Comparative Study Of Best European Practices Of Online Content Regulation

Law and policy of online content regulation, in particular defamation online, in the light of Albanian legislative proposals

Kristina Irion
Paolo Cavaliere
Darian Pavli

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

COMPARATIVE STUDY OF BEST EUROPEAN PRACTICES OF ONLINE CONTENT REGULATION

Law and policy of online content regulation, in particular defamation online, in the light of Albanian legislative proposals

AUTHORS

KRISTINA IRION | PAOLO CAVALIERE | DARIAN PAVLI

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Authors

Dr Kristina Irion	Institute for Information Law at the University of Amsterdam (NL)
Dr Paolo Cavaliere	Edinburgh Law School, University of Edinburgh (UK)
Darian Pavli	Adviser to Special Parliamentary Committee on Justice Reform, Open Society Foundation for Albania/ Parliament of Albania

Disclaimer

The opinions expressed in this work reflect the authors' own views and not of their affiliations nor of the Council of Europe.

Citation

Irion, K., Cavaliere, P., and Pavli, D. 2015. *Comparative study of best European practices of online content regulation. Law and policy of online content regulation, in particular defamation online, in the light of Albanian legislative proposals.* Study commissioned by the Council of Europe, Amsterdam/ Edinburgh/ Tirana, August 2015.

© Council of Europe 2015

Printed by the Council of Europe

Executive Summary

With the advent of the Internet a new public sphere has come into being that has changed modes of creation and consumption of media content where new actors offer online services and individual users can receive and impart information regardless of frontiers. New media and user-generated content greatly enhance the diversity and plurality of online content and allow an unprecedented parallelism of professional and journalistic content and individual speech empowering individual citizens and ordinary users.

PART I - European best practices of online content regulation

European best practices of online content regulation rest on the shared understanding of the Council of Europe and the European Union institutions to protect the freedom of expression online of all actors. First and foremost, communications via the Internet should not be subject to any stricter content rules than other spheres of expression, thus reaffirming the overarching principle that state interventions into the right to freedom of expression and media freedoms in particular must meet the requirements of strict necessity, minimum intervention, and the protection of from unduly interference.

In recognition of the different roles and activities of actors in the new media environment the Council of Europe promotes a ***graduated and differentiated approach*** in state legislation that encompasses ***a new broad notion of the media***. This approach requires that "each actor whose services are identified as media or as an intermediary or auxiliary activity benefit from both the appropriate form (differentiated) and the appropriate level (graduated) of protection" in addition to individuals' right to freely seek and impart information regardless of frontiers. The European Union policy and legislation takes a similar direction providing for tailored liability exceptions for certain online intermediaries.

State actions that aim to protect individuals' personality rights, their reputation and private life, should correspond with these principles and the case-law of the European Court of Human Rights which together outline a coherent and comprehensive frameworks for the regulation of online content at the national level. The respect of individuals' right to reputation and private life can be a legitimate limitation to the freedom of expression, however, measures should be calibrated according to the roles and activities of the actors in the provision of content and the interference must be balanced taking into account the type of speech, the role of the actors involved, the political relevance and public interest, among others.

European best practice thus forestall any one-size-fits-all measures against defamatory online content

and need to be flexible so as to take into account the particular circumstances of the expression and personal characteristics of the parties concerned. Under a graduated and differentiated approach, internet intermediaries' responsibility for hosting online content of third parties has to be determined according to the specific nature of the service they offer. The Council of Europe standard-setting documents and EU legislation provide for a ***limitation of liability and exclude a specific duty to monitor*** the information they receive from users on part of hosting providers which in their role and function remain passive service providers.

The European Court of Human Rights Grand Chamber judgement in *Delfi v Estonia* concerns a case where the defendant played an active role in facilitating the posting of unlawful third-party comments and was thus treated like a "professional" publisher with all responsibilities for the content on its website. This judgement, however, does not overturn the principle that "passive" online intermediaries that provide for the hosting services would not be liable for third party content. Despite the differences of jurisprudence at the national level and with the notable exception of Turkey, European countries' legislation does not establish a general liability regime for providers of hosting services.

PART II - Albania and online content regulation

Against the background of European best practices in online content regulation, the study considered in particular a pending legislative proposal in Albania which seeks to introduce "liability for online publication of comments that infringe upon a person's honour, personality or reputation" on providers of "electronic portals". The study's assessment of the proposal concludes that it conflicts with the graduated and differentiated approach promulgated by the relevant CoE standard-setting instruments, vastly exceeds the ECtHR interpretation in the *Delfi* judgement and would clash with the EU *aquis,* particularly with Art. 14 and 15(a) of the e-Commerce Directive.

In light of the above considerations, the necessity of a legislative intervention in Albania at this time, along the lines of the Bregu proposal, appears less than compelling. It may be more advisable, as in the Estonian *Delfi* case which was based on the general civil law defamation rules, to allow the courts to develop more nuanced rules in this field, under the guidance of the ECtHR. With the exception of England and Wales, which undertook in 2013 long-planned, comprehensive reforms of their defamation laws, no other EU member state has adopted specific laws for online defamation. This has allowed their court systems to gradually develop the case law, taking account of fast changes in technology, information ecosystems and societal attitudes.

If enacted this legislation would retrograde the advancements made with the 2012 reforms to the Albanian civil and criminal defamation laws, introduce an unorganic and unbalanced measure directed against all content and hosting providers that is excessively restraining the freedom of expression online.

In particular, the study identifies the following shortcomings:

1. The definition of "electronic portal" to overly broad, thus capturing "passive" intermediaries contrary to European best practices and the EU *aquis*; the definition does also not allow for taking

into account the defining characteristics of the service but automatically places the obligations of "active" intermediaries on all providers;

2. To the extent that "passive" intermediaries would be regulated the proposal contradicts with Art. 17 of the Albanian ECA which provides for a liability exception for hosting services analogue to Art. 14 of the EU e-Commerce Directive;

3. The obligation on portal administrators to prevent the publication of any offending third-party content amounts to a duty to monitor information contrary to the EU *aquis*;

4. The obligation would appear to apply horizontally to all providers of "electronic portals" irrespective whether they are established in Albania or abroad but the proposal does not include issues of jurisdiction or consider practicalities of extraterritorial enforcement.

5. This in turn can amount to a violation of Art. 3 (2) of the e-Commerce Directive because it would alter the requirements for providers established in another member state within the coordinated field of activities;

6. The general obligations for the content and the take-down procedure do not allow for a balancing exercise taking into account the type of speech, the role of the actors involved, the political relevance and public interest, among others, pursuant to the established case-law of the ECtHR;

7. The legislative proposal lacks procedural safeguards, in particular that courts should primarily assess whether online content is infringing third party's reputation, or at least which requirements the notice has to comply with and other rights and means to assess and protest the notice; and

In light of the above considerations, the study recommends the Albanian legislator not to adopt this legislative proposal. It should be recalled that the Estonian *Delfi* case was based on the general civil law defamation rules and not on dedicated piece of legislation placing a general obligation on providers of hosting services for all published content, irrespective whether this is own or third party content and the provider's activities are passive intermediary or rather media/ "active" intermediary. In light of the fundamental right to the freedom of expression and the recommended nuanced approach Albanian decision-makers should allow the courts to develop case-law, under the guidance of the ECtHR, based on the criteria in Art. Art. 647/a of the civil code.

In order to communicate how the present legal framework applies to the situation of hosting providers it is recommended:

1. to disseminate this study widely to all stakeholders;

2. to organize a workshop for policy-makers and stakeholders covering the legislative status quo in Albania against the backdrop of European best practices and developments in the case law of the European courts; in particular the workshop should aim to convey the qualified requirements promulgated in the ECtHR *Delfi*-judgement;

3. to organize a workshop for judges on the case law of the ECtHR and the CJEU relevant to defamatory content online, in particular how both courts balance the infringement of individual's

reputation and other rights with the freedom of expression online;

4. to promote self-regulation of hosting providers and assist with an overview of best practices and measures deployed by local and foreign hosting providers;

5. to educate the public about already available remedies in Albanian law against online defamation, infringement of privacy and other unlawful content. These include the hardly used notice-and-takedown system of the Albanian ECA.

6. to set-up a dedicated website to promote the public awareness of individual user's possible remedies against online defamation, infringement of privacy and other unlawful content. Inter alia, this website should provide an accessible overview over the mechanisms deployed by the most commonly used hosting providers in Albania and links to their reporting tools and notice-and-action schemes.

TABLE OF CONTENTS

TABLE OF ANNEXES

Albanian legislation relevant to online content regulation, in particular defamation laws, and hosting intermediaries liability for third party comments

ABBREVIATIONS

Art.	Article
AVMS	Audiovisual media services
CC	Civil Code (national law of Albania)
CFR	The Charter of Fundamental Rights (CFR) of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECA	European Commerce Act (national law of Albania)
EU	European Union
ISP	Internet Service Provider
MP	Member of Parliament
Para.	Paragraph
PC	Penal Code (national law of Albania)

Introduction

The advent of the Internet and, in particular, of Web 2.0, has changed modes of both, creation and consumption of media content, and consequently challenged consolidated assumptions about legal safeguards for the right to freedom of expression that is protected as a fundamental right by core human rights instruments at the European regional level and in European states' constitutions.[1] On the one hand, Internet-mediated communications and publishing are heralded as enablers for the exercise of freedom of expression which allow greater participation in the public discourse. A new public sphere has come into being that challenges former gatekeeper positions which required access to distribution infrastructure and/ or substantial resources for content production characteristic of traditional media, such as the press and broadcasting media, where new actors offer online services and individual users can receive and impart information regardless of frontiers. New media and user-generated content greatly enhance the diversity and plurality of online content and allow an unprecedented parallelism of professional and journalistic content and individual speech empowering individual citizens and ordinary users.

The boost for the exercise of the freedom of expression is a most welcome and positive development as recognised in numerous documents by the Council of Europe and the European Union. The practice however also shows that the exercise of the freedom of expression online can at times interfere with individuals' reputation or rights of others, among other issues. Striking the right balance between conflicting positions of rights while keeping state interventions minimal is thus not less important in Internet communications as it was in the context of traditional media and individual speech. The Council of Europe maintains that communication on the Web should not be subject to any stricter content rules or restrictions than any other medium[2] and that state interventions into the right to freedom of expression and media freedoms in particular should be guided by similar general regulatory principles irrespective whether or not professional media outlets, intermediaries or individual users are involved.

It its standard-setting work the Council of Europe has given much attention to the protection of freedom of expression in the new media environment which has clearly been a focal point of its activities in recent years. The 2007 Recommendation of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment[3] recommends guidelines which rest on the empowerment of private users, the accessibility of ICT infrastructure and information, and international common standards to foster content creation and cooperation among stakeholders.

The rich body of case law of the European Court of Human Rights (ECtHR) on how to balance the freedom of expression with the reputation and rights of others offers ample guidance as to how to

1. *Notably in Art 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms; Art 11(1) of the Charter of Fundamental Rights (CFR) of the European Union.*

2. *Declaration on freedom of communication on the Internet, adopted by the Committee of Ministers on 28 May 2003. Cf. Principle 1: "Member states should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery."*

3. *CM/Rec(2007)11, adopted by the Committee of Ministers on 26 September 2007.*

resolve conflicting positions of rights. The most actual ECtHR decision in *Delfi v Estonia* contributes an important piece to the legal puzzle under which circumstances an Internet news portal can be liable for user comments which even cross the boundary of defamatory content but are deemed hateful and racist.[4] This decision and also the 2014 Court of Justice of the European Union (CJEU) decision in the case *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* which finds in favour of a right to be delisted from a search engine's list of result following a search based on an individual's name[5] have sparked much controversy. However, upon closer reading these cases are not framing a general liability regime of Internet Service Providers (ISPs) but formulate specific legal requirements which have to be met in order to rely on either judgement. The case law does not lent itself to argue for the introduction of a general secondary liability of ISP for third party content. Their reading and interpretation should be placed in light of the overarching principles on the protection of freedom of expression online as devised by the Council of Europe, among others.

As part of the project "Promoting freedom of expression and information and freedom of the media in South-East Europe (SEE)" the Council of Europe commissioned this comparative study of best European practices of online content regulation, in particular defamation online. This study seeks to inform legislators, policy-makers, traditional and new media organisations as well as civil society about European standards and best practices in online content regulation and seeks to promote proportionate measures to protect individuals' reputations and personality rights. The study proceeds in two parts: **Part I** of the study covers the Council of Europe and European Union standards on online regulation with a particular view on online speech and defamatory content and it explores different modes of implementation and enforcement at the national level. **Part II** of the study introduces and evaluates a recent legislative proposals pending in Albania which if adopted would introduce far-reaching civil liability for online content (the so-called Bregu proposal).

This study proceeds as follows: In **Part I**, its first section revisits European standards of online content regulation starting with the Council of Europe system followed by European Union law relevant in the context of online content regulation. The next section takes up the major challenges for public policy in the context of online content regulation and introduces selected European countries' experiences in this field to show the practical limitations of any unfettered approach to online content regulation. **Part II** to Albania and interrogates its national legislation and the pending legislative proposal in the light of the previous sections in order to discern policy recommendations on how Albania can best conform with European best practices in online content regulation.

4. *ECtHR, Delfi AS v. Estonia, application no. 64569/09, 18 March 2015, 12-13.*
5. *CJEU, case C-131/12, Google Spain SL, Google Inc. v AEPD, Mario Costeja González, 13 May 2014.*

PART I
EUROPEAN BEST PRACTICES OF ONLINE CONTENT REGULATION

The CoE, because of its traditional mandate, has been particularly active throughout the years in creating a full body of principles and rules that apply to the protection of the freedom of expression online. The CoE bodies have repeatedly stressed the need for national authorities to end the current state of fragmentation of defamation laws and called for more attention to be paid to the ECtHR standards to be incorporated into national laws. The EU institutions concert with the policy approach and the EU acquis has made some particular inroads to the regulatory governance of online content in addition to stressing the relevance of the ECtHR standards to become applied at the national level across the European Union. There are also compelling policy arguments why the liability of Internet intermediaries is limited as a way to create condition that are conducive to the operation of online intermediaries and users' freedom of expression online.

1. COUNCIL OF EUROPE

The advent of the Internet and, in particular, of Web 2.0 has changed modes of both creation and consumption of media content and consequently challenged consolidated assumptions about legal safeguards for the right to freedom of expression enshrined in Art. 10 of the European Convention on Human Rights (ECHR).[6] Within the Council of Europe system, a number of instruments have addressed the most relevant questions, delineating through the years a coherent yet complex assessment of the nature of freedom of expression in the online environment. As a guiding principle, it has been established that communication happening on the Web should not be subject to any stricter content rules or restrictions than any other medium.[7] The Council of Europe maintains that state interventions into the right to freedom of expression and media freedoms in particular should be guided by similar general regulatory principles irrespective whether or not professional media outlets, intermediaries or individual users are involved. Recommended general principles include strict necessity, minimum intervention, and the protection of from unduly interference.[8]

1.1 A graduated and differentiated approach

The *Recommendation of the Committee of Ministers to member states on a new notion of media* grasps the main challenges of regulating online media content in the contemporary technological landscape as follows:

> "Despite the changes in its ecosystem, the role of the media in a democratic society, albeit with additional tools (namely interaction and engagement), has not changed. Media-related

6. *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 <http://conventions.coe.int/treaty/en/Treaties/Html/005.htm> (accessed 10 August 2015).*

7. *Declaration on freedom of communication on the Internet, adopted by the Committee of Ministers on 28 May 2003. Cf. Principle 1: "Member states should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery."*

8. *Recommendation of the Committee of Ministers to member states on a new notion of media, CM/Rec(2011)7, adopted by the Committee of Ministers on 21 September 2011, para. 59.*

> policy must therefore take full account of these and future developments, embracing a notion of media which is appropriate for such a fluid and multi-dimensional reality. All actors – whether new or traditional – who operate within the media ecosystem should be offered a policy framework which guarantees an appropriate level of protection and provides a clear indication of their duties and responsibilities in line with Council of Europe standards. The response should be **graduated and differentiated** according to the part that media services play in content production and dissemination processes."[9]

The efforts of the CoE institutions have been oriented towards a complex task of redefining the limits and balance between already existing principles that correspond to the new media environment. As phrased in the Recommendation the challenge for today's policy-makers and regulators is "how to apply media standards to new media activities, services or actors in a graduated and differentiated manner."[10] The practical impact of this approach entails that, first and foremost, singling out the detailed legal safeguards that protect freedom of expression on the Internet is not an exercise in devising brand new tailored-made provisions to fit today's technologies but, rather, an effort to understand the unbalances that originate from the new environment and reassess the relevant provisions in an attempt to even out such unbalances.

The CoE thus advocates an approach which requires that

> each actor whose services are identified as media or as an intermediary or auxiliary activity benefit from both the appropriate form (differentiated) and the appropriate level (graduated) of protection and that responsibility is also delimited in conformity with Art 10 of the ECHR and other relevant CoE standards.[11]

Solutions should ideally be flexible – in order to keep at pace with the future further developments of technology, likely very fast –, in line with the principles devised by the CoE and suitable to provide adequate level of protection to the different actors involved in the production and dissemination of media content. In practical terms it matters whether an actor in the new online environment meets the revamped characteristic of media or -- *a contrario* – provides intermediary or auxiliary activities because this allocation the appropriate level of regulatory intervention.

1.1.1 A new, broad notion of the media

The effort to define what classifies as media (or not) in today's landscape impacts on the regulatory division of labour to a significant extent. The Recommendation stresses a number of rights and prerogatives (such as the right to investigate and to fair access to distribution channels) as well as duties (such as respect for third parties' rights) that pertain to media outlets only because of the fundamen-

9. *Emphasize added. Ibid., para. 6.*
10. *Ibid, para. 56.*
11. *Ibid., Appendix, para. 7.*

tal role they have within democratic societies. Examples of media privileges explicitly mentioned in the Recommendation, with specific reference to the need for them to apply to the "new ecosystem", include the use of defences of truthfulness and accuracy of information, good faith or public interest; a sharp difference in the assessment of content from that of opinion, with the latter enjoying greater freedom, and a right to partake in satire and even exaggeration[12].

The new online environment thus carries as a first preliminary challenge a re-definition of the boundaries of the media ecosystem. Hence the Recommendation provides a set of indicators to help discern whether a new communication service should be regarded and regulated as a media outlet or rather as an intermediary.

