, about 50 countries discussed the Digital Cooperation Road Map ("Road Map") – launched on 11 June 2020 by the UN Secretary General, António Guterres – expressing their interest in identifying common rules for regulating communication in the network. This happened in a historical moment when people's increased online life due to the globally-shared experience of COVID-19 had the twofold effect of showing both the potential and the limits of the Web. The Road Map has the ambitious aim to ensure that

[8] ICANN (Internet Corporation for Assigned Names and Numbers) is a non-profit public-benefit corporation, founded in 1998 and initiated by the US Government with the purpose of transferring the policy and technical management of the Domain Name System (DNS) to a non-profit body based on its territory, with global participation. In October 2016 the coordination and management of the domain name system was entirely transitioned to the private sector (the IANA stewardship transition). The ICANN webpage explains that "[t]he transition isn't the US Government handing over the Internet to any one country, company or group. The truth is that nobody, including the US Government, has a "control of the Internet" to hand over. The community of stakeholders that has flawlessly coordinated the Internet's domain name and addressing systems since their inception will continue to do so" (ICANN n.d.).

every person has safe and affordable Internet access services by 2030 and is part of the multi-stakeholder process started with the IGF in 2006, which plays a crucial role also in this recently started UN initiatives too (IGF n.d.).

In this context, violence and hate speech receive significant attention. For instance, in the 2020 UN Secretary General's Report on the Road Map (A/74/821), paragraphs 51 and 52 of the section "Human rights and Human Agency" underline that women, people who identify or are perceived as LGBTQI+, young people, members of religious groups, and human rights defenders amount to the groups particularly hit by online threats of violence and hate speech, producing inequalities in the online sphere.

The document suggests addressing the problems related to the encryption of messages without hindering the activities of the police and calls upon States and business initiatives to advocate for "frameworks of transparent and responsible governance [accountable] of the contents that protect freedom of expression, avoid incentives to practice of moderation that are excessively restrictive and protect the most vulnerable subjects" (UN Secretary-General 2020, para. 52).

The global digital cooperation, key to the whole process initiated by the Road Map, is considered to be "highly complex and diffused but not necessarily effective" (UN Secretary-General 2020, para. 67) nor inclusive enough. Three potential models can be explored instead: a strengthened and enhanced Internet Governance Forum Plus; a distributed co-governance architecture; and a digital commons architecture (UN Secretary-General 2020, para. 66). This appears to be one of the hardest but urgent topics due to the need to "ensure a comprehensive representation of global voices" (*ibidem*). Member States expressed the idea of working with a multi-stakeholder task force piloting the distributed co-governance model at the national or regional levels (*ibidem*). The conclusive observations call upon States to adopt human rights-based regulatory frameworks and legislation on the development and use of digital technologies and upon technology leaders to recognise the relevance of protecting human rights in the digital sphere and take company-specific actions to do so (UN Secretary-General 2020, para. 87).

The developments of the Road Map are followed with keen interest by legal experts in legal informatics. This interest is not only for the important legal and practical implications that its implementation could entail but also because it represents an epochal turning point compared to the past and is momentous for fostering a change in this field (for the progresses of the Road Map see Guterres 2020). The still soft regulatory framework and practices emerging from this ongoing process may have the impact to orient States to converge on common legislations in the long-term, and, should it be the case, this would decrease the legal complexity that judges, legal and non-legal operators need to handle. At the time being, the soft normativities agreed at this level may concur in the inter-law (composite law) applied to concrete cases by judicial and quasi-judicial bodies. In the same way, they may be considered in the law production and implementation at the national level.

5.2. Council of Europe and European Union: Realms in the making

In the same way as for the substantive law, there is a proliferation of hard and soft law about the Internet governance by the CoE and the EU. In the EU, specifically, there has been a clear shift from soft to binding law.

5.2.1. The Council of Europe: persuading softly

The Convention on Cybercrime of the CoE (ETS No. 185), adopted on May 20, 2001, is the only binding instrument at the international level specifically dedicated to regulating the Internet. It pursues three main aims: a) harmonising the domestic criminal substantive law in the area of cyber-crime, most importantly, for the topic addressed in the present article; b) providing for domestic criminal procedural law powers for allowing investigation and prosecution of these crimes committed by means of computer systems or collect evidence; and c) setting up an effective regime of international co-operation. Article 23 of this Treaty sets the "General principles relating to international co-operation", by calling on States to co-operate with each other to the greatest extent possible regarding "investigations or proceedings concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form of a criminal offence" by applying "relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws". However, criteria on coordinating national legislations are not suggested. The implications of such provision in tackling hate speech concern only those countries that ratified the Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS No. 189) of 2006.

Besides this Treaty, there is a plethora of soft law measures. Here, it is worth recalling the Recommendation on Combating Hate Speech (CM/Rec(2022)16), adopted in May 2022, aimed at preventing and combating offline and online hate speech in a comprehensive way within the framework of the three CoE pillars (human rights, democracy and the rule of law). If compared with previous non-binding documents on this issue, the Appendix "Principles and Guidelines on a Comprehensive Approach to Combating Hate Speech" to this Recommendation identifies detailed measures that States should adopt in relation both to substantive and regulatory profiles of hate speech, including its online manifestations. In doing so, it confirms States' crucial role within the today's horizontal and heterarchical configuration of the Internet.

In fact, in preventing and combating hate speech, the crucial means remain national policies, legislation, strategies or action plans (para. 5). Of course, the Recommendation mentions international standards that this array of national measures should respect, but it is far from formulating coordination criteria in case of conflicting provisions in the concrete cases. It does suggest a common definition of hate speech[9] – that can directly, though "softly", persuade governments to harmonise their national legal definitions –

[9] For the purposes of this recommendation, hate speech is understood as "all types of expression that incite, promote, spread or justify violence, hatred or discrimination against a person or group of persons or that denigrates them by reason of their real or attributed personal characteristics or status such as "race", colour, language, religion, nationality, national or ethnic origin, age, disability, sex, gender identity and sexual orientation" (para. 2).

but it lies with each State to decide "which types of expression fall outside of the protection provided by freedom of expression" (para. 6(a)). It does require that restrictions of the right to freedom of expression comply with Article 10, paragraph 2, of the European Convention on Human Rights and Fundamental Freedoms (ECHR) and the relevant case law of the European Court of Human Rights (ECtHR) (para. 8), but even its judgements can undergo fluctuations.

Also, governments are encouraged to take a comprehensive approach and engage various stakeholders – spanning from public officials, elected bodies and political parties, media, civil society organisations and Internet intermediaries (para. 5 and para. 6(c)). Regarding the duties and responsibilities of State and non-State actors in addressing online hate speech, national provisions should be in accordance with the Recommendation on the Roles and Responsibilities of Internet Intermediaries (CM/Rec(2018)2) (para. 17).[10]

With respect to online hate speech, the Appendix focuses on national provisions on internet intermediaries operating within their jurisdiction, mechanisms for reporting cases, mechanisms in place for the reporting of cases, and removal procedures and the pivotal role of judicial review (paras. 18–27).

In my view, three issues are noteworthy to examine in an inter-legal approach.