Indicators of activities that fall under the notion of media include:

- self-categorisation as a media outlet, membership in professional media organisations, working methods analogue to those typical of media organisations, and, in the new media environment, the capacity and the availability of technical means (e.g. platform or bandwidth) to disseminate content to large audiences online[13];
- the intent to produce, aggregate or disseminate media content, either through traditional or innovative business models such as online platforms for sharing user-generated content[14];
- editorial control on the disseminated content, which can take various forms including those typical of some online platforms such as ex-post moderation of UGC or predetermined internal procedures to comply with peer review and take down requests, when the ultimate decision, despite of the active involvement of users stay within the relevant organisation with ultimate decisions taken according to an internally defined process and having regard to specified criteria[15];
- compliance with professional, ethical and deontological standards, while conversely expecting to benefit from widely common legal privileges attached to the legal professions[16];
- the scope of dissemination and outreach, taking into account both traditional and innovative means for transmission such as non-linear and on-demand delivery of content[17];
- and finally the expectation from the public which should recognise and acknowledge media outlets as such – meaning that they respect the outlet as a reliable and trustworthy source of information.[18]

12. *Ibid., para. 67.*
13. *Ibid., para.16-22.*
14. *Ibid., para. 23-28.*
15. *Ibid., para. 29-36.*
16. *Ibid., para. 37-42.*
17. *Ibid., para. 43-49.*
18. *Ibid., para. 50-55.*

1.1.2. Intermediary or auxiliary activities

Intermediaries, on the contrary, are not formally defined by (although explicitly non-comprehensive) sets of indicators as those provided for the media, and could likely be defined *a contrario* by the lack of one or more of those essential characteristics that instead define the media. However, the Recommendation does not overlook at the importance of such operators within the contemporary media and communications landscape, and acknowledges that they offer "alternative and complementary means or channels for the dissemination of media content" and contribute to fostering diversity and plurality within the media sphere.[19] Intermediary or auxiliary activities are situated on the opposite side of the spectrum of what is demanded in terms of a graduated and differentiated approach to legal responsibilities and privileges in the new media environment. Typically, such actors are not required to observe media specific requirements for the reason that they do not have any influence over the content and activities of their users are thus "**passive**" in that regard. In some cases, this delineation can amount to treading a fine line until ECtHR jurisprudence provides further guidance on this question, such as the recent Grand Chamber judgement in the *Delfi* case (cf. *supra* 2.1.2.3).

1.2 The link between defamation, freedom of speech and democracy

Within the context of the European Convention on Human Rights, freedom of speech is acknowledged as a fundamental freedom although far from unlimited: the "protection of the reputation or rights of others" is acknowledged by Art 10(2) as a ground for state authorities to impose lawful restriction to freedom of expression. As in the case of other restrictions to free speech, such limitations must be prescribed by law and necessary in a democratic society; furthermore, the European Court of Human Rights has repeatedly stressed the need for such limitations to be constructed narrowly[20]; the possible conflict between these two competing rights is to be decided through a process of **balancing of competing interests**[21] – the Court thus implicitly refusing to establish a hierarchy between the two. However, it emerges from the combined analysis of the CoE standards and the case-law of the ECtHR that the balance is most likely to tip on the side of freedom of expression when the nature of the speech is of relevance to the public interest, as stressed at last in the Declaration on freedom of political debate in the media[22].

In a general perspective, striking a balance between the two has proven to be a challenging exercise and consistency lacks across national jurisdiction. The Council of Europe has recently expressed concern for such a lack of uniformity:

> "In defamation cases, a fine balance must be struck between guaranteeing the fundamental right to freedom of expression and protecting a person's honour and reputation. The proportionality of this balance is judged differently in different member states within the Council of Europe. This has led to substantial variations in the stringency of defamation law or case law, for example different degrees of attributed damages and procedural costs, varying defini-

19. *Ibid., para. 63.*
20. *ECtHR, Grinberg v. Russia, application no. 23472/03, 21 July 2005.*
21. *ECtHR, Bladet Tromsø and Stensaas v. Norway, Application no. 21980/93, 20 May 1999, 324.*
22. *Adopted by the Committee of Ministers on 12 February 2004. Cf. para. I: "Pluralist democracy and freedom of political debate require that the public is informed about matters of public concern, which includes the right of the media to disseminate negative information and critical opinions concerning political figures and public officials, as well as the right of the public to receive them."*

tions of first publication and the related statute of limitations or the reversal of the burden of proof in some jurisdictions."[23]

The Council has further stressed the need for a "reform of the legislation on libel/defamation in member states … in line with the requirements set out in the case law of the Court."[24]

Defamation actions at the national level have been considered as a potential threat to freedom of the media, because of their potential chilling effect. The Recommendation on *Freedom of expression in the media in Europe*[25] urged Member States to bring their national legislations in line with the relevant standards and recommendations of the Coe and the case-law of the European Court of Human Rights. The case-law of the ECtHR is indeed particularly rich of indications on the scope and boundaries of free speech and defamation laws under the CoE system. As mentioned above already, the advent of the Internet has not challenged directly such orientations, which remain valid under the current technological landscape. On the contrary, in the most recent Recommendation on a new notion of media the Committee of Ministers has further recommended that "as a form of interference, any regulation should itself comply with the requirements set out in Art. 10 of the European Convention on Human Rights and the standards that stem from the relevant case law of the European Court of Human Rights."[26]

The ECtHR has not provided a unitary definition of hate speech as such, although the now conspicuous body of case-law rendered on Art 10 has provided the boundaries of what constitutes an acceptable interference with Art 10; the definition of Art 10 as outlined by the ECtHR case-law thus follows an *a contrario* criterion to understand what forms of speech constitute an unlawful interference with the rights of the others and what are, instead, protected by Art 10. Particular attention has been brought to a number of qualifying circumstances.

- In regard of the first circumstance – the nature and content of the speech – the Court has traditionally granted stronger protection to **political speech and matters of public interest in general** (the Court has denied that a sharp distinction between the two exists[27]), under the assumption that such topics are of the highest relevance to the democratic debate and interference should thus be kept to a minimum, as noted in some early seminal decisions[28]. The Court has insisted repeatedly that it is a specific duty of the press to impart information on political questions and on other matters of public interest and this requires that national lawmakers and courts take into account "that the press plays a pre-eminent role in a State governed by the rule of law[29]" when deciding on the boundaries of legitimate speech in such matters.

However, the prominence of political and public interest matters applies as a stand-alone criterion to

23. Steering Committee on the Media and New Communication Services, 'Draft declaration of the Committee of Ministers on the desirability of international standards dealing with forum shopping in respect of defamation, "libel tourism", to ensure freedom of expression', CDMC(2011)018Rev8, 2012, 2.

24. Ibid., 4.

25. Rec 1589 (2003), adopted by the Parliamentary Assembly of the Council of Europe on 28 January 2003.

26. Cf. Ibid., para. 4.

27. ECtHR, Thorgeir Thorgeirson v. Iceland, Application no. 13778/88, 25 June 1992, 64.

28. Cf. ECtHR, Sunday Times v. the United Kingdom, application no. 6538/74, 26 April 1979; Observer and Guardian v. the United Kingdom, application no. 13585/88, 26 November 1991.

29. ECtHR, Prager and Oberschlick v. Austria, Application no. 15974/90, 26 April 1995, 34.

discern the relevance of the speech, even independently from the (logically consequent) pre-eminent role of the press, and thus protects as well private citizens when they raise "issues capable of affecting the general interest[30]" through various means such as for instance open letters – or rather more pervasive and far-reaching digital technologies available today.

- A further distinction established by the Court focuses on **value-judgments and facts** – the former being opinions expressed by the author of the speech which, because of their very nature, cannot be proven true. The likes of questioning an elected politician's morality[31], calling them an idiot[32] and even comparing their ideas to Nazi propaganda[33] thus do not necessarily constitute defamation. The Court has also stressed how the limits of acceptable form depend on the concrete circumstances and in particular on the dynamics of the ongoing public debate; the Court's assessment, in a number of occasions, considered whether the allegedly defamatory comments were instead "proportionate to the stir and indignation caused by the matters alleged"[34] and found them legitimate although severely critical. However, such limits seem to become significantly narrower when the criticized person is a private rather than a public figure, such as for instance a school teacher: in such cases, the assessment of whether or not the critique has overstepped the boundaries of acceptable criticism include the possibility to express the same thought with a different, less afflictive choice of vocabulary and whether the words used went as far as suggesting that the defamed person had committed a crime in absence of a final conviction, thus infringing the right to presumption of innocence.[35]

- The second strand (**special qualifications attached to the defamed persons**) is to a certain extent related to the first, inasmuch as, once established that a certain form of speech is of public interest due to its very own nature, and there thus exists a public's right to know about it, the Court typically performs a "test of necessity" aimed at considering whether the interference at stake is truly necessary in a democratic society. The test typically takes the form of a proportionality scrutiny and consists of weighting the competing rights of the persons allegedly defamed with the public's right to know. The Court has first envisaged the test in *Handyside*[36] and then applied to different other professional categories.

The most relevant stream of decisions focuses on the issue of alleged **defamation of politicians**. The Court has stated that politicians must bear "close scrutiny of [their] every word and deed by both journalists and the public at large[37]" and "display a greater degree of tolerance, especially when [they themselves make] public statements that are susceptible of criticism[38]", and thus concluded that the definition of what constitutes defamation in relation to politicians must necessarily be narrower than usual, for the "limits of acceptable criticism are … wider as regards a politician as such than as regards a private individual."[39]

30. *ECtHR, Marônek v. Slovakia, Application no. 32686/96, 19 April 2001, 56.*
31. *ECtHR, Lingens v. Austria, Application no. 9815/82, 8 July 1986, 45.*
32. *ECtHR, Oberschlick v. Austria (no. 2), Application no. 20834/92, 1 July 1997, 34.*
33. *ECtHR, Oberschlick v. Austria, Application no. 11662/85, 23 May 1991, 63; Scharsach and News Verlagsgesellschaft mbH v. Austria, Application no. 39394/98, 13 November 2003, 41-46.*
34. *ECtHR, De Haes and Gijsels v. Belgium, Application no. 19983/92, 24 February 1997, 48.*
35. *ECtHR, Constantinescu v. Romania, Application no. 28871/95, 27 June 2000, 71-74.*
36. *ECtHR, Handyside v. the United Kingdom, application no. 5493/72, 7 December 1976.*
37. *ECtHR, Lingens v. Austria, Application no. 9815/82, 8 July 1986, 42.*
38. *ECtHR, Oberschlick v. Austria (no. 2), Application no. 20834/92, 1 July 1997, 29.*
39. *ECtHR, Lingens v. Austria, Application no. 9815/82, 8 July 1986, 42.*

It is noteworthy to mention that, in devising such principle, the Court seems to have attached the principle of the expected greater degree of tolerance the personal qualification of the defamed persons – as elected politicians – more than to the professional qualification – as a professional journalist or not – of the authors of the alleged defamations. Hence, individual citizens' comments online criticizing politicians towards matters of public interest would be also met with greater tolerance.

The Court has taken a more varied approach in regard of democratic institutions. The strictest approach has been reserved to **governments**, in whose regard "the limits of permissible criticism are wider … than in relation to a private citizen, or even a politician" because of the dominant position in society that such bodies traditionally hold. Competent state authorities should thus pay the utmost attention to devising proportionate measures to balance the right to free expression with the need to protect the government's reputation; criminal measures, although in theory admissible if "intended to react appropriately and without excess to defamatory accusations devoid of foundation or formulated in bad faith[40]", should in principle be avoided, especially when other means are available for the government to respond to even unduly criticism and attacks. However, it is worth noting that the protection of the Government's reputation has seldom been used as a stand-alone exception but rather jointly with other qualifying causes, such as for instance the prevention of disorder[41]. A similar reasoning has been applied to the case of **foreign heads of State**: even in spite of a legitimate interest such as safeguarding diplomatic relations with foreign states, granting special protection from criticism to such heads of state have been deemed disproportionate and "a special privilege that cannot be reconciled with modern practice and political conceptions.[42]"

When the **judiciary** is instead implicated, the Court has been seemingly much more prone to allow for limitations of free speech in order to protect the judiciary's reputation. The Court has considered the defamation occurs if accusations are brought against judges "personally" and are "likely to lower them in public esteem … without any supporting evidence[43]". The analysis of the Court has considered the special need of the judiciary to rely on public trust in order not to see its institutional role undermined (it "must enjoy public confidence if it is to be successful in carrying out its duties[44]") along with the factual capacity of the allegedly defamed persons to defend themselves in other ways than judicial actions (the "judges who have been criticised are subject to a duty of discretion that precludes them from replying[45]").

The analytical framework can thus be reconstructed as follows: the boundaries of legitimate and acceptable criticism can be considered to be more or less narrow according to some peculiar qualities of the institution addressed by the criticism; qualities to consider include whether the institution occupies a dominant position in the society, the need for the institution to enjoy public trust, the possibilities for the institution to build and strengthen such ties of trust (for instance through elections), and the different means available to the institution to react and respond to the criticism. Such analysis suggests that institutions such as parliaments and governments enjoy greater possibilities,

40. *ECtHR, Castells v. Spain, Application no. 11798/85, 23 April 1992, 46.*
41. *Ibid., Application no. 11798/85, 23 April 1992, 39.*
42. *ECtHR, Colombani and Others v. France, Application no. 51279/99, 25 June 2002, 68.*
43. *ECtHR, Barfod v. Denmark, Application no. 11508/85, 22 February 1989, 35.*
44. *Ibid., 34.*
45. *Ibid., 34.*

compared to the judiciary, to gain and reinforce public trust through cyclical elections and to engage in public debates with their critics and should therefore be prepared to endure harsher expressions of criticism – both in form and substance. Conversely, when the institution at stake benefits from such circumstances to a lesser extent, the scrutiny of the criticism can be stricter, including for instance the accuracy of the critiques.[46] The same analytical framework can be applied to other institutional bodies and figures such as public prosecutors[47], police officers[48], civil servants[49].

It is worth mentioning that the orientation followed by the Court is backed by other instruments approved by other CoE bodies. The centrality of freedom of speech in the democratic debate has been strongly and vehemently advocated by the Committee of Ministers in the *Declaration on freedom of political debate in the media*,[50] in which the "right of the media to disseminate negative information and critical opinions concerning political figures and public officials" (which has a mirroring counterpart in the public's right to receive them) is stated to be a necessary prerequisite to pluralist democracy. The Declaration stresses how political figures and public officials must accept public scrutiny, and therefore should not receive stronger legal protection from robust and strong criticism, even insulting statements, satire and humorous expression – the boundaries for the last two being even wider – than ordinary citizens. This means that neither special legal remedies nor more severe penalties should be provided for the protection of the reputation of such figures; furthermore, defamatory or insulting statements against the state, government and other representative institutions should not be criminalized by national laws.

1.2.1 The liability of professional journalists and the case of user-generated content

The rise of Web 2.0 has greatly increased the possibilities for non-professional media operators to have their voices heard by large audiences. The wide availability of web-hosting services for ordinary individuals to run their own blogs; web-sharing platforms such as, most famously, YouTube; and, perhaps most importantly, social network websites such as Facebook and Twitter are blurring the lines between professional and journalistic content and UGC. At present state, a number of lawsuits filed before national courts have triggered questions, and consequently sparked uncertainty, on whether figures such as a web-master, a blogger or even an occasional author of a post on an online forum could be held liable for possibly derogatory or defamatory content that appears on the Web.

The lack of certainty sheds light on the relevance of the effort taken by the Committee of Ministers to devise indicators to help ascertain which operators configure as professional operators and which not; a sharper definition of the boundaries between the two would also help ascertain the different thresholds of responsibility faced by each category for the content they share. The ECtHR has not, thus far, tackled the question in a decisive fashion. However, a number of principles and illustrative indications can be inferred, either from the case-law or other instruments, to try and navigate this complex question.

---

46. *ECtHR, De Haes and Gijsels v. Belgium, Application no. 19983/92, 24 February 1997, 37.*
47. *ECtHR, Lešník v. Slovakia, Application no. 35640/97, 11 March 2003.*
48. *ECtHR, Pedersen and Baadsgaard v. Denmark, Application no. 49017/99, 17 December 2004.*
49. *ECtHR, Busuioc v. Moldova, Application no. 61513/00, 21 December 2004.*
50. *Adopted by the Committee of Ministers on 12 February 2004.*

As mentioned already, in the *Recommendation on a new notion of media* the Committee of Ministers has released a (non-exhaustive) series of indicators on how to discern what constitutes professional media activities. The Court has further specified that, if an individual classifies as a professional journalist, this qualification carries **higher responsibilities** than those born by ordinary individuals. This principle has been expressed and confirmed on a number of times and includes obligations such as "acting in good faith and on an accurate factual basis and provide "reliable and precise" information in accordance with the ethics of journalism"[51]; it has been reiterated at last in a recent ruling where its link with the advent of online journalism is discussed. The Court has conceded that "in a world in which the individual is confronted with vast quantities of information circulated via traditional and electronic media and involving an ever-growing number of players, monitoring compliance with journalistic ethics takes on added importance"[52]; most notably however, the ruling does not call for different or stricter standards to apply to electronic media, but rather the opposite – the rise of new means for distribution calls for standards of good journalism to be **applied horizontally irrespectively of the medium** chosen.

To confirm this view, a later ruling suggests that obligations that follow from the qualification as a journalist, such as the duty to verify the truthfulness of the facts alleged in a story, are not waived or lowered as a consequence of the use of a non-traditional technology or methodology for the dissemination of content[53]. Furthermore, the professional standards apply irrespectively of whether a journalist is disseminating content through professional means (e.g. the newspaper they work for) or a personal, non-professional outlet (e.g. the journalist's personal Twitter account)[54]. In this respect, the Court has thus seemingly operated in the direction of a **technologically-neutral approach**, which attaches specific obligations to the personal qualifications of the author or disseminator of the content, irrespectively of the medium of choice.

However, parallel to this, the specificities of technology can also be taken into account and regulatory responses should be proportionate to this. In a ruling concerning the reproduction of material from the Internet by the press the Court affirmed that, on the one hand, national policy-makers could legitimately provide for different policies concerning the reproduction of materials from the press or from the Internet. One the other hand, the republication from the Internet by media which is observant of professional standards should also receive adequate protection.[55] In the ruling at stake, a local newspaper had republished an allegedly defamatory letter originally found on a news website and was then convicted before the local courts. The lack in the national law of sufficiently specific provisions to grant the right to republish libel from the Internet, as it is instead the case in regards of other media, had deprived the defendants of the corresponding defence. The European Court found instead that the journalists had acted in respect of professional standards and considered the **lack of Internet-specific legal provisions**, in the specific case, to be unlawful since it was impinging on Art 10. The Court conceded that providing for different regulatory approaches in respect of different technologies would be, as a matter of principle, perfectly fine, although in this specific circumstance

51. *ECtHR, Stoll v. Switzerland, application no. 69698/01, 10 December 2007, 103.*
52. *Ibid., 104.*
53. *ECtHR, Polanco Torres and Movilla Polanco v. Spain, application no. 34147/06, 21 September 2010.*
54. *ECtHR, Fatullayev v. Azerbaijan, application no. 40984/07, 22 April 2010.*
55. *ECtHR, Editorial Board of Pravoye Delo and Shtekel v. Ukraine, application no. 33014/05, 5 May 2011.*

the Court considered that the lack of explicit provisions was diminishing, rather than strengthening freedom of speech, especially since the lack of explicit provisions made it difficult for the media operators to foresee the possibility of receiving penalties as consequences of their behavior.

The regulatory system resulting from the combination of such principles and rulings could be summed up as follows: exercise of freedom of speech carries specific responsibilities not to infringe rights of others. In today's environment, state authorities must operate sensibly and carefully to discern those who disseminate content on a professional capacity from those who operate as private individuals. Standards of responsibility expected from professionals can be higher, whereas the same standards cannot be expected from non-professional Internet users, such as those who post messages in the comment sections of online newspapers or blogs, or Youtube users – who as a result cannot be held liable to the same standards as journalists and expected to meet analogous levels of accuracy, ethics and deontological standards.

The technological means used to transmit the message do not alter this main distinction, meaning that journalists will still be held liable by their professional standards whether they use a professional or a personal outlet to communicate their content. However, courts and decision-makers are also recommended to take into account the specific impact and outreach of the medium of choice of the alleged wrongdoers. This task can prove difficult, especially for courts called to assess lawsuit on individual basis; whereas digital technologies by no doubt offer chances for ordinary users to have their voices heard in ways that were simply unthinkable a few years ago, the effective readership of each allegedly defamatory or harmful content should be assessed specifically and on a case-by-case basis, rather than assuming a blanket impact sparked by all online content in reason of the technology used. From their end, law-makers and regulators are under a positive obligation to provide for suitable legal frameworks that, while taking into account the specificities of each medium, enhance – rather than stifle – freedom of expression and of the media.

1.2.2. Defamation and criminal charges

The use of criminal defamation laws as a way to "harass undesired critics" was also condemned in the Recommendation on *Freedom of expression and information in the media in Europe*.[56] The strong need to align national laws to international standards and – in particular – decriminalise defamation is the main focus of two dedicated instruments, the Resolution 1577 (2007) and Recommendation 1814 (2007), both entitled *Towards decriminalisation of defamation*.[57] Both the Resolution and the Recommendation acknowledge that the protection of the reputation and rights of others are legitimate aims to be pursued by national law-makers, although defamation laws need to be phrased and applied narrowly because of the potential threats to freedom of expression resulting from misuses or abuses of such laws. Other bodies of the CoE have similarly stressed the need to **overcome criminal prosecution of defamation** on a number of occasions: most recently, the Parliamentary Assembly in the *Recommendation on respect for media freedom*[58].

56. *Rec 1506 (2001), adopted by the Parliamentary Assembly of the Council of Europe on 24 April 2001.*

57. *Res 1577 (2007), adopted by the Parliamentary Assembly of the Council of Europe on 4 October 2007; Rec 1814 (2007), adopted by the Parliamentary Assembly of the Council of Europe on 4 October 2007.*

58. *Rec 1897 (2010), adopted on 27 January 2010.*

The ECtHR has been thus far reluctant to find the criminalization of defamation straightforwardly incompatible with Art 10; however, the case-law has developed through the last few years to narrow down progressively the scope of acceptable penalties, in practice reaching a similar result. The Court has mostly operated on the grounds of **proportionality** and the notion of **"chilling effect"**, i.e. the risk of stifling freedom of speech that the sole existence of aggravating penalties implicitly sparks, because of the pressure they exert on journalists, media operators and common citizens at large. In a case involving the author of a scientific publication who had criticized the validity of the existing literature in her field the Court argued more explicitly that even the very existence of the possibility of prison terms for cases of "common defamation" results automatically in a disproportionate chilling effect[59]. It is worth mentioning, however, that the issue of proportionality has also emerged from a number of cases concerning **civil pecuniary sanctions**, with the Court quashing "disproportionately large" sanctions decided by national courts.[60]

1.2.3. The liability of Internet Service Providers

One of the most stringent questions of the last few years concerns the liability of Internet Service Providers (ISPs). Typically, an ISP is a company that provide a service allowing private or commercial users to undertake an activity online – ranging from access to the Internet itself to the use of more specific features such as VoIP, email, web-hosting or file-sharing. The definition is evidently broad and capable to include subjects undertaking significantly different activities. The scattered landscape that results from a plethora of different phenomena included under the same umbrella-term concurs to create the current confusion as to the legal implications and responsibilities of ISPs for the posting of illegal content on the Internet.

The issue of ISP liability is again a case of digital technologies altering the scope and magnitude of dynamics of defamation law consolidated in the analogue world and now challenged by the changes in technology. Publishers of print publications such as books, magazines and newspapers have traditionally been held liable along with the material authors of the defamatory content – often for their larger financial capacities to pay damages back, compared to the authors. The pressing issue of these days is thus whether ISPs could be assimilated to publishers – and held liable for different wrongdoings committed by third parties through the means of the services the ISPs provide – in the online environment.

Obviously, ISPs could only be assimilated to publishers in case they retain a significant degree of editorial control on the published content; central to question on the liability of ISPs is thus the degree of editorial control they retain on the content uploaded onto the platforms they operate. Between the two extremes of full and no control, a larger grey area of partial (for instance, on the time some content will remain visible to users) or potential control spurs debates and scattered approaches.

Within the CoE system, a mixed approach to ISP liability has emerged thus far. As a matter of general principle, the orientation is towards a **limited degree of liability**. Principle 6 of the *Declaration on Freedom of Communication on the Internet* provides that, apart from not being imposed to monitor In-

59. ECtHR, Azevedo v. Portugal, application no. 20620/04, 27 March 2008, 33.

60. Cf. ECtHR, Tolstoy Miloslavsky v. the United Kingdom, application no. 18139/91, 13 July 1995; Maronek v. Slovakia, application no. 32686/96), 19 April 2001; Pakdemirli v. Turkey, application no. 35839/97, 22 February 2005.

ternet content and actively seeking for evidence of illegal activities, ISPs should neither be held liable for content they help to transmit or provide access to. However, ISPs could be held co-responsible, along with the materials' authors of the wrongdoing, only if, in the case they store third-party content and they are made aware of the illegality of such content, they do not take appropriate measures to remove of disable access to it. Under the CoE's graduated and differentiated approach, however, reliance on such privileged liability regime requires that actors are qualified as performing intermediary or auxiliary activity ("passive") contrary to media actors ("active"). As it was referred to above, the CoE formulated a set of indicators to help discern whether a new communication service should be regarded as a media outlet and consequently regulated as such (Cf. *infra* 1.1.1.).

The Court has thus far had only few chances to elaborate on the principle distinction between actors identified as media or as performing an intermediary or auxiliary activity. In a first case, the Court declared inadmissible the application of the two co-founder of a file-sharing website, convicted by Swedish domestic courts for breach of copyright; the Court acknowledged that the convictions represented a possible interference with Art 10, although also conceded that the matter at stake – copyright – left to state authorities a wider margin of appreciation than in the case of political speech.[61] It follows from this decision that state authorities enjoy a lesser degree of margin of appreciation in asserting ISP liability against competing rights and interests when on the opposite of the scale is an interest of the utmost relevance such as political speech and public interest matters.

***The Delfi judgement*[62]**

In *Delfi v Estonia*, the applicant company is one of the largest news portals on the Internet in Estonia which also provides a function below its articles where users could upload and view comments. The comments which were uploaded automatically and not edited or moderated were subject to a system of notice-and-take-down, automated filtering for obscene words in addition to the possibility to directly notify the provider about defamatory content which would then remove this comment. The website clarified that comments did not reflect its editorial opinion and it laid down "Rules of comment". In January 2006, the Delfi news portal published an article about a ferry company destroying ice roads between the mainland and islands. This article received a fair amount of comments by users out of which 20 contained personal threats and highly offensive language directed against the owner of the ferry company. On the day Delfi received notice about the infringing comment -- about six weeks after the publication -- these comments were deleted. Following court decisions of lower courts, in 2009, the Supreme Court decided that Delfie is liable under the Obligations Act and that its liability was not excluded under the Information Society Services Act. The Court argues that Delfi is not merely an intermediary service but has an economic interest in the posting of comments and has control over the comment environment. Delfi subsequently applied to the ECtHR.

61. *ECtHR, Neij and Sunde Kolmisoppi v Sweden, application no. 40397/12, 19 February 2013.*
62. *ECtHR, Delfi AS v. Estonia, application no. 64569/09, 18 March 2015.*

The ECtHR held the defendant – an Internet news portal – responsible for comments posted by third parties in the section below an article concerning a matter of "a certain degree of public interest".[63] Hereby, the Court considers that "because of the particular nature of the Internet, the "duties and responsibilities" that are to be conferred on an Internet news portal for the purposes of Art. 10 may differ to some degree from those of a traditional publisher, as regards third-party content."[64] The Court focused on the activity undertaken by the defendant, which included being "engaged in journalistic activities and … opening up of a comment space [which] formed part of the news portal": such activities contributed towards the classification of the defendant as an "**active intermediary**" – a definition in which the attribution of playing an active role in facilitating the posting of unlawful third-party comments played a central role in the conviction.

Notably, the Court qualified Delfi as a "professional"[65] publisher – thus stressing the fact that, by operating in such capacity, it was under a heightened responsibility to know the law and abide by it – possibly by even seeking professional advice. As in the case of *Perrin* and the definition of the relevant jurisdiction thus, the personal qualification of the defendant turns relevant. It remains unclear at present state whether the same degree of liability could be imposed on an ISP which – although providing its services on a remunerative basis – could not be considered to also exert publishing activities by the same standards of professionalism.

It also needs to be stressed further that the Court engaged again in the distinction between the type of wrongdoing perpetrated by the comments at stake. Whereas the definition of the comments as defamatory stems from the line of reasoning adopted by the domestic courts, the ECtHR elaborates further on their nature and, while regretting that the qualification of the comments operated by the domestic courts "remains murky", insists at length on the seeming hateful and anti-Semitic nature of such comments. The Grand Chamber explicitly observed, in this respect, that "what is really troubling here is never spelled out: that some of the comments are racist"[66], seemingly relinquishing the classification of the comments as defamatory – as originally operated by the domestic courts – and re-classifying them as a different type of wrongdoing, one that involves a different degree of severity and criminal relevance.

The qualification of the comments as tantamount to hate speech and incitation to violence has played a fundamental role leading towards the Court's decision. As a result of such qualification, the possible interference with free speech has had to be assessed against a higher threshold – the extremely severe harm suffered by the possible victim of the wrongdoer – and this, together with the circumstance that the penalty imposed on the portal had been lenient enough for it not to change its business model has made the Court conclude that the interference was proportionate[67]. The balance

63. *Ibid., para. 12-13.*
64. *Ibid. para. 13.*
65. *Ibid., para. 129.*
66. *Ibid., para. 12-13.*
67. *Ibid., para. 161.*

with the harm suffered by the targets of the violent comments has, similarly, led the Court to consider that, in such specific circumstance, it would not be disproportionate to request the portal to monitor the content posted through its service; however, given the different individual rights at stake, this does not suggest that a similar request could be considered lawful if any less significant breach of a third party's fundamental right was at stake[68].

The decision has been perhaps one of the most controversial of the latest few years; the dissenting opinions warn against the risk of imposing excessive duties to monitor third parties' online content on ISPs for its potentially disruptive effect on free speech online; for this reason, there should be no "blanket prior restraints" in the form of expecting ISPs to police the Internet 24/7[69]. On the contrary, any duties imposed on ISPs should result from a careful assessment of the different interests at stake to help assess the "appropriate level of care"[70] required in any practical circumstance, on a case-by-case approach.

The *Delfi* judgment thus contributes to better delineate the landscape of intermediaries' liability under the ECHR system as follows: ISPs ought to be considered generally not responsible for wrongdoings committed by third parties using their services, however partial exceptions to this principle can apply when circumstances occur such as:

- in regards of the activities undertaken by the intermediaries, these should amount to actively facilitating the perpetration of wrongdoings by others, hence going farther than just offering the technical means or platforms to the wrongdoers. Furthermore, the scope of the activities should be so far-reaching to trespass the boundaries of what is normally regarded as an intermediary's role but rather constitutes a journalistic activity; because of such redefinition, stricter standards apply.
- In regards of the type of wrongdoing perpetrated, elements of criminal relevance should likely be present.

In the Delfi decision, both these circumstances were found by the Court, leading to the decision to uphold the conviction of the defendant. At present time, it remains unclear, yet no indications in this sense are available, that a similar decision in lack of either of those two elements would be similarly found to be compatible with the ECHR.

1.3 Online content blurring traditional limits of time and space

The very nature of information posted on the Internet is challenging a series of assumptions on the circulation and consumption of news and online content in general. Internet websites are typically accessible over the world irrespective of the place where the author is located and even of the public the content was originally aimed to. Further to this, such information can normally be easily and promptly retrieved even after a significant number of years since they were originally posted; it is today common practice for the large majority of online newspapers and magazines to make the whole (or almost) collection of published articles available to readers through archives. Such collections

68. *Ibid., para. 158.*
69. *Joint Dissenting Opinion of Judges Sajo and Tsotsoria, ibid, para. 33.*
70. *Joint Dissenting Opinion of Judges Sajo and Tsotsoria, ibid., para. 43.*

often date back of several decades and are potentially, if technology assists, to remain online as long as the media outlet stays in business and even afterwards, if the host does not take the content down. As a result, safe language barriers the advent of the Internet is making a unprecedented amount information available to – potentially – everybody across the planet blurring traditional limits of time and space. This makes questions about jurisdiction and limitation period all the more urgent.

1.3.1. The multiple publication rule

Online archives are a disputed matter for the reason they make news stories and online content in general accessible indeterminately after the original publication, potentially forever. Due to the technical means to retrieve webpages online, each and every time an Internet user accesses a webpage from their device, the information stored in a server is downloaded to such device in order to allow the user to visualize the content on their screen.

The main question at stake is whether such technical operation amounts to a new publication of the same content – if this was the case, a new **limitation period for libel action** (as provided by the national law) would run again from each moment the content is accessed on an individual device. The principle is known as "multiple publication rule" and is common in the British jurisdiction; in brief, it entails that "each individual publication of a libel gives rise to a separate cause of action, subject to its own limitation period".[71] This approach is far from being universally adopted across national legal systems as other options are similarly widespread and viable; for instance, the USA has traditionally adopted the opposite "single publication rule", which entails that only one action can be brought, in only one jurisdiction, and the limitation period runs from the time of the first publication irrespectively of other reprints, further editions, broadcastings could occur afterwards. In the Internet environment, this means that the limitation periods runs once from the original uploading of the content, irrespectively of how many times, and when, such content is then downloaded by individual users.

Under the multiple publication rule, lawsuits filed possibly years after the original publication could put media companies, as defendants, in difficult situations and thus spark a result comparable to a chilling effect. Such was the argumentation of the defendant – the British newspaper Times – in a recent case[72]; the ECtHR seemingly opted for a multiple publication rule similar to the UK model, thus allowing for a media company to be sued multiple times over time – including past the original limitation period following the first publication. The Court however conceded that online archives are themselves protected by the right to freedom of speech and has thus envisaged ways for media outlets to be exempt from liability for the content of their archives. Typically, attaching a warning notice to archive copies of knowingly defamatory material would suffice to exclude the media's liability; in any case, media outlets can not be expected to remove their archives altogether. It is also worth mentioning that the Court has seemingly devised in this decision a **balancing test to mitigate** the potentially disruptive effects of a full and blanket application of the multiple publication rule: the two lawsuits at stake with the case had followed shortly one another and the second in particular was filed when the first trial was still ongoing; it was thus unlikely that the defendant's chances to defend themselves appropriately were seriously impaired in the second lawsuit. However, the Court has con-

71. *ECtHR, Loutchansky v Times Newspapers Ltd, [2002] QB 783.*

72. *ECtHR, Times Newspapers Ltd (Nos. 1 and 2) v The United Kingdom, applications 3002/03 and 23676/03, 10 March 2009.*

ceded that "libel proceedings brought against a newspaper after a significant lapse of time may well, in the absence of exceptional circumstances, give rise to a disproportionate interference with press freedom under Art. 10."[73] While accepting the multiple publication rule, the Court has thus contextually excluded that media outlets could keep being sued for an indeterminate period of time. National legislators should therefore balance "the protection of the right to freedom of expression enjoyed by the press … against the rights of individuals to protect their reputations and, where necessary, to have access to a court in order to do so [and thus] set a limitation period which is appropriate and … provide for any cases in which an exception to the prescribed limitation period may be permitted".[74]

1.3.2. Jurisdiction

The geographical seamless nature of the technologies raises further questions arise, such as where the alleged defamation actually took place, what would be the applicable law and which national court would have jurisdiction on the case. Questions of jurisdictions have been dealt with by the ECtHR on a number of occasions well before the advent of the Internet – which conversely has only added a further layer of complexity to the ongoing issue. Art. 1 of the ECHR provides indeed that the Member States should "secure to everyone within their jurisdiction the rights and freedoms" of the ECHR. The relevant ECtHR case-law has now long established that relevant criteria to identify the reach on national jurisdictions – and thus of the State's obligation to grant claimants access to domestic tribunals – include the **territory** (i.e. not only citizens but only residents and any individuals on the soil should be given access) and **effective control** of State authorities on otherwise foreign territories.

The case-law of the ECtHR has been seen to move, in the latest few years, from a strictly territorial-centred approach[75] towards a more comprehensive approach that also takes into account individual circumstances as elements of connection[76]. In one leading decision,[77] the Court accepted British jurisdiction in a case where the applicant was a French national based in the UK where he had been convicted for publishing obscene material on a webpage operated by a US-based Internet company. The content of the webpage, of an obscene nature according to the British law, was instead lawful according to the US law. The Court however accepted the defendant's residence in combination with the **accessibility of the website** at stake within the UK as sufficient criteria for that state to exert its jurisdiction on the webpage, as opposed to the place of establishment of the company running the website. The *Perrin* ruling is the most recent and evident example of personal connection elements becoming central features of Internet jurisdiction; what is further relevant is that by applying such personal connection, the courts in the domestic proceedings were able to apply the (British) **national substantive content regulations** to a US-based website.

In this sense, the decision seems to differ significantly from the line of reasoning adopted in an earlier

73. *Ibid., 48.*
74. *Ibid., 46.*
75. *Cf. ECtHR, Bankovic & Others v Belgium & Others, application no. 52207/99, 12 December 2001.*
76. *Cf. . ECtHR, Issa and Others v Turkey, application no. 31821/96, 16 November 2004; Ocalan v Turkey, application no. 46221/99, 12 May 2005; Medvedyev and Others v France, application no. 3394/03, 29 March 2010; Al Skeini and Others v the United Kingdom, application no. 55721/07, 7 July 2011.*
77. *. ECtHR, Perrin v. the United Kingdom, application no.5446/03, 18 October 2005.*

decision[78] when the Court found no jurisdictional links between the applicants based in Morocco and a paper publication that had taken place in Denmark. Along with personal connection elements, the outreach and accessibility of online publications thus seems to offer a reason to expand national jurisdictions on online publications. However, it ought to be stressed that in *Perrin* the ECtHR considered significant the fact the applicant was operating in a professional capacity, a circumstance that required a "high degree of caution" in the pursuit of his activities – ostensibly higher than what could be expected from an ordinary Internet user acting in their private capacity –, such as taking into account the laws of the country where his activities took place. It is unclear at present, although possibly unlikely, that the same amount of familiarity and awareness of a foreign legal system and its substantive laws could be expected from an individual neither resident in the country exercising its jurisdiction, nor operating in a professional capacity. The effective significance of the apparently newly devised element of connection of the availability of a website in a country will need to be tested further in future cases.

However, the Recommendation on a new notion of media[79] recalls the need to provide for appropriate measures to cope with the "accumulated or multiplied impact" that today's media can generate compared to traditional analogue media; in particular, explicit reference is made to the need to "apportion responsibility" in case of harm made to third-party rights. National legislators and courts should thus operate with particular care and tackle questions of jurisdiction for online activities; proportionality remains, in this field, a paramount principle.