Firstly, national legislation should require Internet intermediaries "operating within their jurisdiction" (para. 18) to respect the principles of human rights and due diligence in their activities. In the same way, these latter actors are called upon by the same document to ensure that "human rights law and standards guide their content moderation policies and practices with regard to hate speech" (para. 31). These common principles should orient all States and non-State actors' initiatives and hopefully lead to convergent rules and practices over time, but it remains uncertain and unforeseeable. As a result, with online hate speech being a transnational phenomenon, the Appendix does not seem to solve the problem of co-existing heterogeneous legalities/normativities that may apply to the same concrete case. Therefore, inter-legality may help legal and even non-legal actors to make a conscious effort to consider the legal kaleidoscope.

Secondly, Internet intermediaries may continue to face the challenge of conforming to criteria set by very different national legislation. With this purpose, the Appendix tries to strike a balance between two potentially conflicting interests: on the side of Internet intermediaries, it calls upon States to consider the significant differences in the size, nature, function and organisational structure of these private actors to prevent disparate impacts on smaller ones (para. 21) – an aspect to which the EU DSA more accurately ponders (*infra*, para. 5.2.2); on the side of protection from online hate speech,

[10] For thoroughness, it is worth mentioning para. 7 of the Declaration of the Committee of Ministers on ICANN, Human Rights and the Rule of Law, adopted by the CoE in 2015, concerning the possible infringement of Articles 10 and 11 of the ECHR by prohibiting certain words or characters in domain names and name strings. ICANN should ensure that "when defining access to the use of top-level domains (TLDs), an appropriate balance is struck between economic interests and other objectives of common interest, such as pluralism, cultural and linguistic diversity and respect for the special needs of vulnerable groups and communities". Interestingly, Fiorinelli (2021, p. 409) underlines that in some areas the ICANN seems to take an inter-legal approach, as in the Revised Procedure for Handling WHOIS Conflicts with Privacy Law, 18 April 2017, by considering all concurrent legalities identified by the competent authority; see ICANN 2017.

governments must adopt legislation on many aspects that might have the effect of burdening Internet intermediaries. Among others, national provisions should grant that these private actors "*must* take effective measures to fulfil their duties and responsibilities not to make accessible or disseminate hate speech that is prohibited under criminal, civil or administrative law, (…) rapid processing of reports of such hate speech; removing such hate speech without delay" (para. 22, my emphasis). The translation of this balance into legal terms may vary depending on their different sensitiveness and legal cultures. While the EU DSA will be likely to shape EU Member States' provisions, non-EU countries within the CoE will not be bound by this law. As a consequence, their national legislation may be adapted to CoE soft law in a variety of ways and overlap with other national, supranational and international ones. By centring the focus on the concrete case, all relevant legalities/normativities should be taken into account in the attempt to protect users from hate speech, while ensuring free speech as well.

Besides and leading to the third issue, due to the very characteristics of online hate speech (particularly, their permanence, circulation, and persistence), quick responses to it are urged. Although transparency about the criteria on which decisions related to contents are made should be a crucial point (Gillespie 2018), content moderators and, particularly, first responders who report hateful contents should hold a set of specific competencies allowing them to act expeditiously *and* in compliance with law. Internet intermediaries are asked by the Appendix to appoint enough content moderators and guarantee that they are impartial and hold adequate expertise" (para. 34). While regular training could help develop some skills, handling the complexity of law on this issue, also under time pressure to report, may overwhelm appointees and lead to the aforesaid problem of overblocking and collateral censorship. This issue, raised by the Constitutional Council in France (*infra*, para. 5.3), is indeed worth remembering and being taken "seriously". However, should national legislation adhere to these requirements, then potentially, this could open the flow to integrating an inter-legal "culture" in training modules and daily practices. Furthermore, private employees can certainly commit to the principle of impartiality. Still, it raises many theoretical and practical questions such as the non-obvious meaning of the term, deontology and, not least, unconscious biases (Arango *et al.* 2019). All in all, it seems hardly possible for employers to ensure their staff's impartiality.

As a whole, the Recommendation seems to pay larger attention to intra-State dynamics than to international cooperation. However, the States are encouraged to conform to and effectively implement relevant European and international legislation (para. 63).

5.2.2. The European Union: From soft to binding law

Over time, the EU has undertaken a series of initiatives ranging from soft agreements on codes of conduct with major platforms to hard law, with the view to harmonise Member States' provisions on many aspects of the Internet governance, especially concerning the relations with Internet intermediaries. In doing so, it created an "EU legal space" that impacts the number of potential legalities that each concrete case can attract.

With reference to the former (soft) approach, the European Commission in 2016 agreed with Facebook, Microsoft, Twitter and YouTube on a Code of Conduct to counter the

incitement to illegal online hate speech. Instagram, Snapchat and Dailymotion joined the initiative in 2018, followed by Jeuxvideo.com in 2019. Rakuten, Viber and Twitch[11] announced their participation in Spring 2022. The need to adopt this tool arose due to the (above-mentioned) different US and European approaches to the protection against hate speech and freedom of expression and then introduces rather stringent rules for the North American legal culture to which the major platforms belong. To summarise in terms of contrast measures, these platforms have undertaken a role to prohibit the promotion of an incitement to violence and hate behaviour, adopt effective and timely processes for examining reports related to these phenomena, evaluate reports in the light of the European Union legislation – including, if necessary, the national laws of the member countries that implement the aforesaid Framework Decision (2008/913/JHA) – and promptly remove illegal content. In terms of prevention, the platforms are committed to raising the awareness of their users on hate content.

The implementation of the Code of Conduct is monitored periodically through an agreed methodology and in collaboration with a network of organisations in different EU countries.

The monitoring reports show some positive but non-linear progress over time. According to the last data, on average, the companies are now assessing a high percentage (81%) of flagged content within 24 hours but lower than in 2020 (90.4%). Similarly, the average removal rate of the content considered illegal hate speech remains significant (62.5%), but it has decreased if compared to 2019 and 2020 (Reynders 2021).

For accuracy's sake, the 2022 Strengthened Code of Practice on Disinformation should also be mentioned (European Commission 2022a). It substantially reviews and updates self-regulatory standards to fight disinformation contained in the 2018 Code of Practice on Disinformation (European Commission 2018). The 2022 Code was signed by a broad range of actors (including Meta, Vimeo, Twitter and TikTok) and was presented on 16 June 2022. Signatories are allowed to freely decide to which commitments to subscribe and bear the responsibility to make them effective. To be sure, the Code is not endorsed by the European Commission, which issued the Guidance on Strengthening the Code of Practice on Disinformation on 26 May 2021 (European Commission 2021), setting its expectations about the Code.

However, the EU has meanwhile shifted towards a hard law approach to these procedures and related liabilities.

One step in this direction is represented by Directive 2018/1808 (PE/33/2018/REV/1), which aims, *inter alia*, to guarantee "the effectiveness of self- and co-regulatory measures aiming, in particular, at protecting consumers or public health" (para. 31) and establish "proportionate rules" to protect minors and the general public from harmful audio-visual content and hate speech shared on platforms (para. 45).

For the protection against hate speech, this Directive is relevant not only because it extends some rules to video-sharing platforms and for audio-visual content shared on certain social media services, but also because it strengthens the protection of children

[11] At the substantive level, the shift towards binding law started already with the meaning of illegal hate speech, following the adoption of the Framework Decision on Combating Certain Forms and Expressions of Racism and Xenophobia by Means of Criminal Law (2008/913/JHA) in 2008.

and tackles the issue of hatred in a "more effective" way based on the European approach characterised by greater protection against hate speech than the approach in the US. The providers should be required to take appropriate measures to protect minors from content that may harm their "physical, mental or moral development" and "the general public from content that contains incitement to violence or hatred directed against a group or a member of a group on any of the grounds referred to in Article 21 of the Charter of Fundamental Rights of the European Union (the 'Charter'), or the dissemination of which constitutes a criminal offence under Union law" (Whereas 47).