1.3.3. Libel tourism

The strengthening of objective elements of connection such as the country of residence of the defendant taps in a line of reasoning based on the need to avoid libel tourism, i.e. publishers possibly seeking to establish their operations in countries were prosecution would be difficult to pursue, in an attempt to escape their responsibilities. Libel tourism is indeed becoming an issue of major concern at the global level. The Steering Committee on Media and Communication Services, in the aftermath of the *Times Newspapers (Nos. 1 and 2)* decision, has remarked how in the current scenario "libel tourism is an issue of growing concern for Council of Europe member states as it challenges a number of essential rights protected by the Convention such as Art. 10 (Freedom of expression), Art. 6 (Right to a fair trial) and Art. 8 (Right to respect for private and family life)[80]" and thus "the prevention of libel tourism should be part of the reform of the legislation on libel/defamation in member states in order to ensure better protection of the freedom of expression and information within a system that strikes a balance between competing human rights.[81]" Measures recommended by the Steering Committee include, at the domestic level, increasing the possibilities of recognition of foreign judgments across jurisdictions and strengthening the principle of proportionality of damages in defamation cases.

78. *ECtHR, El Mahi and Others v Denmark, Application no. 5853/06, 11/12/2006.*

79. *Ibid., para. 66.*

80. *Steering Committee on the Media and New Communication Services, 'Draft declaration of the Committee of Ministers on the desirability of international standards dealing with forum shopping in respect of defamation, "libel tourism", to ensure freedom of expression', CDMC(2011)018Rev8, 2012, p. 3.*

81. *Ibid., 4.*

1.4. A participatory Internet for all: the role of self- and co-regulation

As noted above, the Coe has already acknowledged that the rise of the Internet and digital technologies in general has modified significantly the chains of production of media content, with the relevant industries now being more scattered and diversified than ever. Since the advent of Web 2.0, i.e. digital technologies that allow professional as well as non-professional Internet users to produce and disseminate content to large audiences, disintermediation has become perhaps the most notable phenomenon that has altered the modes of media production. The changing nature of media industries is reflected in the regulatory approach recommended by CoE Principles, namely the appreciation for **self- and co-regulation** and all measures that "foster and encourage" widespread access to and **participation** in Internet communication and information services (Principle 4) on the one side, and conversely on the other side the disfavour towards forms of prior state control through blocking or filtering measures (Principle 3) or licensing schemes to run individual websites (Principle 4).

As noted above, the fact that state regulation is at high risk of resulting in unduly interference with media freedom is nothing new – and indeed media self-regulation has emerged as a successful regulatory model well before the Internet era; within the contemporary context however, the model seems all the more suitable to address the emerging and pressing issues of the transnational nature of the Internet and the multiplication of stakeholders in the regulated environment, as it was stressed for instance at the 5th European Ministerial Conference on Mass Media Policy "The Information Society: a challenge for Europe"[82]. The more recent Recommendation of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment[83] has confirmed the main pillars of this approach: **empowerment of private users, accessibility of ICT infrastructure and information, international common standards to foster content creation and cooperation among stakeholders** are among the lines of action that the Committee of Ministers has recommended to the Member States.

The Council of Europe has further stressed on numerous occasions the need to embrace openness in policy- and law-making processes and thus relevant stakeholders, such as the private sector and the civil society should be consulted and their opinion taken in account as much as possible while amending or passing new ones. The Council itself has indeed on several occasions opened up to consultation from representatives of various sectors of the civil society – such as NGOs –, the private sector – such as professional media operators –, and the public sector – such as members of the judiciary and regulatory authorities. Recent examples include the regional Conference on defamation and freedom of expression held in Strasbourg on 17-18 October 2002 (which brought toghether members of the judiciary, practicing lawyers and journalists to discuss regulatory issues regarding defamation and alternative measure to litigation such as mediation, and the need to align national laws to the standards of the Council of Europe, in particular the exclusion of special substantive and/or procedural defences for State representatives)[84] and the Luxembourg conference on freedom of

82. *Cf. the resulting Action Plan for the promotion of freedom of expression and information at the pan-European level within the framework of the Information Society (Thessaloniki, 11-12 December 1997): "Action in the area of self-regulation: To encourage, in particular at the transnational level, self-regulation by providers and operators of the new communications and information services, especially content providers, in the form of codes of conduct or other measures, with a view to ensuring respect for human rights and human dignity, the protection of minors and democratic values, as well as the credibility of the media themselves."*

83. *CM/Rec(2007)11, adopted by the Committee of Ministers on 26 September 2007.*

84. *Cf. Defamation and Freedom of Expression – Selected documents. H/ATCM (2003) 1. Media Division Directorate General of Human, 2003.*

expression and the protection of human rights.[85] On this occasion, the risk of misplaced legal rules jeopardizing freedom of the media and the struggle to balance conflicting individual rights were stressed again.[86] The conference concluded with the adoption of a draft law on the freedom of the media which remarked again the need not to provide special measure to protect public officials[87] and the exclusion of criminal liability for publishers[88].

The importance of fostering self-regulation in the media sphere has been also stressed by the ECtHR on a few other occasions[89], with explicit references to the relevant CoE instruments. The Coe has thus delivered a clear and explicit message that the Internet should be an open and collaborative environment; cooperation as an operational principle should extend to the process of rule-making as well. In light of this, national governments and lawmakers should be wary of the intrinsic risk to overregulate the digital media sphere that lies deep in any attempt to provide for regulation from top-down without the involvement of relevant stakeholders from the private sector and the civil society.

1.5. The protection of privacy and identity

As a matter of principle, Art 8 of the ECHR protects the right to private life - and inter alia **of personal data – and private correspondence** – including of Internet mediated communications. The state obligation to protect individuals' personal data creates a complex dynamic with today's Internet environment. ISPs and website owners are often – and increasingly – requested by public authorities to undertake identity checks on their users and retain for a specified period metadata about online communications events for purposes related to public security and the fight against online crimes. Whereas such are definitely legitimate aims of state authorities, the potential for such measures to step too far and breach the right to privacy is all too evident and problematic; while it stays undis-

85. "The media in a democratic society: reconciling freedom of expression with the protection of human rights": Luxembourg – 30 September – 1st Oct. 2002.

86. Cf. Report of Rapporteur Aiden White, Secretary General of the International Federation of Journalists, 'Medias in a Democratic Society: Is There a Possible Balance Between the Freedom of Expression and the Protection of Human Rights'.

87. The suggested wording reads as: "Libel, defamation and insults towards any constituted body shall be liable to the same penalties as libel, defamation and insults towards individuals."

88. The suggested wording reads as:
"Section 1. Criminal liability
Art.20. Liability for offenses committed through the media shall lie with the publisher or his or her assistants, as principal authors.
Art.21. Article 443 of the Criminal Code shall be supplemented by a new sub-paragraph 2, worded as follows:
"2. Neither shall the publisher or an assistant be guilty of libel or defamation if:
1) in cases where the law allows for proof of the facts, such proof is not provided, but the publisher or assistant, subject to having taken due care, show that they had good reason to believe that the facts reported were true and that there was a preponderant public interest in the disputed information being known;
2. it occurs during a live broadcast, provided that:
a) due care has been taken, and
b) the identity of the person uttering the offending words either is apparent from the information disclosed, or may be disclosed to anyone on request;
3. the words are contained in an accurate quotation of another person, provided that:
a) the quotation is clearly identified, and
b) the identity of the author of the quoted words either is apparent from the information disclosed or may be revealed to anyone on request, and
c) disclosure of the quotation to the public is justified by a preponderant public interest in the quoted words being known.
Section 2. Civil liability
Art.22. The publisher and his or her assistants shall be jointly liable for the reparation of all damage caused by the public release of a publication, which shall be ordered payable to third parties on the basis of Articles 1382 and 1383 of the Civil Code."

89. Cf. ECtHR, Mosley v. the United Kingdom, application no. no. 48009/08, 10 May 2011, 55-61; Delfi AS v. Estonia, application no. 64569/09, 18 March 2015, 39.

puted that only a thin line separates legitimate forms of scrutiny of Internet traffic from unlawful intrusions, where such line should be drown remains unclear. It is particularly disputable whether the right to privacy amounts to a **right to retain anonymity online**. A blanket prohibition in such sense does not certainly operate, since the Court has recently found compatible with the Convention an obligation imposed on an ISP to disclose the identity of the author of an advertisement concerning the facilitation of a minor's sex acts;[90] however, the ruling indicates a need to construct the balancing test taking into account the severity of the wrongdoing and the result of the test could be different whereas the anonymous wrongdoer was charged with a criminal accusation of procuring an underage prostitute as opposed to the case of a less aggravating, typically civil charge such as defamation.

Such orientation would be in line with the direction drawn by the Committee of Ministers in the *Declaration on freedom of communication on the Internet*: principle 7 requires member states to "respect the will of users of the Internet not to disclose their identity", except for the purpose of investigating criminal acts. A similar position has been taken more recently by the Parliamentary Assembly in the Resolution on Improving user protection and security in cyberspace.[91] Needless to say, the combined result of such indications along with the strong disfavor towards criminalization of defamation strongly hints at the incompatibility with the Convention of provisions allowing state authorities to obtain from ISPs information disclosing the personal identities of otherwise anonymous authors of defamatory Internet content. Such an approach is also best compatible with the approach of the ECtHR to data retention in a more general perspective; national legislation authorizing the retention of personal data referring to unsuspicious, suspected but not convicted, and convicted criminals in the same indiscriminate approach has been found incompatible with the Convention, notably due to the stigmatizing effect resulting from different situations being treated in the same manner.[92] The ruling confirms once more the need to provide for different ways to handle private information including first and foremost identity, with stronger protections of individual privacy being provided in cases where no criminal charges are implied.

2. EUROPEAN UNION

Within the EU legal system, the Charter of Fundamental Freedoms explicitly provides for freedom of speech at Art 11, largely drawn from the example of the equivalent Art 10 ECHR. The almost exact matching of the wording suggests that the appreciation of the value and importance of freedom of speech within the two systems (EU and CoE) are comparable to each other. The EU institutions have developed, throughout the years, their own set of standards and detailed guidance on the practical implementation of the theoretical principle. Interestingly enough, the similarities between the EU and the CoE approaches seem to greatly outnumber the differences.

90. *ECtHR, K.U. v. Finland, application no. 2872/02, 2 December 2008.*

91. *Resolution 1986 (2014) Final version, adopted on 9 April 2014. Cf. para. 6.4: "Criminal activities on or through online services must be combated effectively by the competent State authorities in accordance with Article 8 of the European Convention on Human Rights; law-abiding users have the right to remain anonymous, while law-infringing users must be identifiable and criminals must be identifiable by law-enforcement bodies subject to the legal safeguards required under the European Convention on Human Rights".*

92. *ECtHR, S. and Marper v the United Kingdom, applications no. 30562/04 and 30566/04, 4 December 2008, 122.*

2.1. EU policy approach

The Committee on Civil Liberties, Justice and Home Affairs has recently released a Report on the EU Charter concerning *Standard settings for media freedom across the EU*[93] which includes a motion for a EP Resolution on the same subject. The Report is revelatory of a number of principles and lines of action that the Parliament considers of the outmost importance in order to enhance freedom of speech, and offer guidance on the actions recommended to national law-makers, administrative and executive authorities, and the judiciary.

2.1.1. Open Internet, Self- and Co-Regulation

Similarly to the CoE, the EU stresses the importance of fostering **openness and participation in the online environment**, and extends this principle to the process of policy- and law-making, as recommended by the CoE as well. The Committee has stressed indeed how independent self- and co-regulatory measures can play "an important role to play in ensuring media freedom" and should be thus encouraged at the supranational as well as at the national level. The Report stresses how the independence, impartiality and transparency of **self- and co-regulatory bodies** should be carefully monitored and implemented; furthermore, independence should be insured from both State and commercial influences[94].

More in detail, the Report cites as viable examples of such regulatory arrangements the likes of **editorial charters and internal codes of conduct**, and stresses the need to protect the independence of journalists from possible source of unduly influence such as editors, publishers or owners, political or economic lobbies or other interest groups[95]. As a further sign of the strong conformity of the EU guidelines with the CoE orientation, the Report recommends to national authorities the "strict application of European Court of Human Rights case-law in this area"[96].

2.1.2. The protection of media operators

A number of principles and recommendations included in the Report focus specifically on the relevance of journalistic professions – **investigative journalism** in particular – and the need for state authorities to provide for best suitable legal frameworks to protect and safeguard their indispensable role within the society. Similar to the guidelines of the CoE, the Report also recalls the fundamental role of professional responsibilities and the duty for professional media operators to **comply with ethical standards** and recommends the provision of professional training by media associations and unions[97]. Such standards should include "the obligation to indicate a difference between facts and opinions in reporting, the necessity of accuracy, impartiality and objectivity, respect for people's privacy, the duty to correct misinformation and the right of reply", and it is a specific duty pending on state authorities to make sure that the relevant industries would establish independent media regu-

93. *Report on the EU Charter: standard settings for media freedom across the EU (2011/2246(INI)), A7-0117/2013, adopted by the plenary sitting of the European Parliament on 25 March 2013.*
94. *Ibid., para. 9.*
95. *Ibid., para. 18.*
96. *Ibid., para. 20.*
97. *Ibid., para. 21.*

latory bodies to provide for adequate regulatory measures in this sense[98].

In terms of safeguards to journalistic freedom, the Report calls for the **decriminalization of defamation** and points at the disruptive effect generated by a variety of practices such as "pressures, violence and harassment … exerted on journalists"[99].

Attention is also paid to **ordinary citizens' communication rights** in the context of digital technologies. The Report includes a strong endorsement in favour of net neutrality and expresses concern for state authorities' attempts at requiring registration or authorization to access online content, as well as at imposing curbing legal provisions in an attempt to halt illegal behaviours.

2.1.3. A focus on digital technologies

Even more recently, the Council has adopted the *EU Human Rights Guidelines on Freedom of Expression Online and Offline*[100]. As the title suggests, the Guidelines take a broader approach to the issue of free speech in the contemporary world and take into account the different ways in which digital technologies have altered the flow of information, thus considering also the case of non-professional media operators. Throughout the document, the strong endorsement of the CoE standards as the best practice that national authorities are recommended to follow is, again, made explicit on a number of occasions[101].

Legal safeguards should cover both professionals and ""citizen journalists", bloggers, social media activists and human rights defenders, who use new media to reach a mass audience"[102], as well as "media actors, NGOs and social media personalities"[103]. The orientation stems from the preliminary observation that the advent of digital technologies has altered the dynamics of production and delivery of content and enabled individuals to reach out wide audiences and play a fundamental role in democratic debates and decision-making processes. The Guidelines thus consider that, with the scope of technological means expanding and widening the process the boundaries of the public sphere, the **scope of human rights should expand** accordingly and cover content disseminated both online and offline[104].

It is also noteworthy to observe how the Guidelines consider that Member States are under a **positive obligation** to provide for suitable legal frameworks to implement such rights[105].

The Guidelines also provide an assessment of what constitutes a **threat to freedom of speech**. Again, the Guidelines take a particularly broad and comprehensive approach to the matter, considering that not only statutory laws, but also any measure resulting in censorship or self-censorship (e.g. "criminal, financial and administrative sanctions on the exercise of freedom of opinion and expression, in viola-

98. *Ibid., para. 24.*
99. *Ibid., para. 25.*
100. *Adopted at the Foreign Affairs Council meeting in Brussels, 12 May 2014.*
101. *Ibid., para. 61.*
102. *EU Human Rights Guidelines on Freedom of Expression Online and Offline, para. 5.*
103. *Ibid., para. 31.*
104. *Ibid., para. 6, 16 and 35.*
105. *Ibid., para. 24 and 35.*

tion of international human rights law"[106]; "arbitrary attacks, indiscriminate abuse of criminal and civil proceedings, defamation campaigns"[107]) and call for the member states' law-makers to make sure the national legal frameworks are in line with such requirements.

The *Annex to the Guidelines* recommends some more specific action to be taken by national law-makers. In detail, such recommendations include:

- Restrictions on freedom of expression must be provided by law, and abide by international human rights law and strict tests of necessity and proportionality, in order to avoid inconsistent and abusive application of legislation which in turn could spark media's self-censorship;
- Taking advantage of defamation laws as a tool to censor criticism amounts to a misuse of such laws, in particular when they entail imprisonment or severe criminal or civil sanctions;
- Interference on Internet usage, such as blocking, slowing down, degrading or discriminating against specific content or applications by operators, including when requested by law, should always be avoided;
- Illegal surveillance and interception of communications, as well as illegal collection of personal data, amount to breach of the right to privacy. Unlawful or arbitrary government or private company access to personal data, and Undue interference with individuals' privacy in general, have a direct potential to stifle free speech and should therefore be avoided.

As mentioned above already, the orientations of the EU and the CoE are significantly similar and in line with each other. While this circumstance further strengthens the authority of both the sets of guidelines and indications, it also offers direct evidence that at the European level, irrespectively of which supranational institution takes the lead in affirming relevant principles, a broad and horizontal consensus in emerging towards common sets of principles and practical ways to implement them.

2.2. EU legislation

Apart from policy declarations and recommendations the EU *acquis* covers legislation and jurisprudence that impacts on online content regulation in the member states. However, it should be noted that the field of online content regulation is not fully harmonized and that a number of aspects are not inside the competence of the EU to regulate.

2.1.4. The liability of ISPs under EU law

The E-Commerce Directive explicitly limits its scope to the provision of services on a remunerative basis, albeit not necessarily paid by the users who receive the service as explained by Recital 18 of the Directive. Pursuant to this definition, Commercial ISPs fall under the scope of the Directive.

Several provisions in the Directive deal with the question of intermediaries' liability. As a general principle, **intermediaries are exempted from liability** for any wrongdoing committed by third parties by using the means of services they provide inasmuch as:

106. *Ibid., para. 30.*
107. *Ibid., para. 31.*

- the service consists of operating and giving access to a communication network to transmit or store made available by third parties (i.e. not by the ISP itself);
- the nature of the service provided is merely of technical, automatic and passive nature;
- and as a result of this the ISP has neither knowledge of nor control over the information which is transmitted or stored108.

Further provisions specify the cases for exclusion of liability in light of specific services that could be provided by ISPs. When the ISP acts as a mere conduit (i.e. the ISP transmits third party's content), liability is excluded under condition that the service provider did not initiate the transmission, nor selected the receiver of the transmission, nor selected or modified the information at stake[109]. The qualification as a **mere conduit** is further defined as including the "automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network", and the storage must be limited to the time strictly necessary to transmitting the content at stake[110]. Recital 43 helps to better understand what is meant by the requirement that ISPs, in order to be kept non-liable, should not modify the transmitted content: the Recital specifies that the ISPs are only allowed to manipulations of a technical nature, which do not alter the integrity of the information contained in the transmission[111].

When the ISP provides **caching** services (i.e. they merely store information, provided by a recipient of the service, on a temporary basis), liability is excluded under condition that it did not modify the information; it complied with conditions on access to the information, with common industry rules regarding the updating of the information; did not interfere with the lawful use of technology to obtain data on the use of the information; and acted expeditiously to remove or to disable access to the information it has stored after obtaining actual knowledge of the fact that the original information has been removed, or access to it has been disabled, or that a judicial or administrative order for such content to be removed or disabled has been released[112].

When the ISP acts as an **host** (i.e. it merely stores information, provided by a recipient of the service, on a permanent basis), liability is excluded if the provider was unaware of the illegal nature of the activity facilitated or of the information stored, including facts or circumstances that made such illegality apparent, or as soon as it is made aware of such illegality, acts expeditiously to remove the illegal content or disable access to it[113].

In light of this, a specific **duty to monitor** the information which they transmit or store is excluded, as well as any blanket provision requiring them to actively to seek evidence of wrongdoings. However, state authorities have a choice to provide for such measures to request ISPs to communicate information about alleged wrongdoing, and information concerning the identity of alleged wrongdoers, to

108. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) Rec. 42.