Member States should also afford out-of-court redress mechanisms for dispute settlement between users and video-sharing platform providers relating to cases under art. 28b, paragraphs 1 and 3. Such procedures should grant impartiality and users' legal protection provided by national law. If alternative dispute resolutions should gain ground in the future, this may be a fruitful, though challenging, place that inter-legality scholars need to explore.

The most recent step (in October 2022) taken by the EU towards the transformation of the legal and regulatory framework of the digital space is the EU DSA (hereafter just "DSA", European Parliament and Council, Regulation 2022/2065), approved by the European Parliament on 5 July 2022 upon the proposal of the European Commission in December 2020 and after a political agreement between the European Parliament and the Council on 23 April 2022.

This agreement was welcomed by the European Commission as "historic" both in terms of substance and procedure (European Commission 2022b). By adopting the DSA, the EU endorses the prevailing State trend to consider illegal online what is illegal offline (*ibidem*; Council 2021). The urgency to adopt this document is obviously generated by the wider Internet users' exposure to online harms, such as the dissemination of illegal content and limitations of fundamental rights and the need to create a uniform legal framework in the EU Member States. It also remedies problems raised from Member States' heterogeneous and disparate legislation and case law concerning the liability of providers, which hinders the functioning of the online market. The process leading to its adoption entailed States' efforts to agree on common rules that inherently concern their understanding of freedom of speech and hate speech too. Scholars pointedly observe that the DSA promotes a "process of constitutionalisation – as well as regulation and institutional governance – of platform responsibility, content moderation and related private ordering practices" (Frosio 2022, p. 4) that might serve as a blueprint for future reform in other jurisdictions.

An in-depth analysis of such a complex text as the DSA goes beyond the purpose of the present contribution, and I will focus here on some innovations that interrogate the inter-legal approach to online hate speech cases.

As it is well known, the broad goal of this piece of law is to contribute to the functioning of the internal market for intermediary services by establishing uniform rules "for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter" (Art. 1), but it may produce relevant consequences for tackling online hate speech too.

For instance, the extent of the notion of "illegal content" seeks to reflect the existing rules in the offline space and encompasses each form of information, including "information relating to illegal content, products, services and activities" (Whereas 12).[12]

The scope of application refers to so-called "information society services", i.e. intermediary services that "have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment" (Art. 2).[13] As a consequence, "territoriality" serves as a framework that allows the EU provisions impact on transnational phenomena line online hate speech.

A thorough list of definitions – such as "content moderators" (Art. 3(t)) – also contributes to preventing possible heterogeneous interpretations of the DSA while, at the same time, making its meaning accessible and intelligible, one of the key factors of effective law.

The DSA does not use a "one size fits all" perspective. Thus, it establishes differentiated and proportionate obligations depending on the type and extent of the service offered by distinguishing among general provisions (Articles 11–15) applicable to all providers. It also sets specific and additional obligations bearing on hosting services, online platforms, online platforms enabling consumers to conclude distance contracts, online platforms of very large size and online search engines of very large size, due to "their special role and reach" (Whereas 48). Further provisions target online platforms (Articles 19–28).

To provide some examples of the implication for tackling hateful, discriminatory content and practices in the EU context, providers must establish a single point of contact to allow recipients to interface directly and fast with them in a user-friendly way, beyond automated tools (chatbots, FAQs, etc.). Users should have the chance to choose the means of communication they prefer (Art. 12(1)). Such measures may allow the most vulnerable targets of hate – i.e., those without or with low digital literacy – to stand for their rights more easily. Moreover, providers' terms and conditions need to inform of any restrictions imposed on users in relation to their services. The information – that needs to be expressed in a clear, understandable, user-friendly and unambiguous language and also made publicly accessible – includes information on "policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system" (Art. 14(1)). These private actors should also act in a "diligent, objective and proportionate manner in applying and enforcing the restrictions (…) with due regard to the rights and legitimate interests of all parties involved" (Art. 14(4)), including fundamental rights such as the freedom of expression and others enshrined in the Charter.

[12] Whereas 12 explains that "illegal content" "should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities".

[13] The DSA distinguishes service of mere conduit service, temporary storage service ("caching") and "hosting" service; and online platforms as online platforms enabling consumers to conclude distance contracts, online platforms of very large size and online search engines of very large size.

Also, under Art. 23, online platforms must suspend offering their services, for a reasonable period, to users who routinely deliver manifestly illegal content after prior notice to them.

Providers of very large online platforms and search engines are bound to follow due diligence obligations related to the assessment and mitigation of systemic risks that may arise and adjust the design of their recommender systems, for example, by taking measures to prevent or minimise *biases* that lead to risks (Whereas 94), a hard to reach goal as discussed in the previous paragraph.

The method chosen by the EU to ensure a safe online space is to place increased obligations and related responsibilities on providers of intermediary services. This choice raises both satisfaction and concern. On the one hand, it imposes the European approach to illegal content, which admits justified limitations of freedom of speech that infringes other fundamental rights and seeks to counter-balance large online platforms' liberal approach above all. On the other hand, the circumstance that very large online platforms primarily bear the responsibility for these tasks and their interpretive sovereignty (Just 2022) poses the question of "what cultural imprint this will inflict on fundamental rights in Europe and what normative values will eventually be accentuated" (*ibidem*).

All in all, the DSA seeks to ensure harmonised measures to effectively safeguard Internet users' fundamental rights and allow them to express themselves freely, while protecting non-discrimination, a balance whose implementation is confronted by many challenges in practice. Creating a common "EU legal space" decreases the complexity raised by EU Member States' heterogeneous approaches that had previously characterised this field. Put simply, the "DSA will be directly applicable across the EU and will apply fifteen months [after] or from 1 January 2024, whichever comes later, after entry into force. Regarding the obligations for very large online platforms and online search engines, the DSA will apply from an earlier date, that is, four months after their designation" (European Commission 2023). As a consequence, this will be EU law overlapping with other pieces of legislation stemming from non-EU legal orders that judicial and quasi-judicial authorities need to consider deciding on concrete cases in the subject matter in an inter-legal perspective.

Lastly and noteworthy, the DSA provides a wide range of possibilities to settle disputes between providers of online platforms and users: internal complaint-handling systems; out-of-court dispute settlement, including those that could not be solved through internal complaint-handling systems in a satisfactory manner; judicial proceedings. Additionally, internal complaint-handling systems should meet the conditions of granting that they are "easily accessible and lead to non-discriminatory, non-arbitrary and fair outcomes, and are subject to human review where automated means are used" (Whereas 58). Lodging complaints should be user-friendly and informal, with no requirement to refer to "relevant legal provisions or elaborate legal explanations" (Ibidem). Similarly, out-of-court dispute settlements by certified bodies must be independent and have the means and expertise to carry out their activities "in a fair, swift and cost-effective manner" (Whereas 59).

Drawing some conclusions on this document, at least three aspects seem relevant for applying an inter-legal approach to online hate speech cases.

Firstly, the illegality of the information or activity results from EU law or national law complying with it (Whereas 12), and, in the coming years, the DSA will intersect other legalities in concrete cases. As mentioned previously, the legal complexity to handle may decrease.

Secondly, given the costs and length of judicial review, the provision of internal complaint-handling systems and out-of-court dispute settlement may ensure reaching fast and, plausibly, cheaper solutions, which may better respond to the urgency of removing hateful content. At the same time, the multiplication of ways to settle disputes requires inter-legality to explore new *loci* where concrete cases will be handled.

Thirdly, in the years to come, it will also be interesting to observe how the European Court of Justice (EUCJ) will position itself. In fact, before the adoption of the DSA, the Luxembourg judges addressed the issue of the possibility for Member States to extend the effects of an injunction worldwide under Directive 2000/31/EC (now amended by the DSA) in the landmark case *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (EUCJ 2019). As Gaia Fiorinelli pointedly underlines, the EUCJ did not prevent States from adopting national measures having extra-territorial effects but "made their legitimacy conditional on compliance with all other possibly applicable rules" (Fiorinelli 2021, p. 432). In this case, the preliminary ruling was requested by the Oberster Gerichtshof (Austrian Supreme Court) in proceedings between Ms. Glawischnig-Piesczek and Facebook Ireland Limited in relation to the publication of a message harmful to her reputation on the page of a hosted user on Facebook. The EUCJ underlines that, in view of the global dimension of electronic commerce (to which the case refers), the EU considered it necessary to adopt consistent rules in that area, applicable at international level. Member States must ensure that their measures that produce effects worldwide "take due account of these rules" (para. 52), opening space to an inter-legal approach.

5.3. Some EU countries' centrifugal forces

In the EU, Germany, France and Austria adopted rather stringent legislation to regulate digital communication with the aim of tackling hate speech, even before the adoption of the DSA, despite the characteristic of any online content to produce simultaneous effects in every other part of the world.

Although the entry into force of the DSA may require adaptations to the legislation adopted at national level and lead to a uniform framework in the EU zone, it is worth analysing them at least for three reasons. None of the national provisions seems to account for the interconnectedness between their legal order and others;[14] at the same time, by enhancing out-of-court dispute settlements (to a different extent though), they show that the courts are not necessarily the only places where inter-legality may provide a method to consider all relevant legalities/normativities applicable to the concrete case, in order to ensure the protection against online hate speech. On a different note, all of the provisions raised concern about risks, such as overblocking and collateral censorship (Dreyer 2020, Eifert *et al.* 2020a, *passim*, 2020b, *passim*; cf. Deutsche Bundesregierung 2020, 21–23, Koltay 2022).

[14] On the contrary, an example in this direction can be found in the US' so-defined "CLOUD Act" (see, insightfully, Fiorinelli 2021, 417-419).

Germany was the first country to take this step by adopting the *Netzwerkdurchsetzungsgesetz* – NetzDG (German Law for the Protection of Rights on Social Networks) on 1 September 2017 (entered into force on 1 October of the same year)[15] (Balkin 2018, Fiano 2021, Peukert 2022). This law is also known as "Facebook-Gesetz" (Facebook-Law) because the restrictive measures introduced appeared to take a strong position towards the well-known platform above, considered too permissive.

The provisions concern the providers of social network platforms with more than two million registered users in Germany (Article 1 (2)) and bind them, among others, to adopt "effective and transparent" procedures for timely removing illegal content and handling complaints. For instance, the removal and blocking of access to obviously illegal content should be carried out within 24 hours of receiving the complaint unless the social network has agreed to a longer period of time with the law enforcement authorities (Article 3(2)(2)).

If the providers receive more than 100 reports on illegal content in a calendar year, they are also required to publish a half-yearly report in German on the handling of complaints which contains the information expressly provided for by Art. 2, including procedures, number of appeals, removal policies and practices, and content removed. The penalties that follow violations due to intentionality or negligence of the legislative prescriptions can reach a very high amount (Art. 4).

While the structure of the law in question has remained unchanged, it was amended repeatedly since its enforcement, for instance, by the Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (German Legislation to Combat Right-Wing Extremism and Hate Crimes) of 30 March 2021. This latest piece of legislation consists of a package of amendments – both substantive and procedural – aimed at protecting public discourse from the effect of hate speech and hate crimes. It entered into force on 1 July 2021 and represented a response to some ideologically motivated verbal and physical violence incidents that occurred in recent years in Germany, including the murder of a governmental district president by Walter Lübcke Kassel. Some commentators have pointed out that the need to adopt the extra measure of amendments shows that the mere removal or blocking of access to hateful content is not enough to stem the violence.

Other changes followed up some suggestions resulting from the first evaluation exercise of the first three years of the law implementation. The report summarising the data collected was published in September 2020, and scholars and practitioners observed the evolutions of the German experiment with particular interest both because it was unprecedented among the EU Member States and because of the assessment, which provided insights for other countries too.

An example relevant to an inter-legal approach to hate speech cases is the introduction of private law institutions – once recognised by an administrative authority referred by the Facebook-Gesetz (Art. 4) – as conciliation bodies for the out-of-court settlement of disputes between complainants or users for whom the content complained of has been

[15] The Law was accompanied by the Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG, Act to Improve Enforcement of the Law in Social Networks) (see the comment by Article 19 2017).

stored and social network providers' decisions concerning particular cases addressed by Art. 3(2), first sentence, numbers 1 to 3 (Art. 3c).

The need for additional out-of-court possibilities for legal action surfaced by the evaluation report that also suggested to facilitate the access to court, by taking into due consideration the psychological impediment and cost-bearing of the persons concerned in referring to a court or a law firm (Eifert *et al.* 2020a, 146–147, 2020b, p. 190 ff.; cf. Deutsche Bundesregierung 2020, p. 42 and p. 46). Interestingly, the document delves into another way to settle dispute, namely the establishment, by network providers, of a neutrality-based private "cyber court", which has not been followed up by the German government. This virtual body should act as an arbitration court (first instance) in providing protection against illegal content on the Web (Eifert and Gostomzyk 2018, p. 169 ff; Eifert *et al.* 2020a, p. 147, 2020b, p. 190). Courts should be as second instance and operate through online, simplified as well as cheap procedures. An example is the afore mentioned Oversight Board established by Meta (*supra*, para. 4).

However, the evaluation report raises the crucial issue of the difficulty of either courts or possible out-of-court mechanism to handle the high number of cases timely (Eifert *et al.* 2020a, p 146 ff.; 2020b), which apparently remains the still unsurmountable challenge of online hate speech cases. These mechanisms are a field of extreme interest for the new places where an inter-legal approach may be applied.

A law similar to the German one was adopted in France on 24 June 2020 – Loi n. 2020-766 visant à lutter contre les contenus haineux sur internet (Law against hateful contents on Internet), better known as "Loi Avia" from the name of the first signatory Laetitia Avia. Most of the text of this law, however, did not pass the constitutionality test by the Conseil Constitutionnel (Dreyer 2020, Siccardi 2021).

The decision raises extremely current profiles that well represent the challenges faced by platform regulations, including the responsibility of the platform operators who were entrusted with the task of viewing all the reported content without the prior intervention of a judge (para. 13). The Council notes that though the reports were numerous, operators were still required to promptly review them in order not to risk incurring penalties (*ibidem*). Besides, they were placed in a position to examine the reported content in the light of numerous criminal provisions to which the Loi Avia referred, even if the constituent elements of some of them presented a legal technicality or required "an assessment of the context of the enunciation or dissemination of the content in question" (para. 14).