109. Art. 12(1).

110. Art. 12(2).

111. Rec. 43.

112. Art. 13(1).

113. Art. 14 (1-2).

the competent authorities on their request[114]. The specific boundaries of such possibility are further defined in the Directive: those entail the possibility for national law-makers to authorize courts to provide for the service providers to terminate or prevent an infringement, even when those operate as mere conduits[115] or providers of caching[116] or hosting[117] services. It is noteworthy to mention that, whereas these mentioned provisions grant a discretionary power to legislators to allow national courts to award injunctions towards ISPs, **no mention is made of damages or other penalties to be imposed on ISPs** – which thus seem to be excluded from the number of measures that courts can be lawfully authorized to use.

Despite such definitory efforts, it seems that interpretative problems remain at both the national and the supranational level. Most of the doubts have revolved thus far on the notion of "awareness" of a wrongdoing by ISPs and the "promptness" of their response after being made aware of any illegalities. To further complicate the matter, the notion of ISP is notably broad and capable to encompass the provision of very services and activities; it is thus unclear whether the same notions of awareness and promptness should apply to all of them or if a more balanced, differentiated approach should rather be adopted.

The Court of Justice of the European Union (CJEU) has so far had the chance to clarify such questions, although to a limited extent, in a handful of cases. It has, for instance, considered that activities such as optimising the visual display of the content stored in their facilities amounts to taking an active role in the storage and delivery of the content, excludes the possibility of unawareness and thus makes the ISP liable under Art 14(1)[118]. However, ISPs cannot be required by law to install monitoring softwares and analyse all the data stored and transmitted through their facilities[119]. In a more general perspective, the Court has repeatedly stressed the principle that, whereas payment terms and the overall business models cannot be a stand-alone indicator of whether a service fall under the definition of "information society service provider", attention must be paid to factual hints of whether the provider had knowledge and/or control of the content transmitted through their facilities. In a more recent ruling, this was undisputedly the case of a newspaper publishing company relative to the website on which the online version of the newspaper was posted[120]. Whereas the Court considered that the Directive 2000/31 "does not preclude a Member State from adopting rules of civil liability for defamation, applicable to information society service providers established in its territory", liability still has to be assessed against said checks of previous knowledge and control of the information transmitted[121].

In spite of such interpretative difficulties, it clearly emerges from the joint analysis of the Directive and of the relevant case-law that, once more, **both the EU and the CoE systems are oriented towards excluding ISP liability as a general rule**. Compared to the CoE guidelines, EU Law provides for more explicit exceptions to the principle, although these have not proven to be as straightforward

114. *Art. 15.*
115. *Art. 12(3).*
116. *Art. 13(2).*
117. *Art. 14(3).*
118. *CJEU, C-324/09, L'Oréal SA and Others v eBay International AG and Others, 12 July 2011, para. 107-124.*
119. *CJEU, C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, 16 February 2012, para. 36-40.*
120. *CJEU, Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd and Others, C-291/13, 11 September 2014, para. 46.*
121. *Ibid., para. 31-36.*

as desired, at least thus far. However, it remains clear that none of the existing or pending decisions of either of the two Courts have thus far challenged the principle that ISPs should not be assumed to be aware of any wrongdoing, cannot be forcibly requested to police the content they help to store or transmit, and in lack of any actual and proven awareness of any illegality related to such content, should be held liable for it.

2.1.5. The limited scope of the right of reply

The Audiovisual Media Services Directive represents a first significant attempt by the EU authorities to provide a suitable legal framework for the new technological environment in which the audiovisual media operate. The Directive introduces the category of on-demand audiovisual media services, i.e. those provided on a non-linear basis, especially on the Internet. The Directive rolls out a graduated system of regulation with a bottom layer that applies to all audiovisual media services and some differentiated legal provisions for traditional linear and on-demand audiovisual media services respectively.

The right of reply applies only to providers of linear audiovisual media services, ie. broadcasters and television channels. As a general consideration, the Directive states the principle that "the right of reply is an appropriate legal remedy for television broadcasting and could also be applied in the on-line environment"[122]. The Directive requires national authorities to make sure that broadcasters will grant a **reply (or an equivalent measure)** to those whose reputation and good name have been damaged as a result of an assertion of incorrect facts. While carrying out such duty, the provider should not be faced with **unreasonable terms or conditions**, nor should be given unreasonable time spans to comply with the request[123].

It is noteworthy to mention that, during the preparatory works that led towards the final draft of the Directive, the possibility to extend such provision to on-line media was considered and discussed animatedly. The final version of the text leaves the provision confined to the broadcasting sector and does not alter the substance of the norm to any significant extent compared to the previous provision in the Television Without Frontiers Directive. A number of technology-driven motivations are likely behind this choice (for instance, the wider possibilities that the Internet offers to amend a dynamic page – as opposed to the case of a printed book or newspaper, which obviously cannot be altered once published; the broader access to the medium granted to all individuals, including those who find themselves defamed, to publish an alternative view or perspective on the facts alleged against them), while it is interesting to note the further motivation that an extended right of reply would have a potentially disruptive effect on the uptake of Internet media at the European level and make the European Internet media outlets more vulnerable to their international competitors[124]. Such considerations, originally put forward by the British representatives, could be taken into consideration by national authorities as they proceed to legislate on this matter.

---

122. Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 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), para.. 103.

123. Ibid., Art 28.

124. Department for Culture, Media and Sport, Protection of Minors and Human Dignity: Right of Reply, 2007.

2.1.6. Information duties in the AVMS and in the E-Commerce Directives

Under the EU legal system, information duties are imposed on both ISPs and providers of audiovisual media services; despite the differences in nature and scope they all share a similar rationale, consisting in an attempt to provide more information to the customers of each type of service, regarding the nature of the providers or of the service itself. All such information duties can thus be considered an example of a different approach taken by the EU authorities in this field; whereas democracy-driven consideration are at the heart of other provisions such as protection of journalists and ordinary citizens to access means of communication, the focus here is on users of electronic commerce and media services as consumers. All the provisions discussed below, although different one from another, share this same perspective.

A first batch of information duties requires ISPs to provide a minimum set of information to the recipients of their services, in order to make it possible for them to identify the provider. Such information is considered to be kept at a minimum in order to not infringe the – possibly competing – right to privacy.

Pursuant to the E-Commerce Directive, information to be provided includes:

- the name of the ISP;
- its geographical address;
- its details including the electronic mail address;
- if available, the public or trade register in which the service provider is entered and his registration number;
- the particulars of the relevant supervisor authority, if applicable;
- the details of the registration to any relevant professional body, if applicable;
- the professional title and the Member State where it has been granted,
- a reference to the applicable professional rules in the Member State of establishment and the means to access them125.

A different set of rules is provided in respect of **commercial communications that constitute part of the service provided**. In such cases, information must be available to make immediately identifiable:

- the commercial communication;
- the natural or legal person on whose behalf the commercial communication is made;
- any promotional offers and the conditions thereof;
- promotional competitions or games and the conditions thereof.

Lastly, a third set of analogous provisions is included in the AVMS Directive and focuses on providers of media services (hence in a broad sense, encompassing both providers of linear and on-demand programmes). It establishes an obligation for them to provide to the public clear information on **sponsorship agreements** – through the name, logo, symbols of the sponsor and any appropriate

125. *E-Commerce Directive, Art 5.*

and distinctive sign. The provision evidently aims at avoiding exposing viewers to unwitting sponsoring. To any extent, it is forbidden for tobacco products and medicine to sponsor programmes; the scheduling should always result from an independent editorial decision of the provider and not be influence by the sponsors to any extent[126].

Similar to this, **product placement** is only allowed for cinema productions provided that viewers are clearly informed of the existence of product placement; through appropriate identification of at the start, end, and after resuming from advertising breaks[127].

2.1.7. The rights to privacy and data protection

The Charter of Fundamental Rights (CFR) of the European Union provides in Art 7 for the right to privacy and in Art 8 for the right to the protection of personal data. The EU regulatory framework for data protection regulation consists of the general Data Protection Directive (95/46/EC)[128] and a number of sector-specific instruments, notably the e-Privacy Directive (2002/58/EC)[129]. The publication of personal data online, i.e. "any information relating to an identified or identifiable natural person"[130], constitutes a relevant act of personal data processing which must comply with EU data protection law save where this constitutes a purely personal or household activity.[131] Where this is the case, the individual to which the personal data relates can exercise a number of rights which are provided for in the Data Protection Directive. Pursuant to Art 14(a) of the Directive the individual has the right to object "at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him".[132]

The right to be delisted

Whether data protection law can be invoked to remove online content that affects an individual's reputation has been at issue in a recent Spanish case. In 2010, Mr. Mario Costeja González lodged with the Spanish Data Protection Authority AEPD (*Agencia Española de Protección de Datos*) a complaint against a Spanish newspaper La Vanguardia and Google. He objected against the online publication of two archived pages of the newspaper of January and March 1998 and the links to these webpages which were displayed after entering his name as a query in the search engine. Those pages in particular contained an announcement for a forced real-estate auction in relation to the recovery of social security debts owed by Mr Costeja González. He argued that the proceedings and debts were resolved now for a number of years and that the ongoing reference to them is no longer

126. *AVMS Directive, Art 10.*
127. *Ibid., Art 11.*
128. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31-50.*
129. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications, OJ L 201, 31.07.2002 pp. 37-47.*
130. *Directive 95/46/EC, infra, Art 2(a).*
131. *CJEU, Case C-101/01, Bodil Lindqvist, 6 November 2003, para. 27.*
132. *Directive 95/46/EC, infra, Art 14(a).*

relevant. AEPD rejected the complaint against the newspaper La Vangardia because the information had been lawfully published but upheld the complaint against the search engine requesting the operator Google to take the necessary measures to withdraw the personal data from their index and to render access to the data impossible in the future.

The ensuing court case eventually resulted in a reference to the CJEU which interpreted the Data Protection Directive as placing a responsibility on the operator of the search engine to remove links to web pages that are published by third parties and contain information relating to a person from the list of results displayed following a search made on the basis of that person's name.[133] The Court explicitly maintains that such an obligation may also exist in a case where that name or information is not erased beforehand or simultaneously from those webpages because they were published lawfully by third parties containing true information relating to the individual personally.[134] The Court argues that the search on the basis of an individual's name enables any Internet user to obtain, through the list of results, a structured overview of the information relating to an individual on the Internet.[135] It is through the search engine that a vast number of personal information are interconnected and made available which could not have been interconnected or could have been only with great difficulty.

While the potentially serious interference with an individual's private life cannot be justified with the economic interest of the search engine operator the Court recognizes that the removal of links from the list of results could affect the legitimate interest of Internet users in having access to that information.[136] However, the Court holds that a fair balance should be sought in particular between that interest and the data subject's fundamental rights, in particular the right to privacy and the right to protection of personal data. In this regard the Court holds that whilst it is true that the data subject's rights also override, as a general rule, that interest of internet users, this balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, **according to the role played by the data subject in public life**.[137]

Contrary to what it is often referred to, this judgement does not provide for a general right to be forgotten. In order to request from a search engine operator to remove links to web pages that are published lawfully by third parties and containing true information relating to the individual personally this information must be found to be "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine"[138]. The Court makes an important distinction between the protected interests of ordinary persons and other persons that play a role in public life which should preclude leveraging the right to be delisted

133. *CJEU, case C-131/12, Google Spain SL, Google Inc. v AEPD, Mario Costeja González, 13 May 2014.*
134. *Ibid. para. 94.*
135. *Ibid. para. 80.*
136. *Ibid. para. 81.*
137. *Ibid., para. 81.*
138. *Ibid. para. 94.*

in favour of politicians and other important figures of public life. In the latter case -- very much in line with the case law of the ECtHR jurisprudence – the balancing between the Internet users' interest and that of the persons that play a role in public life would play out in favour of the public. Moreover, the legal effect of this judgement is narrow given that the obligation to remove links would only apply in the context of a search query that is based on an individual's name whereas other search terms would not affect the display of exactly the same websites. Last but not least, the website on which the personal information about an individual are published remains unaltered and can be found using different search criteria.

3. POLICY AND ENFORCEMENT OF ONLINE CONTENT REGULATION IN EUROPEAN COUNTRIES

In addition to the protections vested by the right to freedom of expression, in particular media freedoms, and to observing best practices emanating from CoE standards-setting and EU law, any state intervention with online content pose particular challenges and governance issues. This section introduces this challenges and illustrates them with some examples of policy and enforcement of online content regulation in European states.

3.1. Challenges with regulatory interventions online

As a globe-spanning ecosystem the Internet operates to an appreciating extent different to traditional distribution infrastructures which are primarily national, such as broadcasting and print media. Moreover, the open and interconnected Internet architecture offers an easy means to provide online services and to impart information across borders. A host of intermediaries facilitate different functions; most important in the context of this study are hosting providers which via their platforms host third party content that can be accessed by Internet users worldwide. Consequently, any attempt to regulate online content inevitably faces issues with jurisdiction and the potentially extraterritorial reach of local laws in addition to practical problems when implementing and enforcing local laws against foreign operators and providers, primarily.

3.2. Reconciling legislative and enforcement jurisdiction

Any legislation that aims to regulate online content needs to reconcile legislative and enforcement jurisdiction. Legislative jurisdiction which refers to a state legislature's authority to make its substantive laws apply to particular parties or circumstances is undisputed where it remains within a given state's territory or addresses its residents.[139] If the scope of application is not *expressis verbis* limited to national actors and locally hosted content, the regulation of online content, however, is bound to take a cross-border effect whenever online content crosses borders and foreign actors are involved. What is more controversial but an increasingly accepted basis for legislative jurisdiction is the prohibition of actions taken in a foreign state that cause injury or bad "effects" in the receiving state or where there is a personal link to the jurisdiction (cf. *infra* 1.3.2.).[140]

139. *Henkin, Louis et al (1993). International Law. Cases and Materials (3d ed. 1993, St. Paul: West Publ.), pp. 1046f.*
140. *Ibid.*

The jurisdiction to enforce refers to the authority of a state to use its resources to compel compliance with its law.[141] Enforcement jurisdiction is significant weakened in cross-border constellation when a party is abroad and there is no other link to the territory of a country against which enforcement actions can be directed.[142] While the international law principles of comity usually require states to assist in the enforcement of judicial decisions of third states such enforcement via proxy requires the investment of substantial resources, is time-consuming and – more generally – unfit as a mode of regulatory implementation. In some situations, third countries may refuse international cooperation. For example, in the U.S., the 2010 SPEECH Act prohibits the enforcement of foreign judgments concerning defamation in U.S. courts unless the court finds that the foreign judgment is consistent with the First Amendment.[143]

3.3. Targeting intermediaries v. ISPs' safe harbours

State interventions with Internet-mediated communications, in particular measures that have as their aim online content regulation, face a particular effectiveness tradeoff. On the one hand, with a view to enforcement targeting Internet intermediaries can be more effective than going against individual users who can be difficult to identify in the first place. Moreover, measures directed at intermediaries, such as ISPs that host third party content, can be a means to centralize regulatory intervention in an otherwise highly decentralized online environment. Quasi a wholesale approach, it would be arguably more effective to compel intermediaries' compliance with regulatory obligations instead of enforcement actions against a multitude of individual perpetrators.

However, a regulatory logic that is targeting from the outset the intermediary defies the principle that measures should aim first and foremost at actors that are primarily responsible for infringements. The mere fact that otherwise uninvolved intermediaries would be better placed to give effect to regulatory obligations would not satisfy this principle of regulatory intervention. Where secondary liability has been installed this is commonly made conditional upon additional and distinct criteria that define under which circumstances the responsibility of an intermediary arises in addition to the primary responsible actor. There must be compelling reasons why an intermediary without further ado should face the same obligations as the primary responsible actor.

Aside from these principle considerations, what can be gained from compelling intermediaries for third parties' conduct may be quickly set off by the dynamics such a regulatory approach likely generates.[144] When facing extensive liabilities intermediaries will reasonably adjust their activities with the aim to reduce their exposure to legal risks and thus introduce all changes deemed necessary to the business model. In practice, the massive volume of UGC that is uploaded on leading hosting platforms can render it impossible or economically unviable to pre-monitor all content for potentially

141. Ibid.

142. Here is a difference to the ECtHR ruling in Perrin that upheld the conviction of a French national in UK courts who was a resident in the UK for publishing obscene material on a webpage operated by a US-based Internet company but accessible by UK Internet users; cf. Perrin v. the United Kingdom, application no.5446/03, 18 October 2005.

143. Cf. Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act, P.L. 111-223, codified at 28 U.S.C. para. para. 4101-4105.

144. Cynthia Wong and James X. Dempsey. "The Media and Liability for Content on the Internet", in: Marius Dragomir and Mark Thompson (eds.), Mapping Digital Media (London: Open Society Foundation, 2011), p. 11 <https://www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-liability-content-internet-20110926.pdf> accessed 10 August 2015.

infringing substance. As an illustration, every minute 300 hours of video are uploaded to YouTube[145] and every second, on average, around 6,000 tweets are posted on Twitter.[146] For other hosting provider the situation would be similar relative to their economic capability.

Extensive pre-monitoring duties would eventually lead to the disappearance of certain publically available online services that used to cater for hosting users' content and thus provided the crucial platforms of the participatory Internet for all users. In turn, this would harm the diversity of viewpoints that characterize the online environment today, produce a chilling effect for the exercise of the freedom of expression and reinforce gatekeeper positions at the level of intermediaries.[147]

Another problem with monitoring duties is that of "private censorship" and the potential lack of judicial protection for freedom of expression. The freedom and diversity of expression on the new "global public squares" of the Internet would be seriously curtailed if the private operators that control such space (from the Facebook's and Google's of the web to national and local platforms) acted capriciously and arbitrarily in deciding what speech to greenlight or censor.

It should be recalled in this context that the save harbours from intermediary liability as laid down in the e-Commerce Directive and affirmed by the relevant CoE standard-setting documents have been calibrated precisely to reduce legal uncertainty for ISPs and create a regulatory environment which is conducive for the exercise of individual user's freedom of expression.[148]

3.4. European countries' experiences with enforcing content regulation against Internet intermediaries

The fast evolving online environment and European countries' different legal traditions have led to rather diverse legislative practices in their approaches to regulate online content and the extent to which such regulation is targeting Internet intermediaries. Member states of the EU and enlargement countries have transposed the e-Commerce Directive into their national law which provides for the liability immunity for mere conduit, catching and hosting providers subject to respective requirements being met. While this continues to be quite uncontroversial for ISPs whose activities concern mere conduit and catching, hosting providers can be much less assured that their immunity from liability for the information stored at the request of a user is not contested.

In the recent past a few European countries have initiated legal proceedings against hosting providers that were challenging various aspects of the safe harbor regimes. The ECtHR *Delfi*-judgement discussed at length above (cf. *infra* 1.2.3.) clarifies that a commercial Internet news portal providing in connection to their own editorial content a comment space for users does not meet the requirements of a passive intermediary activity and can thus not invoke the liability exceptions of "passive" hosting providers. In an earlier Italian court case involving Google's video sharing platform YouTube the appeal court did find in favour of applying the hosting provider's liability exception.