Furthermore, the French ruling calls into question the short period of time (24 hours) within which the operators of online platforms were required to assess the manifestly illegal nature of the reported content, however numerous and possibly unfounded (para. 15). A final aspect noted by the Court is the high amount of the sanction in case of failure to comply with the obligation to remove or make inaccessible content manifestly illegal (para. 16).

The last law to be examined is the Austrian Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Federal law on Measures to Protect Users on Communication Platforms), entered into force on 1 January 2021, which aims to foster "the responsible and transparent handling of reports by users (…) on communication

platforms and the prompt handling of such reports" (Art. 1). Apart from certain criteria concerning the providers, many provisions draw inspirations by the German Facebook-Gesetz, such as the transparent communication of information, reporting obligations (Art. 4(1)) and the short time set for the removal and blocking of access to obviously illegal content. The "obviousness" is thought better circumstantiated, requiring that contents' "unlawfulness is already obvious to a legal layman without further without further investigation" (Art. 3(3)(1))).

Differently from Germany and interesting for further developments of an inter-legal approach, since the very beginning alternative dispute resolutions are encouraged regarding complaint procedures. Users thus may lodge claims about the inadequacy of the notification or the review procedures (pursuant, respectively, Art. 3(2)(1-3) and Art. 3(4) of the law to the Beschwerdestelle der Rundfunk und Telekom Regulierungs-GmbH (Complaints Body of the Broadcasting and Telecom Regulation) (see RTR n.d.). However, to access this body, users must have previously contacted the service provider and either have not received an answer back, or were unable to settle the dispute with the platform. The body should try to reach an amicable solution by proposing a solution to the dispute or giving its opinion on it (Art. 7(1)). This two-step procedure appears to be time-consuming if compared to the fast circulation of online hate speech. At the same time, it paves the way to broaden up spaces for applying inter-legality.

6. Final (provisory) remarks

As is often the case with contingent and evolving phenomena and legal/normative fields – like, respectively, online hate speech and Internet governance – final remarks open up space for doubts and questions *in lieu* of conclusions. This happens, even more, when scholars interrogate theories or approaches travelling across disciplines and contexts, as *interlegality* to *inter-legality* does, and seek their way to be *done* in practice rather than being confined to *abstractness*. In this constant and unpredictable flux, in my view, tackling online hate speech represents a challenging – and therefore interesting – area to engage inter-legality in concrete cases. Social and legal changes frequently do not occur simultaneously, especially when their transnational dimension involves a plethora of public and private decision-making powers imbued by different legal cultures and agendas about the protection of fundamental rights.

At the time being, we find ourselves in a fervent phase of promoting soft (UN) and hard (EU) co-regulation within frameworks of defined principles. In addition, there co-exists the CoE hard and soft law provisions, which seem to pay more significant attention to intra-State coordination than inter-States cohesion, although within the framework of the ECHR principles. A few EU Member States exerted their sovereignty through stringent binding law and show both pitfalls and potentials of taking a "territorial" approach to transnational phenomena. At the same time, the EU will act a pivotal "regional" role in the future due to the DSA, which takes a proportionality-driven approach towards platforms in case of violation. Platforms try to cope with the accountability and liability bearing on them for the sake of human rights and to adapt to the various legal scenarios.

At a different level, it is conceivable to outline some areas at which inter-legality scholars will have to look closer in the near future.

Firstly, while access to courts needs to be improved in terms of costs and duration of proceedings and structural overload of cases in some countries, it is unlikely that they will be in the condition to cope with the necessary speed of intervention, even though online hate speech-related cases would be prioritised upon others. However, courts remain the main "interlegality hubs" (Parolari 2021, p. 124) that can recognise and consider/include all provisions relevant to the concrete case so far.

Secondly, the trend seems to converge towards out-of-court dispute settlement. Still, the problem remains of identifying which subjects guarantee adequate knowledge and skills, such as not compromising the fundamental principles at stake. Additionally, establishing an independent governmental agency or authority for regulation, supervision and resolution of disputes between individuals emerges as a viable way to try to reconcile the need for the promptness of protection and competence. In these latter cases, inter-legality may prove helpful and transformative for combating online hate speech also in these still unexplored places. In fact, depending on the types of alternative dispute resolution, this kind of dispute settlement may offer opportunities for dialogue, creativity, inclusiveness and consideration for several aspects that may not be accounted for by courts.

Thirdly, from the perspective of platforms, the risk of being transformed into "judges of first instance" (among many others, Rosen 2012, 2016, Ziccardi 2016) on content has been widely discussed by scholars who warned about the excessive subjective discretion in delegating such assessments to these actors. Besides that, the timeliness of responses by first responders in light of the technologies currently available pressures them to make quick decisions either without or with low legal competencies if compared with the complex legal framework and specific language. In my view, for these very reasons, an inter-legal approach may hardly help this process, but trainings for platforms' staff – foreseen by the DSA – may potentially offer the opportunity to sensitise the need to acknowledge all competing legalities and spread the "cultural message of *inclusiveness*", as Alberto di Martino puts it (2021, p. 89).

Fourthly, if it is true that inter-legality has the very pragmatic aim to suggest "a method of handling the case" (Chiti *et al.* 2021b, p. 21) to courts and, I allow myself to add, to existing and prospective private actors or public bodies settling disputes, it would be significant to spread a "cultural message of *inclusiveness*" to that part of civil society, including lawyers, engaged at the forefront of the fight against hatred.

Lastly, in their hard and soft law, law-makers could – and maybe should – integrate an inter-legal approach to online hate speech, by setting coordination criteria among provisions stemming from a plurality of legal orders or at least encourage the plethora of legal and non-legal actors to take this looking glass to it. The rigidity of law might constrain the creative space of inter-legality in relation to the concrete case, but legal provisions may nonetheless have an awareness-raising function that can empower governments themselves, along with many legal and social actors, to exit the comfort zone of their own particularistic legal culture in today's plural world.

References

Abba, A., and Alù, A., eds., 2020. *Il valore della carta dei diritti di internet*. Naples: Editoriale Scientifica.

Adler, J., 2011. The Public's Burden in Digital Age: Pressures on Intermediaries and the Privatization of Internet Censorship. *Journal of Law and Policy*, 20(1), 231–266.

Arango, A., Pérez, J., and Poblete, B., 2019. Hate Speech Detection is Not as Easy as You May Think: A Closer Look at Model Validation. *SIGIR'19: Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information*, 45–54.

Balkin, J.M., 2018. Free Speech is a Triangle. *Columbia Law Review* [online], 118(7). Available at: https://columbialawreview.org/content/free-speech-is-a-triangle/

Bassini, M., 2019. Fundamental Rights and Private Enforcement in the Digital Age. *European Law Journal*, 25(2), 182–197.

Bassini, M., and Pollicino, O., eds., 2015. *Verso un Internet Bill of Rights*. Rome: Aracne.

Bello, B.G., 2021. I discorsi d'odio in rete. *In*: T. Casadei and S. Pietropaoli, eds., *Diritto e tecnologie informatiche: Questioni di informatica giuridica. Prospettive, istituzionali e sfide sociali*. Padua: Cedam, 247–262.

Bello, B.G., and Scudieri, L., 2022. Discorsi d'odio online. Spunti per un dibattito interdisciplinare. *In*: B.G. Bello and L. Scudieri, eds., *L'odio online: forme, prevenzione e contrasto*. Turin: Giappichelli, 1–18.