145. *Cf. <https://www.youtube.com/yt/press/statistics.html> (accessed 10 August 2015).*

146. *Cf. <http://www.internetlivestats.com/twitter-statistics/> (accessed 10 August 2015).*

147. *Ibid., p. 12.*

148. *Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee - First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (COM/2003/0702 final) p. 12f.*

Italy: The Youtube case

An illustration of the issues at stake is the Italian Youtube case in which Google executives had been held personally liable for the 2006 publication of a video clip on YouTube. The video which was taken with a mobile phone showed a boy with down-syndrome who was being beaten and insulted on a schoolyard in Italy. The video which was posted on 8 September 2008 was eventually taken down on 7 November just a couple of hours after Google was formally notified by the Italian police. Italian prosecutors brought criminal charges against four Google executives who were sentenced in 2010 in absentia by the Milan Court of First Instance for defamation and failure to exercise control over personal data.149 In this trial, the court did not accept that Google as a hosting provider should not be held liable for third party content as provided for in the Italian equivalent of the e-Commerce Directive. The court followed the prosecution's argument that Google should have known better and acted on the video clip which gained notoriety as a most-viewed clip and had been a subject of heated controversy in Italy for some time already.

In 2012, the Milan Court of Appeal overturned the initial decision, subsequently backed in 2014 by the Italian Supreme Court (the Court of Cassation), on the grounds that Google's Youtube is a host provider merely storing content posted by its the users and Google employees had no prior knowledge of the illicit nature of that video.150 Moreover, it was resolved that Google executives had committed no criminal offence because ISPs have no obligation to inform their users about data protection obligations and due to the lack of knowledge about the existence of the video. The Court resolved that the uploader is exclusively responsible for the indeed grave interference into the personality rights of the victim of this incident.

In many EU countries, the judiciary has embraced the distinction between "active" and "passive" hosting intermediaries that is decisive for the application of the liability exemption in Art. 14 of the e-Commerce Directive as transposed into their national laws. However, the criteria national courts have successively developed are diverging in detail.[151] This case law mainly emanates in the context of copyright enforcement actions but the distinction drawn between "active" and "passive" hosting intermediaries can extrapolate to online content that is infringing an individual's reputation and other personality rights. Italian courts, for that matter, are more strict in finding in favour of an "active" provider which is treated as a publisher and does not benefit from the liability exception when it modifies the content, categorizes it or retains control over what is admitted to its services.[152] For French courts a hosting provider does not automatically become an "active" intermediary because revenues are

149. Milan Court of First Instance, judgment no. 1972 of 4 February 2010; cf. John Hooper, "Google executives convicted in Italy over abuse video" The Guardian, 24 February 2010, <http://www.theguardian.com/technology/2010/feb/24/google-video-italy-privacy-convictions> accessed 10 August 2015.

150. Eric Pfanner, "Italian Appeals Court Acquits 3 Google Executives in Privacy Case" The New York Times, 21 December 2012, <http://www.nytimes.com/2012/12/22/business/global/italian-appeals-court-acquits-3-google-executives-in-privacy-case.html> accessed 10 August 2015.

151. Cf. Juan Benjumea Moreno, "Publisher or Technical Provider? Monitoring as Editorial Control and the "Safe Harbor"of Art. 14 E-Commerce Directive", Jura Falconis 49(4), pp. 663-683, 675.

152. Ibid. with reference to Tribunale di Roma, RTI v Worldstream, 26 October 2011; RTI v YouTube, 16 December 2009; Tribunale di Milano, RTI v Italia On Line, 16 of June 2011.

generated from advertisement placed on the service.[153] The Court did also regard re-encoding, formatting and organizing of video content as merely technical operations which are below the threshold of what constitutes editorial choice about third party content.[154]

Only the UK has enacted a dedicated defamation law in 2013 after a long and careful legislative process.[155] This reform had been guided by an effort to strike the right balance between the right to freedom of expression and the protection of reputation in the light of the new online environment. Among others, it regulates under which circumstances an action for defamation is brought against the operator of a website in respect of a statement posted on the website:

England and Wales: Art. 5 of the Defamation Act: Operators of websites

(1) This section applies where an action for defamation is brought against the operator of a website in respect of a statement posted on the website.

(2) It is a defence for the operator to show that it was not the operator who posted the statement on the website.

(3) The defence is defeated if the claimant shows that—

(a) it was not possible for the claimant to identify the person who posted the statement,

(b) the claimant gave the operator a notice of complaint in relation to the statement, and

(c) the operator failed to respond to the notice of complaint in accordance with any provi sion contained in regulations.

(4) For the purposes of subsection (3)(a), it is possible for a claimant to "identify" a person only if the claimant has sufficient information to bring proceedings against the person.

(5) […]

(6) Subject to any provision made by virtue of subsection (7), a notice of complaint is a notice which—

(a) specifies the complainant's name,

(b) sets out the statement concerned and explains why it is defamatory of the complainant,

(c) specifies where on the website the statement was posted, and

(d) contains such other information as may be specified in regulations. […]

(11) The defence under this section is defeated if the claimant shows that the operator of the website has acted with malice in relation to the posting of the statement concerned.

(12) The defence under this section is not defeated by reason only of the fact that the operator of the website moderates the statements posted on it by others.

153. *Ibid, p. 676, with reference to Tribunal de grande instance de Paris, TF1 v. Dailymotion, 13 September 2012, <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3486> (accessed 10 August 2015).*

154. *Ibid.*

155. *UK Defamation Act 2013 < http://www.legislation.gov.uk/ukpga/2013/26/contents/enacted> (accessed 10 August 2015).*

Whereas the removal of illegal online content either after a court order or pursuant to a notice-and-takedown procedure is a common practice in most European countries, the blocking of access to websites is a much more selectively applied measure that is reserved for the most severe incriminated content. For example, in a range of European countries, e.g. in France, Germany, Switzerland, and the United Kingdom, website blocking is used to combat the sexual abuse of minors by preventing the dissemination and access to child abuse images and content. Many European countries have no general legislative provisions on the blocking of online content or no legislation that would authorize the wholesale blocking of websites.[156] The following example of Turkey is thus not representative of European legislative practices but an outlier of state intervention into the open Internet.

Turkey, a member state of the Council of Europe, has enacted specific laws directed at websites hosting third party content and here in particular UGC. The country has a track-record for successively passing highly restrictive Internet laws in 2007, 2014 and 2015, blocking entire social media sites and leading the charts for content removal requests with global websites.[157] In addition to lowering the procedural safeguards for such interferences Turkey has also complemented the more archetypical removal of prohibited content with blocking access to websites, sometimes whole domains. In most cases, content removal request and blocking orders target ISPs and content intermediaries directly.

Turkey: Law no. 5651 of 4 May 2007 on regulating Internet publications and combating Internet offences

Already in 2007 Turkey enacted its Internet Law No. 5651.5 which imposed new obligations on websites which provide own content or host third party content to block websites and to take down unlawful content as enumerated by the law.[158] The catalogue of unlawful content comprises of incitement to suicide; sexual abuse of children; facilitation of the use of narcotics; provision of substances harmful to the health; obscenity; prostitution; facilitation of gambling; the crimes against Atatürk; and betting and gambling. The law grants authority to an implementing agency, the Presidency of Telecommunication and Communication (TIB), to issue administrative orders to local and foreign online providers. In addition, data retention by ISPs and website providers is mandatory under the law in order to facilitate prosecution.

In two decisions, in April and May 2014, ruled the Turkish Constitutional Court that blocking access to Twitter and YouTube respectively violated freedom of expression.[159] In the latter YouTube-case the the administrative authority TIB did not comply with the judgement of the Ankara Administrative Court to lift its blocking order.

156. *Yaman Akdeniz, Freedom of Expression on the Internet: A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States (Vienna: OSCE, 2011) < http://www.osce.org/fom/105522?download=true > (accessed 10 August 2015).*

157. *Mustafa Akgül and Mehli Kırlıdoğ, "Internet censorship in Turkey", Internet Policy Review 4(2), DOI: 10.14763/2015.2.366*

158. *Jeffrey Rosen, "Google's Gatekeepers", New York Times 28 November 2008 <http://www.nytimes.com/2008/11/30/magazine/30googlet.html> (accessed 10 August 2015);*

159. *Zeynep Oya Usal, "TR-Turkey: Constitutional Court declares that YouTube ban is unconstitutional", IRIS 2014-7/33.*

On 2 October 2014, Turkey's Constitutional Court annulled most parts of a new law which was passed in September 2014 as an amendment to the Internet Law 5651.5.[160] The aim of this new piece of legislation was to protect the dignity and privacy of individuals who become victims of defamation on the Internet. It authorized the Turkish Telecommunications Authority (TIB) to order ISPs to block any websites without a court order within four hours of a request, and to collect and store all user logs. After the partial annulment of the new law the previous situation has been restored which requires a court order in order to compel ISPs to block websites.

In March 2015, the Turkish government passed its latest Internet-related legislation which allows for a temporary ban of websites for the duration of up to 48 hours and the blocking of anonymous comments made online, mainly in an effort to reign into Twitter.[161]

In December 2012, the ECtHR ruled against Turkey in a case concerning the powers to block Internet access under law no. 5651 of 4 May 2007 on regulating Internet publications and combating Internet offences.[162] The facts of the case concerned the wholesale blocking of Google Sites – a service which hosts users' blogs and websites – in the context of criminal proceedings against the owner of one website, who was accused of insulting the memory of Atatürk. The blocking order by a local court, however, authorized the implementing authority TIB to block all access to Google Sites, which hosted not only the offending site but also the applicant's site, among others. Although neither the hosting provider Google Sites nor Mr Yıldırım's site were the subject of court proceedings the blocking of the entire domain made it technically impossible to access any of those sites.

The Court qualified the collateral effect of the blocking order by the public authorities as a restriction on Internet access which interfered with the applicant's right to freedom of expression.[163] Such restriction on access to a source of information – the Court reiterated -- was only compatible with the ECHR if a strict legal framework was in place "ensuring both, tight control over the scope of bans and effective judicial review to prevent any abuse of power."[164] The Court concluded that the interference was not foreseeable and did not afford the applicant with the degree of protection to which he was entitled by the rule of law in a democratic society. Besides, the Court also pointed out that the right to freedom of expression in Art. 10(1) ECHR applies "regardless of frontiers". Consequently, the Court ruled that the over-blocking in this case violated Art. 10. Regardless, Turkish authorities continue blocking entire websites on the basis of Internet Law No.

160. A.A., "Turkish Constitutional Court strips Internet authority of right to close websites" Hurriyet Daily News 2 October 2014 <http://www.hurriyetdailynews.com/turkish-constitutional-court-strips-internet-authority-of-right-to-close-websites.aspx?pageID=238&nID=72479&NewsCatID=339> (accessed 10 August 2015); Humeyra Pamuk, "Turkey's top court annuls part of law tightening Internet controls –media" Reuters 2 October 2015 <http://uk.reuters.com/article/2014/10/02/uk-turkey-internet-idUKKCN0HR20B20141002> (accessed 10 August 2015).

161. Gulsen Solaker and Jonny Hogg, "Turkey proposes tighter internet law, pursues Twitter critic", Reuters, 22 January 2015 <http://www.reuters.com/article/2015/01/22/us-turkey-internet-idUSKBN0KV1Y720150122> (accessed 10 August 2015); Emre Peker and Sam Schechner, "Turkey Briefly Blocks YouTube, Twitter Access and Threatens Google Ban", The Wall Street Journal, 6 April 2015 <http://www.wsj.com/articles/turkish-court-bans-access-to-internet-sites-over-hostage-crisis-content-1428325451> (accessed 10 August 2015).

162. ECtHR, Ahmet Yildirim v. Turkey, application no. 3111/10, 18 December 2012.

163. Ibid., para. 56.

164. Ibid., para. 64.

5651.5 which produces has a collateral effect on numerous other sites hosted at the same service. Aside from the issue of over-blocking there are a host of other aspects with the application of the Turkish Internet law which do not conform with best practices of online content regulation and are criticized for restricting the right to freedom of expression in multifarious ways.

In a number of European countries, individuals took legal actions against search engine listings of links to content that were deemed to infringe personality rights.[165] In implementing the 2014 CJEU judgement in *Google Spain* Google offers a form to residence in EU member states to request delisting which Google complies with the requirements for delisting are met (cf. *infra* 2.2.4.). Also a member state of the Council of Europe, Russia has recently passed a law which targets Internet search engines.

Russia: Internet Privacy Law

In July 2015, the Russian parliament passed the Internet Privacy Law arguably emulating the CJEU precedent in *Google Spain*. The new law once taking effect in January 2016, after being signed by President Vladimir Putin, grants Internet users the right to request the delisting of links from the search results to websites with users' personal information that is incorrect or "no longer relevant because of subsequent events or actions".[166] Apart from local search engines, the law would apply to foreign search providers as well if their advertisement targets Russian users.

3.5. Social media dynamics and unwanted effects

Online media and Internet communications are known to develop their own dynamics and – at times – even influence the agenda of mass media. The virality of online content connotes a situation in which information quickly spreads in social media and gains increasing popularity. Oftentimes negative or revelatory information about figures in the public interest, such as politicians, and about celebrities have a tendency to seed quickly in social media until it is eventually reported in mass media. Named after the singer Barbra Streisand what has become known as the "Streisand" effect describes how efforts to suppress a piece of online information can contribute to raising the interest of Internet users.[167]

165. E.g., the litigations brought by Max Mosley against Google in Germany, France and the UK which are now settled in a confidential agreement, cf. Ulrike Dauer and Elisa Fleisher, "Former Formula One Chief Max Mosley Settles Legal Dispute With Google" The Wall Street Journal, 15 May 2015 <http://www.wsj.com/articles/former-formula-one-chief-max-mosley-settles-legal-dispute-with-google-1431702038> (accessed 10 August 2015).

166. A.A., "Russian parliament approves Internet privacy bill", Reuters, 3 July 2015, <http://www.reuters.com/article/2015/07/03/us-russia-internet-idUSKCN0PD1OQ20150703> (accessed 10 August 2015.

167. A.A., "The Economist explains: What is the Streisand Effect?" The Economist 15 April 2013 <http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-what-streisand-effect> accessed 10 August 2015; Mario Cacciottolo, "The Streisand Effect: When censorship backfires" BBC 15 June 2012 <http://www.bbc.com/news/uk-18458567> accessed 10 August 2015.

The "Streisand" effect

The California Coastal Records Project is an award-winning online database documenting in thousands of photographs California coastline. One of these photographs captures the residence of Barbra Streisand in Malibu. In relation to this image Streisand sued the photographer, inter alia, for invasion of privacy and asked for $50 million in damages. Before the lawsuit was filed, only six times the photo of Streisand's residence had been downloaded, twice by her lawyers.[168] The publicity, however, surrounding the legal action led to the photo being downloaded over 420,000 times within a month. In December 2003, the lawsuit was dismissed.[169]

There are a number of examples, where authorities, politicians and celebrities in European countries have been caught by similar events when their endeavors to remove online content was actually drawing attention to it. A famous football player in the UK for that matter sued Twitter after a user revealed that he was the subject of an anonymous privacy injunction preventing the publication of details regarding an alleged affair with a model. When this became public more than 75,000 Twitter users posted the footballer's name and affair claim who eventually gave in to his name being published in this context.[170]

4. CONCLUSIONS

Both the EU and the CoE, through their different bodies, have revealed similar understanding of what freedom of speech in the online environment entails and how law-makers, regulators and the judiciary should operate in order not to stifle the free circulation of voices and opinions on the Internet.

The two institutions share a similar favour towards models of self- and co-regulation. For the Internet to be an open a participatory environment, regulation should stem from bottom to top to largest possible degree. The relevant institutions should try and involve the relevant industry representatives, journalist and judiciary representatives, as well as the civil society, in the law-making process. Given the increasingly scattered and diverse nature of the media industries in these days, such a feature is key to ensure that no unduly limitations on the flow of information on the Web will not be imposed by the means of legal norms.

The impact and significance of new communication technologies within the public sphere is also understood in similar terms. The fundamental role of journalist for the democratic debate, and the need for strong legal safeguards, is acknowledged by both the EU and the CoE; further to this, the possibilities offered by the Web 2.0 for ordinary citizens to have their voices heard by large audiences have made both these institutions become increasingly oriented towards a technologically-neutral regulatory approach, capable of protecting voices and opinions irrespectively

168. Sue Curry Jansen and Brian Martin (2015) "The Streisand Effect and Censorship Backfire" International Journal of Communication 9 (2015), 656–671.

169. Ibid.

170. Mario Cacciottolo, "The Streisand Effect: When censorship backfires" BBC 15 June 2012 <http://www.bbc.com/news/uk-18458567> accessed 10 August 2015.

of the medium of choice. As a result, both the EU and the CoE agree that the Internet should not be subject to any stricter rules than the analogue media.

Furthermore, the active rise of user-generated content has also raised attention towards the extension of legal protections in favour of ordinary citizens who partake in the public debate through their personal blogs, social network profiles etc., and should not face unduly legal threats because of such activities. Both the EU and the CoE have been recently expanding their analytical framework of communication rights in order to capture this new social behaviours and their need to be protected by the law. It follows from this that providing for suitable legal frameworks for freedom of speech to flourish in the media sphere (irrespectively of the technology used and of the possible professional qualifications, or lack thereof, of the persons who engage in such activities) is not just an option, but a specific obligation on national authorities; in particular, decriminalizing defamation and avoiding similar measures that could potentially spark a chilling effect, such as disproportionate civil sanctions, represent one of the most urgent needs that national law-makers should fulfill.

The combined orientations of the ECtHR case-law and the Recommendations of the Parliamentary Assembly and the Council of Ministers outline a coherent and comprehensive recommended regulatory frameworks to apply to the regulation of online content at the national level. Such recommended norms include:

- in today's digital environment, literally every individual could reach out to unprecedented large audiences: this does not entail that every private citizen should be considered along the same lines as professional media outlets – and subject to the same legal rules. National law-makers should clarify as much possible what kind of activities amount to professional media services and what do not. Suggested indicators include the likes of editorial control, outreach, respect of professional and ethical standards among others. From such classificatory effort, it follows that different categories (professional media outlets, UGC, intermediaries, etc.) can be regulated differently, although a minimum threshold of protection of freedom of speech must be granted to all.
- The respect of third parties' right to reputation can be a legitimate limitation to free speech. However, the balance between the two should be assessed narrowly and strictly, particularly in light of the fundamental contribution to democracy offered by the media sphere. The Court has considered that the boundaries of legitimate speech are particularly broad under a number of circumstances, such as:
    - when a matter of political relevance or public interest is at stake;
    - when the alleged defamatory content concerns value-judgments, which contrary to facts cannot be proven true;
    - when the allegedly defamed person is an elected politician, from whom a greater level of tolerance can be expected;
    - when the alleged defamatory content concerns the government as an institution: in such cases, no special protection should be granted to the members of such body, compared to other ordinary citizens;

On the contrary, the judiciary has been considered to deserve a higher threshold of protection than the executive.

- The legal protection of journalists should apply across all available technologies, irrespective of the medium of choice;
- Conversely, high standards of professional ethics can be legitimately expected from individuals operating as professional journalists; the same standards cannot be applied to private citizens who disseminate their UGC on the web.

A further strand of indications focuses on contemporary questions related more directly with the rise of digital technologies. Such indications include:

- For online archives, the Court has indicated, at present time, a preference for the multiple publication rule. However, the principle seems to be mitigated by a major caveat (the limited period of time between the original publication and the actions brought against the media outlet following retrieves of the content at stake) in order to avoid a chilling effect on archives. To any extent, however, online newspapers cannot be requested to delete their archives.
- Jurisdiction represents another emerging issue of Internet regulation. The Court has identified territory and effective control as criteria for a State to exert its jurisdiction (and also apply its substantive laws) over a dispute. Relevant criteria could be of an objective (e.g. the availability of the content at stake within the State's boundaries) as well as of a subjective (e.g. the defendant's awareness of the local laws and the foreseeability of their application) nature.
- While a right to anonymity online does not seem to exist as such, on the other way round ISPs are under a specific obligation to protect their users' identity as a general principle (although exceptions can apply, for instance in the case of criminal prosecutions) and national law-makers should not impose obligations on ISPs to reveal sensitive data of their users to the authorities or third parties.
- As a general principle, the liability of ISPs for any wrongdoings committed through their facilities or services by third parties should be excluded. However, partial exceptions can apply to the case of active intermediaries, (i.e. the ISP took a more active role in the dissemination of the illegal content than just acting as a mere conduit), in the case the ISP was aware of the wrongdoing and, following such awareness, yet did not react readily to remove the relevant content.

European best practice thus forestall any one-size-fits-all measures against defamatory online content and need to be flexible so as to take into account the particular circumstances of the expression and personal characteristics of the parties concerned. Under a graduated and differentiated approach, internet intermediaries' responsibility for hosting online content of third parties has to be determined according to the specific nature of the service they offer. The Council of Europe standard-setting documents and EU legislation provide for a ***limitation of liability and exclude a specific duty to monitor*** the information they receive from users on part of hosting providers which in their role and function remain passive service providers.

Both the EU and the CoE agree to exclude intermediaries' liability as a matter of general principle.

However, they also both introduce some partial and specific limitations to the principle. Under both the EU and the CoE systems, the lack of knowledge of the illegality of the content transmitted is a sufficient defence to exclude the intermediary's liability. Further to this, the CJEU has been seemingly even more proactive in requesting that intermediaries should have taken some form of active involvement in the wrongdoing in order to be held liable. On the other way round though, the e-Commerce Directive has been more explicit in excluding interediaries' liability for a number of activities such caching, hosting, and acting as mere conduit. In a similar sense, the EU has also more explicitly – albeit being again in line with the CoE on this – excluded the possibility for national law-makers to lawfully impose duties to monitor the legality of online content on intermediaries.

The distinction between active and passive ISPs has some echoes in the European Court of Human Rights Grand Chamber judgement in *Delfi v Estonia* and is thus poised to become the transversally adopted test by both the European courts. *Delfi* concerns a case where the defendant played an active role in facilitating the posting of unlawful third-party comments and was thus treated like a "professional" publisher with all responsibilities for the content on its website. This judgement, however, does not overturn the principle that online intermediaries that provide for the hosting services would not be liable for third party content. Despite the differences at national level and with the notable exception of Turkey, European countries' legislation does not establish a general liability regime for providers of hosting services.

Public policy considerations of interventions against online intermediaries, notably hosting providers, and a review of selected European countries experiences underscore the importance of striking the right balance between the protection of freedom of expression online and the reputation and rights of others. Only a graduated and differentiated approach which takes into account the role and activities of intermediaries in relation to online content is capable of ensuring the benefits of the participatory Internet for all users by preserving an open environment to freely impart and seek information online. This involves that Internet intermediaries are not deputized to monitor third party content *per se*, except where in exceptional circumstance certain providers qualify as media or "active" intermediaries.

PART II
ALBANIA AND ONLINE CONTENT REGULATION

According to International Telecommunication Union Data, 60.10% of the Albanian population had access to the Internet as of June 2014, including fixed and mobile connections.[171] This penetration rate places Albania in the mid-range of the Southeastern European region and it is actually slightly higher than those of its EU neighbors Italy, Greece and Bulgaria. The rate of broadband coverage is another matter, reaching only some 180,000 households by the end of 2013.[172] However, since 2011 there has been an explosion in the number of mobile phone users with access to 3G technology, reaching 1.23 million in 2013.[173]

Successive Albanian governments have generally adopted a liberal approach toward freedom of expression on the Internet. There is no evidence of systematic or even sporadic filtering or blocking of online content, and no requirements for online media and information websites to register or obtain any sort of operating permission by the authorities.[174] Furthermore, it has been noted that "online journalism and online media have offered a greater degree of freedom" to media professionals, especially vis-à-vis media owners and their interests, which tend to cast a longer shadow in the print and electronic media environments.[175]

In Albania, online media is generally dominated, with few exceptions, by the websites of the leading traditional print and broadcast media. Online-only news and opinion sites, while offering a distinct voice, have not been able to significantly alter the news agenda and investigative journalism remains quite limited, both online and offline. The overall media environment is characterized by highly partisan approaches, which tend to reflect the high level of polarization within the country's political class and its democratic maturity deficits.[176]

Albanian users can access information and provide UGC freely to Albanian and foreign websites and platforms. The dominant language of online media targeting Albanian users is Albanian. Besides, leading Albania-based outlets can attract significant following from Albanophone users in Kosovo and the former Yugoslav Republic of Macedonia, as well as the substantial Albanian diaspora in Europe and beyond.

A few of the global platforms, such as Google, also provide localized versions of their services. Social networks sites and online platforms for professional content and UCG are among the most widely used online offers in Albania. Among social networks, Facebook is by far the most popular in the

171. *Cf. Internetworldstats.com*

172. *Electronic and Postal Communications Authority (AKEP), 2013 Annual Report (in Albanian) <http://www.akep.al/images/stories/AKEP/publikime/raporte/RAPORTI-VJETOR-2013.pdf> (accessed 10 August 2015).*

173. *Ibid..*

174. *Remzi Lani (ed.), Balkan Media Barometer. Albania 2013, pp. 20-21 (Tirana: Friedrich Ebert Foundation, 2013) <http://www.institutemedia.org/Documents/PDF/FES%20-%20BMB%20Albanian%202013%20book%20ENG%2003_12_2013.pdf> accessed 10 August 2015.*

175. *Ibid. at 60.*

176. *Ibid.*

country, with some 1,340,000 registered users in early 2015; 73 percent of its users belong to the 18-34 age group.[177] YouTube and, to a lesser extent, Twitter also have extensive user bases.[178] Empirical data about whether, where and how often Albanian users contribute and share UGC is not available.

1. POLITICAL DISCOURSE AND DEFAMATORY SPEECH ONLINE

There is also a dearth of reliable data on various aspects of the Albanian online news and information environment. There have also been, to our knowledge, no court proceedings or judgments related to online defamatory user comments as such. That notwithstanding, there is a good deal of negative commentary and public debate about various forms of perceived abuses in this space, including invasion of privacy, hate speech and verbal threats, personal attacks, and a general lack of quality UG comments.

According to a recent survey of 39 Albanian online media and opinion sites, five indicated that they allow immediate publication of reader comments without any moderation; twelve answered that they allow immediate posting, followed by post-publication moderation; eighteen indicated that reader comments can only be posted following approval by a moderator; and four did not allow for any user comments.[179] The responses would suggest that the great majority of news sites engage in some kind of moderation, either pre- or post-publication.

However, existing measures seem to have little practical effect. A cursory overview over the leading/most popular Albanian-language sites reveals low numbers of edited comments and an abundance of off-topic and personal attack commentary. This suggests, in turn, that either the sites do not actually employ the degree of oversight they claim to or they adopt a fairly high bar for censoring user comments. There is also, with very few exceptions, a significant absence of properly elaborated community standards to guide the user commentary and reporting mechanisms on websites are rather the exception than the rule. Some observers have, in fact, noted a trend toward a lighter touch in moderating comments in recent years, perhaps due to competitive pressures and/or financial inability to deploy sufficiently-staffed moderation teams. A few site managers have argued that unfettered user comments tend to generate greater traffic.[180]

While the link between commercial strategies and moderation practices is not limited to Albania, it is important to highlight that online services of global appeal in general tend to have adopted community standards and reporting mechanisms.

---

177. Rrapo Zguri, The Development of the Internet and Social Media in Albania, sec. 3.1. (Tirana: Albanian Media Institute, forthcoming, copy on file with the authors).

178. Ibid.

179. Ibid., p. 20.

180. Balkanweb.com and shekulli.com.al have been offered as examples of this trend. See Zguro, ibid, p. 21.

2. THE CONSTITUTION OF ALBANIA

The 1998 Constitution of Albania provides for free speech interests in succinct terms, noting simply that freedom of expression, including "freedom of the press, radio and television," is guaranteed.[181] "Prior censorship of the means of communication" is prohibited.[182] A separate provision guarantees the right "to obtain information on the activity of state bodies and persons exercising state functions."[183]

There is no provision establishing a general right to reputation. Art. 35(1) guarantees the right of everyone "not to be forced, except when required by law, to make public any data related to his person." Art. 36 guarantees the "freedom and secrecy of correspondence or any other means of communication."

There are no special provisions concerning the limitations of these rights. Instead, a general clause provides that restrictions on constitutional rights and freedoms "may be established only by law, in the public interest or for the protection of the rights of others. Any restriction must be proportional to the condition that has dictated it."[184] The second section of Art. 17 specifies further that restrictions on fundamental rights "may not violate their essence" and – in a rather unique provision – that they may not "be greater than the restrictions provided for in the European Convention on Human Rights."

By virtue of this provision, the Albanian Constitution has essentially incorporated the restrictions scheme of the European Convention and, by implication, the relevant jurisprudence of the European Court of Human Rights, into the country's highest law. The national courts are, of course, free to be more protective of guaranteed constitutional rights than the Strasbourg system, but not less so. This unusual arrangement has left a number of open questions, such as what to do when one of the two systems (the Albanian Constitution and the ECHR) guarantees a right not specifically provided for in the other;[185] or when the courts are required to resolve clashes between two or more fundamental rights of the same level, as is often the case in disputes involving free speech and privacy or reputational interests.

Of special interest for our purposes is the prohibition in Art. 22 on prior censorship, which seems to allow for no exceptions. However, when read together with Art. 17, it is more likely to be construed by Albanian courts in line with ECHR jurisprudence, permitting certain forms of prior restraint in exceptional circumstances clearly delineated by law.[186]

A Constitutional Court is established, but with limited powers of adjudication on fundamental rights matters insofar as it can only hear "complaints by individuals for the violation of their constitutional rights *to a due process of law*."[187] This has generally been interpreted as covering procedural (rather than substantive) due process rights, which means that individuals cannot take a pure freedom of

181. *Art. 22.*

182. *Art. 22.3.*

183. *Art. 23.*

184. *Art. 17.1.*

185. *There are multiple instances of less than complete overlap: the catalogue of rights in the Albanian Constitution is longer and more comprehensive than the ECHR's. On the other hand, there are a few ECHR rights, such as privacy, that are not explicitly included in the Constitution.*

186. *Cf. e.g. the case law summary in ECtHR, Ahmet Yildirim v. Turkey, application no. 3111/10, 18 December 2012.*

187. *Art. 131(f), emphasis added.*

expression case to the Constitutional Court, unless and only insofar as it involves a due process claim. Therefore, the Supreme Court maintains the last word on substantive fundamental rights disputes arising from individual complaints, including in the context of defamation cases.

However, the Constitutional Court can hear questions affecting substantive fundamental rights in abstract or incidental review proceedings regarding the constitutionality of a statute (law) or other act of government. Such actions can be brought by other branches of government, ordinary courts and even non-governmental entities on questions related to their mission.[188] In practice, however, no such cases have been brought involving matters of defamation law and online freedom of expression. As we will see in the next sections, recent changes of the country's defamation law regime have been implemented through legislative changes.

3. LEGISLATION IN FORCE

Since the almost complete repeal of the much-criticized 1993 press law, Albania has had a media statute composed of a single provision that states simply: "The press is free. Freedom of the press shall be protected by law."[189] The rest of the statute was abrogated in 1997, after the civil unrest that followed the massive collapse of the Ponzi schemes, as a signal of clear departure from the media policies of the previous government. Whatever one might think of such political symbolism, in legal terms it means that current Albanian law includes no clear provisions on matters of editorial responsibility and related questions.

As a result, the general provisions of the penal and civil codes on, respectively, criminal and civil liability for defamatory publications apply. These include no specific provisions governing secondary or contributory liability for unlawful publications, such as involving the liability (or not) of distributors, sellers and others not bearing primary publication responsibility. Especially the latter contributes to uncertainty about the legal responsibilities (if any) of online platforms hosting and distributing UGC.

This situation did not change substantially with the adoption of the 2013 Audiovisual Media Act which includes a detailed provision on the right of reply in audiovisual media.[190]. Only services that meet the definition of audiovisual media are required to comply with the right to reply which does not concern most online services. This is in line with the EU acquis pursuant to the Audiovisual Media Services Directive (cf. *infra* 2.2.2.).

In early 2012, the Albanian Parliament adopted significant reforms to the country's civil and criminal defamation laws. This was the result of a multi-year campaign by civil society groups and like-minded parliamentarians, which for the most part helped to bring the existing legal framework into closer alignment with relevant European standards.[191]

---

188. Art. 134.

189. Law on the Press No. 7756/1993, as amended by Law 8239/1997.

190. Art. 53.

191. Cf. Darian Pavli, "Running the Marathon: The Effort to Reform Albania's Libel Laws," <http://www.opensocietyfoundations.org/publications/arguments-effort-reform-albanias-libel-laws> (accessed 10 August 2015). For the sake of disclosure, one of the authors of this paper was closely involved with the elaboration of the 2012 defamation law amendments.

3.1. Penal Code

3.1.1. Defamation

Perhaps the most significant change in the Penal Code (PC) was the complete repeal of three offenses concerning defamation of public officials, including the president of the republic.[192] Public officials no longer enjoy any special protections in this respect, including no involvement by the police or public prosecutors in cases in which officials claim to be victims of criminal defamation. They must prosecute such cases privately, like ordinary citizens, following Council of Europe standards and jurisprudence by the European Court on Human Rights.

Also significant was the abrogation of prison terms for defamation offenses. However, the reform fell short of complete decriminalization. Insult (Art. 119 PC) and libel (or more precisely, calumny, Art. 120 PC)[193] were maintained as misdemeanors, subject to a fine. In fact, maximum fine amounts were increased to 3 million leke (ca. 21,000 Euros). In addition, a conviction under either article will still produce a criminal record.

An amendment to the old Art. 120 PC clarified that, to be found guilty of calumny, a defendant must have acted with "knowledge of the falsity" of the defamatory utterances. This is a fairly high bar for the prosecution of such offenses. However, it is not applied strictly by the courts in practice, making it easier to file and proceed with charges than the definition of the offense would suggest (more on this below).

3.1.2. Hate speech

The Penal Code includes a number of provisions that criminalize: the incitement of hatred among racial, ethnic and religious groups;[194] propagation of hatred, defamatory statements and instigation of violence against "parts of the population";[195] incitement of terrorist acts;[196] and desecration of state symbols exposed by public institutions.[197]

In November 2008, a number of offenses committed "through computer systems" were introduced. These include:

- denial or apology of genocide or crimes against humanity, punishable by three to six years of imprisonment;198
- dissemination of racist or xenophobic statements, punishable by a fine or up to two years of imprisonment.199 The provision does not define what constitutes a racist or xenophobic statement;

---

192. Cf. Law No. 23/2012 on Certain Additions and Amendments to the Penal Code (adopted on 1 March 2012, entered into force on 11 April 2012)

193. Calumny is defined as "[t]he deliberate dissemination of utterances as well as any other information that harms a person's honour and dignity, committed with knowledge of their falsity."

194. Art. 265 PC.

195. Art. 266 PC.

196. Art. 232/a PC.

197. Art. 268 PC, as amended.

198. Art. 74/a PC. Interestingly, this is an offense only if committed through "computer systems."

199. Art. 119/a PC.

– deliberate insults against a person "because of his ethnic, national, racial or religious affiliation", punishable by a fine or up to two years of imprisonment.[200]

The definition of these offenses committed "through computer systems" suffers from significant overbreadth and lack of qualification. As such, they arguably raise serious questions of compatibility with ECHR's freedom of expression (Art. 10) jurisprudence and, therefore, Art. 17 of the Albanian Constitution.[201] In addition, there has been hardly any judicial practice interpreting and applying these provisions, which conversely reflects a lack of prosecutions under the new "computer systems" offenses.

3.2. Civil Code

Since the introduction of the Italian-influenced 1994 Civil Code (CC), civil defamation claims in Albania have been governed by its Art. 625, which covers all forms of moral (or non-pecuniary) damage. However, the original text of Art. 625 was very broad in its formulation, providing no specific guidance for the resolution of civil defamation disputes and leading to significant variance and inconsistency in the case law. The 2012 amendments[202] to the Civil Code introduced a number of important clarifications in this respect.

First, amendments to Art. 625 clarified the establishment of causes of action for harm to one's honour, reputation or personality. They also added new causes of action for violation of the right to one's name[203] and breach of privacy torts.[204]

Secondly, a new Art. 647/a introduced detailed criteria for assessing the question of civil liability for harm to one's honor or reputation, as well as the amount of compensation, where appropriate. As a general principle, any compensation granted under the new provision should be proportionate and seek to "reinstate the right that has been violated," rather than punish the defendant.[205]

In addition, the new provision sets out eleven specific, non-exhaustive factors to be taken into account by the courts in determining liability. These include: whether the allegations constitute fact or opinion; whether they are true or false, or constitute accurate references to third-party statements; whether they relate to "matters of public interest, or persons in government functions or running for election"; and whether the author has complied with any relevant rules of professional ethics (e.g. in the case of media and information professionals).[206]

With respect to the amount of compensation awarded, courts are also required to consider whether the damages "may significantly worsen the financial condition" of the defendant. This would apply,

---

200. Art. 119/b PC.

201. Cf. e.g., on the question of denial of genocide, ECtHR, Perincek v. Switzerland, Application No. 27510/08, judgement of 17 December 2013; cf. Dirk Voorhoof, "European Court of Human Rights: Perinçek v. Switzerland", IRIS 2014-2:1/1 <http://merlin.obs.coe.int/iris/2014/2/article1.en.html> (accessed 10 August 2015).

202. Cf. Law No. 17/2012 on Certain Additions and Amendments to the Civil Code (adopted on 16 February 2012, entered into force on 29 March 2012).

203. Art. 625(c) CC, as amended.

204. Art. 625(ç) CC, as amended.

205. Art. 647/a CC, as amended.

206. Ibid.

for example, where high damages might cause a media outlet to go bankrupt.[207] Finally, the statutory limitation period for bringing defamation and privacy actions was reduced from three years to one year.[208]

When the 2012 reforms were being debated in parliamentary committees, the need to regulate questions of online defamation was briefly considered but ultimately dropped as premature. It appears that the question has forced itself back into the parliamentary agenda in short order (more on this below).