Bentham, J., 1821. *On the Liberty of the Press and Public Discussion*. London: William Hone.

Berman, P.S., 2009. The New Legal Pluralism. *Annual Review of Law and Social Science*, 5, 225–242.

Berman, P.S., 2014. *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders*. Cambridge University Press.

Blasi, V.A., 2020. Holmes's Understanding of His Clear-and-Present-Danger Test: Why Exactly Did He Require Imminence? *Seton Hall Law Review*, 51(1), 175–204.

Castells, M., 2010. *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*. Hoboken: Wiley.

Chiba, M., 1989. *Legal Pluralism: Toward a General Theory Through Japanese Legal Culture*. Tokyo: Tokai University Press.

Chiti, E., di Martino, A., and Palombella, G., eds., 2021a. *L'era dell'interlegalità*. Bologna: Il Mulino.

Chiti, E., di Martino, A, and Palombella, G., 2021b. Nel mondo delle legalità al plurale e dell'interconnessione. *In*: E. Chiti, A. di Martino and G. Palombella, eds., *L'era dell'interlegalità*. Bologna: Il Mulino, 9–26.

Commaille, J., and Jobert, B., 1998. Introduction. La régulation politique: l'émergence d'un nouveau régime de connaisance. *In*: J. Commaille and B. Jobert, eds., *Les métamorphoses de la régulation politique*. Paris: LGDJ.

Cotterrell, R., 2014. A Concept of Law for Global Legal Pluralism?. *In*: L. Heckendorn Urscheler and S.P. Donlan, eds., *Concepts of Law: Comparative, Jurisprudential and Social Science Perspectives*. Farnham: Ashgate, 193–208.

Council Framework Decision on Combating Certain Forms and Expressions of Racism and Xenophobia by Means of Criminal Law, 28 November 2008 (2008/913/JHA).

Council of Europe Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, 1 March 2006. *European Treaty Series,* no. 189.

Council of Europe Convention on Cybercrime. 23 November 2001. *European Treaty Series*, No. 185.

Council of Europe Declaration on ICANN, Human Rights and the Rule of Law, 3 June 2015. (Adopted by the Committee of Ministers on 3 June 2015 at the 1229th meeting of the Ministers' Deputies).

Council of Europe Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech. (Adopted by the Committee of Ministers on 20 May 2022 at the 132nd Session of the Committee of Ministers).

Council of Europe Recommendation on the Roles and Responsibilities of Internet Intermediaries (CM/Rec(2018)2). (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies).

Council of the EU, 2021. *What is illegal offline should be illegal online: Council agrees position on the Digital Services Act* [online]. Press release, 25 November. Available at: https://www.consilium.europa.eu/en/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act

Curwen, P., 2022. Must I tweet? If you musk. *Digital Policy, Regulation and Governance* [online], 24(4), 398–399. Available at: http://dx.doi.org/10.1108/DPRG-06-2022-188

Cutler, F., 1999. Jeremy Bentham and the Public Opinion Tribunal. *The Public Opinion Quarterly*, 63(3), 321–346.

Delmas-Marty, M., 1986. *Le flou du droit: Du code pénal aux droits de l'homme*. Paris: Presses Universitaires de France.

Delmas-Marty, M., 2007. *Les forces imaginantes du droit (III): La refondation des pouvoirs.* Paris: Seuil.

di Martino, A., 2021. Dalla regola per il caso al caso della regola. *In*: E. Chiti, A. di Martino and G. Palombella, eds.. *L'era dell'interlegalità*. Bologna: Il Mulino, 65–90.

Dreyer, E., 2020. La censure de la loi Avia par le Conseil constitutionnel. *Légipresse*, 384, p. 412.

Eifert, M., and Gostomzyk, T., eds., 2018. *Netzwerkrecht: Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation.* Baden-Baden: Nomos.

Eifert, M., *et al*., 2020a. *Evaluation des NetzDG: Im Auftrag des BMJV* [online]. Available at: https://www.bmj.de/SharedDocs/Downloads/DE/News/PM/090920_Juristisches_Gutachten_Netz.pdf?__blob=publicationFile&v=1

Eifert, M., *et al*., 2020b. *Netzwerkdurchsetzungsgesetz in der Bewährung. Juristische Evaluation und Optimierungspotenzial.* Baden-Baden: Nomos.

European Commission, 2018. *2018 Code of Practice on Disinformation* [online]. September. Brussels. Available at: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

European Commission, 2021. *Communication on Guidance on Strengthening the Code of Practice on Disinformation* (COM(2021) 262 final) [online]. 26 May. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:262:FIN

European Commission, 2022a. 2022 Strengthened Code of Practice on Disinformation [online]. 16 June. Brussels. Available at: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

European Commission, 2022b. *Digital Services Act: Commission Welcomes Political Agreement on Rules Ensuring a Safe and Accountable Online Environment. Press Release* [EU-DSA] (online). 23 April. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545

European Commission, 2023. *The Digital Services Act package* [online]. 23 January. Brussels. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

European Parliament and Council Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on electronic commerce), 8 June 2000.

European Parliament and Council Directive 2018/1808 amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities, 14 November 2018 (PE/33/2018/REV/1). *Official Journal*, L 303, 28.11.2018, 69–92.

European Parliament and Council Regulation 2022/2065 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act, EU DSA), 19 October 2022.

Fiano, N., 2021. Il linguaggio dell'odio in Germania: tra *wehrhafte Demokratie* e *Netzwerkdurchsetzungsgesetz*. *In*: M. d'Amico and C. Siccardi, eds., *La Costituzione non odia. Conoscere, prevenire e contrastare l'hate speech on line*. Turin: Giappichelli, 155–164.

Fiorinelli, G., 2021. Ordinamenti interconnessi. Il contributo dell'interlegalità alla regolazione della rete. *In*: E. Chiti, A. di Martino and G. Palombella, eds., *L'era dell'interlegalità*. Bologna: Il Mulino, 405–440.

Fischer-Lescano, A., and Teubner, G., 2004. Regime-Collisions: The Vain Search for Legal Unity in the Fragmentation of Global Law. *Michigan Journal of International Law* [online], 25(4), 999–1045. Available at: https://repository.law.umich.edu/mjil/vol25/iss4/12?utm_source=repository.law.umich.edu%2Fmjil%2Fvol25%2Fiss4%2F12&utm_medium=PDF&utm_campaign=PDFCoverPages

Floridi, L., ed., 2015. *The Onlife Manifesto. Being Human in a Hyperconnected Era* [online]. Cham: SpringerOpen. Available at: https://link.springer.com/book/10.1007/978-3-319-04093-6

Floridi, L., 2018. Soft Ethics and the Governance of the Digital. *Philosophy & Technology* [online], 31, 1–8. Available at: https://link.springer.com/article/10.1007/s13347-018-0303-9

Floridi, L., and Taddeo, M., 2016. What is Data Ethics? *Philosophical Transactions of the Royal Society A* [online], 374, 1–5. Available at: https://doi.org/10.1098/rsta.2016.0360

Frosio, G., 2022. Platform Responsibility in the Digital Services Act: Constitutionalising, Regulating and Governing Private Ordering. *Queen's University Belfast Law Research Paper*, 1–21. Available at: https://ssrn.com/abstract=4236510

Furnivall, S., 1939. *Netherlands India: A Study of Plural Economy*. Cambridge: University Press; New York: Macmillan Company.

Gillespie, T., 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media.* London: Yale University Press.

Gordon, J., 1997. John Stuart Mill and the "Marketplace of Ideas." *Social Theory and Practice*, 23(2), 235–249.

Grossi, P., 2002. Globalizzazione, diritto, scienza giuridica. *Il Foro Italiano*, 125(5), 151–164.

Guterres, A., 2020. *Secretary-General's Roadmap for Digital Cooperation* [online]. United Nations. Available at: https://www.un.org/en/content/digital-cooperation-roadmap/

Internet Corporation for Assigned Names and Numbers (ICANN), 2017. *Revised ICANN Procedure For Handling WHOIS Conflicts with Privacy Law* [online]. 18 April. Available at: https://www.icann.org/en/system/files/files/whois-privacy-conflicts-procedure-redline-18apr17-en.pdf

Internet Corporation for Assigned Names and Numbers (ICANN), no date. *The IANA stewardship transition: What you need to know* [online]. Available at: https://www.icann.org/iana-transition-fact-sheet

Isin, E., and Ruppert, E., 2020. *Being Digital Citizens*. 2nd ed. Lanham: Rowman & Littlefield International.

Itzcovich, G., 2012. Legal Order, Legal Pluralism, Fundamental Principles. Europe and Its Law in Three Concepts. *European Law Journal*, 18(3), 358–384.

Johnson, D.R., and Post, D., 1996. Law and Borders. *Stanford Law Review*, 48(5), 1367–1402.

Just, N., 2022. The Taming of Internet Platforms – A Look at the European Digital Services Act. Competition Policy International (CPI), 15 June.

Kahn, R., 2013. Why Do Europeans Ban Hate Speech? A Debate Between Karl Loewenstein and Robert Post. *Hofstra Law Review*, 41(3), 545–585.

Kahn, R., *et al.*, 1997. The Evolution of the Internet as a Global Information System. *International Information & Library Review*, 29(2), 129–151.

Kettemann, M.C., 2020. *The Normative Order of the Internet: A Theory of Rule and Regulation Online*. Oxford University Press.

Koltay, A., 2022. The Protection of Freedom of Expression from Social Media Platforms. *Mercer Law Review* [online], 73(2), 523–588. Available at: https://digitalcommons.law.mercer.edu/jour_mlr/vol73/iss2/6?utm_source=digitalcommons.law.mercer.edu%2Fjour_mlr%2Fvol73%2Fiss2%2F6&utm_medium=PDF&utm_campaign=PDFCoverPages

Kosseff, J., 2019. *The Twenty-Six Words That Created the Internet.* Ithaca: Cornell University Press.

Lee, S.P., 2010. Hate Speech in the Marketplace of Ideas. *In*: D. Golash, ed., *Freedom of Expression in a Diverse World.* London/New York: Springer, 13–25.

Mancini, L., 2015. *Introduzione all'antropologia giuridica*. Turin: Giappichelli.

McCarthy, K., 2005. UN outlines future of US-less internet WGIG provides four models. *The Register* [online], 15 July. Available at: https://www.theregister.com/2005/07/15/un_wgig_report/

Mill, J.S., 1977. On Liberty. *In*: J.M. Robson *et al*., eds., *Collected Works of John Stuart Mill.* University of Toronto Press, 18. (Originally published in 1859).

Moore, S.F., 1973. Law and Social Change: The Semi-Autonomous Social Field as an Appropriate Subject of Study. *Law & Society Review*, 7(4), 719–746.

Musk, E. [@elonmusk], 10 May 2022. Great meeting! We are very much on the same page. [Answer to the European Commissioner Thierry Breton, @ThierryBreton]. *Twitter* [online], 10 May. Available at: https://twitter.com/elonmusk/status/1523798885205876736

Musk, E. [@elonmusk], 25 April 2022. [Tweet]. *Twitter*, 25 April.

Nath, H.K., 2009. The Information Society. *SIBCOLTEJO – A Journal of the SCTU* [online], vol. 4, 19–29. Available at: https://www.shsu.edu/eco_hkn/The%20Information%20Society.pdf

Newitz, A., 2022. The US Myth of Free Speech. *New Scientist*, 254(3388), 28.

Ost, F., 2013. Dalla piramide alla rete. Un nuovo paradigma per la scienza giuridica?. *In*: M. Vogliotti, ed., *Saggi sulla globalizzazione giuridica e il pluralismo normativo. Estratti da "Il tramonto della modernità giuridica. Un percorso interdisciplinare"*. Turin: Giappichelli, 31–37.

Ost, F., and van De Kerchove, M., 2000. De la pyramide au réseau ? Vers un nouveau mode de production du droit ? *Revue interdisciplinaire d'études juridiques* [online], 44(1), 1–82. Available at: https://www.cairn.info/revue-interdisciplinaire-d-etudes-juridiques-2000-1-page-1.htm

Ost, F., and van De Kerchove, M., 2002. *De la pyramide au réseau? Pour un théorie dialectique du droit*. Brussels: Fusl.

Palombella, G., 2018. Interlegalità. L'interconnessione tra ordini giuridici, il diritto, e il ruolo delle corti. *Diritto & Questioni Pubbliche* [online], 18(2), 315–342. Available at: http://www.dirittoequestionipubbliche.org/page/2018_n18-2/11-studi_Palombella.pdf

Palombella, G., 2019. Theory, Realities, and Promises of Inter-Legality. A Manifesto. *In*: J. Klabbers and G. Palombella, eds., *The Challenge of Interlegality.* Cambridge University Press, 363–390.

Palombella, G., and Scoditti, E., 2021. L'interlegalità e la ragion giuridica del diritto contemporaneo. *In:* E. Chiti, A. di Martino and G. Palombella, eds., *L'era dell'interlegalità.* Bologna: Il Mulino, 29–64.

Parolari, P., 2020. *Diritto Policentrico e interlegalità nei paesi europei di immigrazione: Il caso degli shari'ah councils in Inghilterra*. Turin: Giappichelli.

Parolari, P., 2021. L'interlegalità come metodo? La decisione giudiziale negli spazi ibridi. *In*: E. Chiti, A. di Martino and G. Palombella, eds., *L'era dell'interlegalità*. Bologna: Il Mulino, 119–135.

Pastore, B., 2017. Sul disordine delle fonti del diritto (inter)nazionale. *Diritto & Questioni pubbliche* [online], 17(1), 13–30. Available at: http://www.dirittoequestionipubbliche.org/page/2017_n17-1/DQ17-2017-1_03-mono_1_02_Pastore.pdf

Peukert, A., 2022. *Das Netzwerkdurchsetzungsgesetz: Entwicklung, Auswirkungen, Zukunft* [online]. Arbeitspapier, Fachbereich Rechtswissenschaft. Goethe-Universität Frankfurt am Main. Available at: https://www.nomos-elibrary.de/10.5771/9783748932741-229.pdf

Pollicino, O., and Bassini, M., 2014. The Law of the Internet between Globalisation and Localisation. *In*: M. Maduro, K. Tuori and S. Sankari, eds., *Transnational Law: Rethinking European Law and Legal Thinking*. Cambridge University Press, 346–380.

Pollicino, O., and de Gregorio, G., 2019. A Constitutional-Driven Change of Heart: ISP Liability and Artificial Intelligence in the Digital Single Market. *The Global Community Yearbook of International Law and Jurisprudence*, 18(1), 237–264.

Post, D.G., 2008. Governing Cyberspace: Law. *Santa Clara High Technology Law Journal*, 24(4), 883–913.

Post, R., 2009. Hate Speech. *In*: I. Hare and J. Weinstein, eds., *Extreme Speech and Democracy*. Oxford University Press.

Radu, R., 2019. *Negotiating Internet Governance*. Oxford University Press.

Raustiala, K., 2016. Governing the Internet. *American Journal of International Law*, 110(3), 491–503.

Redeker, D., Gill, L., and Gasser, U., 2018. Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights. *International Communication Gazette*, 80(4), 302–319.

Redish, M.H., 1982. Advocacy of Unlawful Conduct and the First Amendment: In Defense of Clear and Present Danger. *California Law Review*, 70(5), 1159–1200.

Reidenberg, J.R., 1997. Lex Informatica: The Formulation of Information Policy Rules Through Technology. *Texas Law Review*, 76, 553–593.

Reynders, D., 2021. *6th Evaluation of the Code of Conduct. Factsheet* [online]. European Commission, Directorate-General for Justice and Consumers, 7 October. Available at: https://ec.europa.eu/commission/presscorner/detail/en/fs_21_5106

Rodotà, S., 2010. Una Costituzione per Internet?. *Politica del diritto*, 41(3), 337–351.

Rosen, J., 2012. The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google. *Fordham Law Review*, 80(4), 1525–1537.

Rosen, J., 2016. *The Deciders: The Future of Free Speech in a Digital World* [online]. 21 October. Available at: https://shorensteincenter.org/jeffrey-rosen-future-of-free-speech-in-a-digital-world/

RTR, no date. *Die Beschwerdestelle* [online]. Vienna: RTR. Available at: https://www.rtr.at/medien/was_wir_tun/Beschwerdestelle/Startseite_Beschwerdestelle.de.html

Santos, B. de S., 1987. Law: A Map of Misreading. Toward a Postmodern Conception of Law. *Journal of Law and Society*, 14(3), 279–302.

Santos, B. de S., 2005. Beyond Neoliberal Governance: The World Social Forum as Subaltern Cosmopolitan Politics and Legality. *In*: B.S. Santos and C.A. Rodríguez-Garavito, eds., *Law and Globalization from Below*. Cambridge UK and New York: Cambridge University Press, 29–63.

Santos, B. de S., 2016. Epistemologies of the South and the future. *From the European South*, 1, 17–29.

Scamardella, F., 2021. La *governance*: genesi, diffusione e disavventure di un lemma fortunato. *Rivista di filosofia del diritto*, 1, 11–32.

Shany, Y., 2019. International Courts as Inter-Legality Hubs. *In*: J. Klabbers and G. Palombella, eds., *The Challenge of Inter-Legality (ASIL Studies in International Legal Theory*, 319–338.

Shapiro, M., 1993. The Globalization of Law. *Indiana Journal of Global Legal Studies*, 1(1), 37–64.

Siccardi, C., 2021. La Loi Avia. La legge francese contro l'odio on line (o quello che ne rimane). *In*: M. d'Amico and C. Siccardi, eds., *La Costituzione non odia. Conoscere, prevenire e contrastare l'hate speech on line*. Turin: G. Giappichelli, 167–183.

Steinfield, C., and Salvaggio, J.L., 1989. Toward a Definition of the Information Society. *In*: J.L. Salvaggio (ed.), *The Information Society: Economic, Social, and Structural Issue*. Hillsdale, NJ: Lawrence Erlbaum Associates, 1–14.

Transparency Center, no date. *Oversight Board* [online]. Menlo Park: Meta. Available at: https://transparency.fb.com/it-it/oversight

UN News, 2004. *Experts meet at UN to examine Internet regulation* [online]. 25 March. Available at: https://news.un.org/en/story/2004/03/98332

UN Secretariat of the Internet Governance Forum (IGF), no date. *The IGF and UN Processes* [online]. Geneva: IGF. Available at: https://www.intgovforum.org/en/content/the-igf-and-un-processes

UN Secretary-General, 2020. *Report of the Road Map for Digital Cooperation: Implementation of the Recommendations of the High-level Panel on Digital Cooperation*, 29 May 2020 (A/74/821).

UN Sustainable Development, 2016. *World Summit on the Information Society (WSIS)* [online]. UN. https://sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=102&menu=3170

UNESCO, 2015. *Countering Online Hate Speech*. Geneva: UNESCO.

Waldron, J., 2012. *The Harm in Hate Speech*. Cambridge, MA: Harvard University Press.

Webster, F., 2014. *Theories of the Information Society*. London: Routledge. (Originally published in 2000).

WGIG-Working Group on Internet Governance, 2005. *Report of the Working Group on Internet Governance* [online]. Available at: http://www.wgig.org/docs/WGIGREPORT.pdf

WSIS-UN World Summit on the Information Society, 2003. *Declaration of Principles and Action Plan*, 12 December 2003 (WSIS-03/GENEVA/DOC/0004).

WSIS-UN World Summit on the Information Society, 2005a. *Tunis Agenda for the Information Society*, 18 November 2005 (WSIS-05/TUNIS/DOC/6(Rev 1)-E).

WSIS-UN World Summit on the Information Society, 2005b. *Tunis Commitment*, 18 November 2005. (WSIS-05/TUNIS/DOC/7-E).

Wu, F.T., 2013. Collateral Censorship and the Limits of Intermediary Immunity. *Notre Dame Law Review*, 87(1), 293–349.

Ziccardi, G., 2016. *L'odio online: Violenza verbale e ossessioni in rete*. Milan: Raffaello Cortina.

Ziccardi, G., 2019. Le espressioni d'odio online. *In*: G. Ziccardi and P. Perri, eds., *Tecnologia e Diritto*. Milan: Giuffrè Francis Lefevbre, 153–177.

Ziccardi, G., and Perri, P., 2022. L'odio online tra profilazione, big data e protezione dei dati personali. *In*: B.G. Bello and L. Scudieri, eds., *L'odio online: forme, prevenzione e contrasto*. Turin: Giappichelli, 91–106.

National legal sources

France

Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet (Loi Avia) [online]. Available at: https://www.legifrance.gouv.fr/eli/loi/2020/6/24/JUSX1913052L/jo/texte

Germany

Deutsche Bundesregierung, 2020. *Bericht zur Evaluierung des Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG)* [online]. Available at: https://www.bmj.de/SharedDocs/Downloads/DE/News/PM/090920_Evaluierung_NetzDG.html

Deutsches Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, 30 March 2021.

Deutsches Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG), 1 September 2017.

Deutsches Netzwerkdurchsetzungsgesetz – NetzDG, 1 September 2017.

Austria

Österreichisches Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Gesamte Rechtsvorschrift für Kommunikationsplattformen-Gesetz) (Kommunikationsplattformen-Gesetz – KoPl-G), 17 December 2020.

Case law

Conseil Constitutionnel n. 2020-801 DC du 18 juin 2020.

EUCJ-European Court of Justice, C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, 3 October 2019 (ECLI:EU:C:2019:821).

US Supreme Court, *Abrams v United States*, 250 U.S. 616 (1919; dissenting).

US Supreme Court, *Schenck v United States*, 249 U.S. 47 (1919).