3.2. Electronic Commerce Act (ECA)

In 2009, Albania adopted an Electronic Commerce Act, which according to the government was "fully approximated" with the EU's e-Commerce Directive following a spate of amendments to the original act introduced in 2013. [209]

The ECA follows the structure and largely the substance of the e-Commerce Directive, including with respect to the limitations of liability for pure conduit, caching and hosting service providers.[210] Unlike the e-Commerce Directive, the ECA makes special provision for the liabilities of information location services (search engines), which are subjected to a notice-and-take down regime similar to that of hosting providers.[211]

Like the e-Commerce Directive, the Albanian ECA makes clear that service providers are under no general duty of monitoring and prevention of illegal activities by their uses.[212] However, they are required to provide the "responsible authorities," upon request and "in compliance with the legislation in force," with access to any data that allows the identification of their users.[213]

Some important aspects of the e-Commerce Directive liability regime have been lost or changed in translation, however. This includes the concept of "effective knowledge" of illegality by hosting providers,[214] which has been transformed into simple "receipt of information" about the supposed illegal activities of their third-party users. The e-Commerce Directive duty to remove or disable access to the illegal content *expeditiously*[215] (upon receipt of effective knowledge) has been formulated in the ECA as a duty to disable access *immediately*,[216] which imposes a significantly higher burden on service providers.

207. *Art. 647/a, (g) CC.*
208. *Art. 115(e) CC, as amended.*
209. *Law No. 10128, adopted on 11 May 2009, as amended by Law 135/2013.*
210. *Art. 16-19 e-Commerce Directive.*
211. *Art. 20 e-Commerce Directive.*
212. *Art. 21.1 ECA.*
213. *Art. 21.3 ECA.*
214. *Cf. Art. 14(1)(b) e-Commerce Directive.*
215. *Ibid.*
216. *Art. 17.1(b) ECA. The word used in Albanian is "menjëherë."*

4. JUDICIAL PRACTICE

In the field of defamation, the most significant and problematic aspect of the case law in recent years has been the high level of civil damage awards granted to claimants,[217] often reaching tens of thousands of Euros even against individual (rather than corporate) defendants.[218]

It is also noteworthy that most high-profile disputes in recent years have not involved media defendants, but members of parliament and senior politicians suing each other over allegations of corruption and malfeasance, in a direct extension of political battles into the courtrooms. Many of these cases have been brought directly to the Supreme Court because the latter has original jurisdiction over cases involving criminal prosecution of members of parliament and senior officials, and claimants often throw criminal calumny or insult charges on top of civil damage claims. (Both sets of claims are normally dealt with in the same proceedings.)

This level of politicization has not helped the development of the jurisprudence. While the courts tend to pay lip service to the relevant ECHR case law, its application remains uneven at best. E.g. in the above mentioned *Vokshi* case, the key ECHR precedent relied on by the Tirana appeals court – arguably the most experienced in the country -- was a marginal judgment on which the Strasbourg panel itself was badly divided, with a four to three majority and a strong dissent by the three judges in minority.[219] It was an odd choice that ignored the seminal judgments of the Strasbourg Court on the question of political speech, but that appeared to usefully endorse the appeal court's conclusion in the case before it.

There have been, to our knowledge, no court cases involving defamation, breach of privacy or other violations specifically in the online context.

It remains difficult to tell what lasting effects the 2012 reforms will have, especially in civil defamation cases. The changes to the Penal Code entered into effect more or less immediately since they tend to be favorable to defendants and, as such, must be applied to ongoing cases. E.g. any charges brought under the repealed offenses of libel or insult against public officials must be immediately dismissed at any stage of the proceedings.[220] The amendments to the Civil Code, on the other hand, could not be applied in proceedings that started before their entry into force in March 2012.

The most significant hate speech case of recent years is the 2006 conviction of five individuals in connection with anti-Albanian statements they made during a rally in the southern town of Himara to protest the results of the 2003 municipal elections. They were charged with incitement to national hatred and defamation of the Republic and its symbols, and sentenced in absentia to three years in prison each.[221] The case is currently pending at the ECHR, with applicants claiming violations of Art. 6 and 10 of the Convention.[222]

---

217. Remzi Lani (ed.), ibid., p. 8.

218. Cf., among others, Vokshi vs Tahiri, a libel dispute between two members of Parliament that resulted in a damage award of 3.3 million leke (more than 23,000 Euros), reduced on appeal to one million leke (equal to about seven monthly salaries of an Albanian MP). Tirana Court of Appeal, Judgment of 11 January 2013.

219. Cf. ECtHR, Barata Monteiro Da Costa Nogueira and Patricio Pereira vs Portugal, Application no. 4035/08, judgment of 11 January 2011.

220. Thus, in October 2012, Genc Pollo, then a cabinet member, withdrew a criminal libel case he had brought against a Socialist MP, citing the amendments to the Penal Code (though he continued to demand civil damages).

221. The domestic courts found that the applicants' statements during the rally included: "Down with Albania", "Albania is Al Qaeda", "Vote for Greece to be free", "Himara is Greek", and "This is Greek land".

222. Beleri and Others v. Albania, Application no. 39468/09 <http://hudoc.echr.coe.int/eng?i=001-115715> (accessed 10 August 2015).

5. PENDING PROPOSALS

As noted, the question of regulation of liability for defamatory online content was briefly discussed at the time of the 2012 amendments to the Civil Code. However, the first specific proposal to this effect was introduced as a private member's bill by an opposition Member of Parliament and former minister, Majlinda Bregu, in January 2015 (hereinafter the Bregu proposal).[223]

5.1. Bregu proposal

The Bregu proposal seeks to introduce a new Art. 617/1 into the Civil Code regulating "liability for online publication of comments that infringe upon a person's honour, personality or reputation." It includes five main components and sets of provisions:

- It establishes that "the administrator of an electronic portal, including the official websites of print or visual media" shall be required to "prevent the publication of any comment that infringes upon the honour, personality or reputation of any person".
- A failure to comply with the above duty of prevention renders the portal administrator liable for any damages caused by the said publication.
- If the offending comment has been "classified for publication"224 by the portal administrator, the latter is required to "delete" the comment "immediately" upon obtaining notification by the affected party. A failure to comply with this duty makes the administrator liable for any (presumably additional) damages caused by the publication
- If the author of the comment is identifiable, the administrator shall be jointly and severally liable with the author for any damage caused. If the author is unidentifiable, the administrator shall be solely liable.
- "Any provision made by the portal excluding or limiting the administrator's liability for published comments" shall be void. Portals must make public the name of the administrator and his contact information; failure to do so shall result in the blocking of access to the portal by a government agency specified in the proposal.

In a brief statement of intent filed in support of her bill, MP Bregu notes that user comments facilitated by "social media" are often "offensive and denigratory, going beyond [what is permitted by] ethical norms."[225] Bregu cites in particular the need to protect the dignity of "female victims of violence" and their family members, but does not clarify whether and how this category is disproportionately targeted by offensive UGC, and how the proposal is tailored to ensure protection of their rights – considering that the proposal's language is of universal application. Media commentators noted that the proposal appeared at a time when the campaign for municipal elections was gearing up, generating an (expected) surge of heated political commentary in online platforms.

---

223. Bill No. 229/2015 Proposing an Amendment to the Civil Code of the Republic of Albania, As Amended; available in Albanian at <http://www.parlament.al/web/pub/pligj_m_bregu_21283_1.pdf> (accessed 10 August 2015). Cf. Annex for an English translation.

224. It is unclear what is meant by this phrase in the Albanian original.

225. Cf. in Albanian <http://www.parlament.al/web/pub/relacion_m_bregu_21284_1.pdf> (accessed 10 August 2015).

5.2. Current status of the proposal

The Bregu proposal was referred to the parliamentary Laws Committee, which held a public hearing on the matter in late April 2015. After the hearing, the Committee decided to table the discussion in anticipation, among others, of a final judgment by the Grand Chamber of the ECHR in the case of *Delfi v. Estonia* (cf. *infra* 1.2.3.). There have been no further public developments as of the end of July 2015, when Parliament went into summer recess.

Also in April, several Kosovo-based sites released highly embarrassing footage showing a well-known Albanian TV host engaging in sexual activity. The incident prompted fresh calls for legal interventions to ensure protection of privacy online.[226]

5.3. Compliance with CoE standards and EU acquis

The proposal raises a number of serious questions regarding its compatibility with Council of Europe standards and European Union law. A summary of the main shortcomings identified is provided below.

5.3.1. Scope and definitions

If adopted in the current form, the Bregu proposal would become *lex specialis,* for a category of website operators and certain forms of illegal content, in relation to the general liability rules of the Albanian ECA. However, the proposal uses terms that are neither part of the ordinary terminology employed by comparative law, nor otherwise properly defined in the proposal itself.

First and most importantly, the proposal does not define what constitutes an "electronic portal" (other that the concept includes "the official sites of print and visual media"). If the intent is to cover only news and information websites, this should be made clear. At the same time, it has become notoriously difficult to define what constitutes a news or information operation at a time when new technologies and business models are profoundly and constantly reshaping the gathering and delivery of online news. For example, would a personal blog containing primarily opinion pieces by its owner be covered by the proposal? In addition, the proposed introduction of the new rule into the civil code instead of sectoral regulation could lend itself to a much broader scope than narrowly defined operators of "electronic portals".

It is worth noting, in this respect, that the *Delfi* judgment of the ECtHR is applicable to "a large professionally managed Internet news portal run on a commercial basis which published news articles of its own and invited its readers to comment on them."[227] The Court specifically noted that the ruling was not meant to apply to other Internet fora, such as discussion forums or "a social media platform where the platform provider does not offer any content."[228]

Secondly, given the relatively high penetration of global platforms in the local market it is astonishing that the proposal's language does not make any reference to foreign "electronic portals" and what is their link to the Albanian jurisdiction. It may nevertheless apply horizontally for all online content

226. *See, among others, Dardan Mustafaj, "The Sokol Balla case and why we need reforms to protect online privacy," MAPO, 24 April 2015 <http://www.mapo.al/2015/04/rasti-ligjor-sokol-balla-ose-pse-duhet-nje-reforme-per-mbrojtjen-e-jetes-private> (accessed 10 August 2015).*

227. *ECtHR, Delfi AS v. Estonia, application no. 64569/09, 18 March 2015, para. 115.*

228. *Ibid., para. 116.*

although it would seem rather difficult for individual claimants to lodge legal proceedings in an Albanian court against non-domestic providers of "electronic portals". In some situations, individuals' interest may be better served if -- instead of pressing legal charges -- they request the removal of the defamatory content according to the reporting mechanism of the foreign provider directly where this is provided for.

Finally, the proposal is not explicit whether it seeks to define liability in relation to a portal's own content, third-party content hosted by a portal or both. Most provisions seem to have been drafted with third-party content in mind, but the point needs to be properly clarified. As already noted, there are no general rules of editorial responsibility in Albanian law, so the lack of precision on this matter may add to the legislative confusion.

5.3.2. Duty to prevent illegal publication of third parties

The most drastic provision of the proposal is the introduction, in its first and second paragraphs, of a duty for portal administrators to prevent the publication of any offending third-party content in the first place. As it should be clear by now, this goes against the very core of the EU approach to intermediary liability, which assumes no general duty of *ex ante* monitoring of the legality of user activities facilitated by an intermediary, including a hosting provider.[229]

There is no other EU member state which has adopted such a duty of prevention or *ex ante* liability, which would be in clear violation of Art. 15 of the e-Commerce Directive. The only way for an "electronic portal" to comply with such a duty would be to establish a system of comprehensive prior review and authorization of all user comments, which would be a highly burdensome arrangement for most online operations. While a number of Albanian online media platforms claim that this is their standard *modus operandi*, they are a minority and do not include the sites with the greatest amount of reader comments.[230]

Such a legal regime would also produce the highest level of "private censorship" of UGC as overcautious portal operators would seek to stay well clear of any expression that might be found offensive or controversial, and therefore prevent such content from ever being published.

It is important to note, in this respect, that the *Delfi* ruling of the ECtHR Grand Chamber did in no way endorse a general duty placed on all hosting providers of prevention of unlawful third-party comments. The Grand Chamber interpreted the judgment of the Estonian Supreme Court as having found the portal liable for its failure to remove the offending comments "without delay" *after* their publication.[231] It was this form of *ex post* liability that the Grand Chamber found—in the circumstances of that case—not to give rise to a violation of Art. 10 ECHR. In so doing, the *Delfi* ruling provides no basis for imposing on intermediaries a general duty of monitoring and prevention of illegal third-party content. In view of the broad European consensus on this question, it is highly questionable that such an approach would pass Art. 10 ECHR muster at this time.

---

229. Art. 15(a) e-Commerce Directive. Cf. Principle 6 of the Declaration on freedom of communication on the Internet, adopted by the Committee of Ministers on 28 May 2003.

230. Rrapo Zguri, infra.

231. ECtHR, Delfi AS v. Estonia, application no. 64569/09, 18 March 2015, para. 141 in fine and para. 153.

5.3.3. Within the coordinated field of the e-Commerce Directive

It should be noted that the requirements concerning the liability of service providers fall inside the scope of the coordinated field of the e-Commerce Directive (Art. 2(i)). The e-Commerce Directive defines a 'coordinated field' within which by the mechanisms of Article 3(1) and (2) member states may not obstruct the internal market. This means that a member state has to ensure that the information society services provided by a service provider established on its territory comply with its national provisions but may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another member state. This means that member states of the EU could not derogate from the internal market clause of the Directive with legislation that subjects providers to stricter requirements than those provided for by the substantive law applicable in the member state in which that service provider is established if this would amount to a barrier to provide services.

Art. 3(4) provides an exhaustive list of derogation from the internal market mechanism in the coordinated field if the measures are necessary for one of the following reason:

- public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons,
- the protection of public health,
- public security, including the safeguarding of national security and defence,
- the protection of consumers, including investors.

In a 2011 judgement the CJEU has ruled on the mechanism provided for by the e-Commerce Directive:

> [t]he mechanism provided for by the Directive prescribes, also in private law, respect for the substantive law requirements in force in the country in which the service provider is established. In the absence of binding harmonisation provisions adopted at European Union level, only the acknowledgement of the binding nature of the national law to which the legislature has decided to make the service providers and their services subject can guarantee the full effect of the free provision of those services. Article 3(4) of the Directive confirms such a reading in that it sets out the conditions under which Member States may derogate from Article 3(2), which must be regarded as being exhaustive. [232]

As a candidate country Albania is not directly bound by the EU *acquis* but accession to the EU requires the transposition of the EU *acquis*. The proposed legislation of providers of "electronic portals" would be incompatible with the EU *acquis* for the reason that it subjects service providers from other member states to stricter requirements than those in its country of establishment. The obligation placed on administrators of "electronic portals" for all hosted content woud amount to a barrier to the freedom to provide services in the internal market. The protection of "a person's honour, personality or reputation" – i.e. the aim of the Bregu proposal – would likely not meet the threshold of the admissi-

232. *CJEU, Joined Cases C-509/09 and C-161/10, eData Advertising a.o. v X a.o., judgment of 25.10.2011, para. 59.*

ble grounds for derogations being "the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons" especially when weighting in the protection of the right to freedom of expression as protected in Art. 11 of the EU Charter.

5.3.4. Notice and action scheme

The third paragraph of the Bregu proposal appears, at first sight, to establish a notice-and-takedown scheme for defamatory comments published by an electronic portal, similar to the scheme provided for in the e-Commerce Directive and the Albanian ECA. There are, however, several important differences that can be discerned at closer reading.

First, the Bregu proposal "obliges" the portal to "immediately delete" an offending comment upon notification by the affected person. Conversely, the e-Commerce Directive safe harbour conditionality simply renders the intermediary liable for its failure – whether deliberate or simply negligent -- to remove, or disable access to, the relevant content upon obtaining knowledge of its illegality. This is a crucial distinction, from a freedom of expression perspective, as the e-Commerce Directive allows the intermediary to make an independent decision about the legality of the relevant content, its newsworthiness and overall journalistic or expressive value—and assume the legal consequences of its decision. The Bregu proposal leaves the portals no choice in the matter, subjecting their editorial autonomy to the simple claims, or legal interpretations, of a not-disinterested private party.

Secondly, under the e-Commerce Directive scheme, a service provider must obtain "effective knowledge" of illegality. This is a term of art that has been interpreted in somewhat varying fashion by the legislatures and courts of different EU member states. In some EU countries, proper notification by an affected party is considered sufficient to give the service provider "effective knowledge." In other jurisdictions, including Finland, Spain and Portugal, only notification by a court or other competent public authority is generally deemed to constitute "effective knowledge" of illegality.[233]

Thirdly, as already noted, a service provider can lose its safe harbour protection under the e-Commerce Directive's scheme if it fails to act "expeditiously" to delete the supposedly offending content. This has been converted in the Bregu proposal in a much more onerous duty to act "immediately." The e-Commerce Directive does not define "expeditiously," but its recital 46 provides some guidance in stating that "the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level." This suggests that the Directive does not require measures which would take forms that would infringe the rights of innocent users or "leave the alleged infringer without due possibilities of opposition and defence."[234]

5.3.5. Lack of notification procedures and due process safeguards

Another significant shortcoming of the Bregu proposal is the lack of any procedures and due process safeguards regarding the notice-and-takedown system it establishes. Providing basic procedures by

233. Cf. Audiencia Provincial of Madrid (9th Section), Paloma v. Google, 19 February 2010, Judgment 95/2010 <http://audiencias.vlex.es/vid/-220093371> (accessed 10 August 2015); Cf. Opinion of Advocate General Jääskinen, Case C-324/09, L'Oreal SA v. eBay International AG, 9 December 2010, para. 160.

234. Opinion of Advocate General Jääskinen, ibid., para. 158.

law is important to ensure that the takedown scheme is not abused by frivolous or aggressive complainants, at the expense of open debate. While the e-Commerce Directive itself does not include procedural clauses, many of the national laws implementing the e-Commerce Directive do.

In France, for example, a valid notification must include details such as the full identity of the notifying party, the date and precise location of the purportedly illegal information, and the legal basis for the complaint.[235] The 2013 Defamation Act for England and Wales and its implementing regulations establish even more detailed requirements for notifications.[236] These include: the name and email address of the complainant; the URL or location of the statement complained of; an explanation of what the statement says and why it is defamatory of the complainant; the meaning the complainant attributes to the statement complained of; the aspects of the statement which the complainant believes are factually incorrect or opinions not supported by fact; ***confirmation that the complainant does not have sufficient information about the author to bring proceedings against them***; and confirmation of whether the complainant consents to his name and email address being provided to the poster.

Furthermore, the Bregu proposal is one-sided in the sense that it makes the takedown of disputed content automatic upon the mere request of the affected party, but provides no remedy whatsoever for the author of the comments, whether anonymous or identifiable. It is considered a good practice in the field that, prior to any takedown, the service provider grant the author of the disputed comment a so-called counter-notification, which enables the author to defend the legality of her content and provide any other relevant information within a reasonably short amount of time.[237] The author of the content should also have the right to seek the reinstatement of any information that has been improperly taken down, whether by the service provider itself or by judicial order.

It is difficult to imagine that the current one-sided arrangement in the Bregu proposal would be found balanced or compatible with Art. 13 of the ECHR, which requires states parties to provide an "effective remedy"—normally by a court of law—for violations of any of the Convention rights, including those guaranteed by Art. 10 ECHR. In the *Delfi* case, the relevant reader comments on the Estonian Internet news portal were found by the Grand Chamber to be so extreme as to fall outside the scope of protection of Art. 10 ECHR altogether. For this reason, the Court did not find it necessary to discuss the remedies and procedural protections to which the authors of the comments were entitled. That is not the case with allegedly defamatory statements, interference with which must be justified on the basis of Art. 10.2 of the Convention.

5.3.6. Questions of "private censorship" and post-publication liability

The question of private censorship presents itself forcefully when considering the Bregu proposal. That is because such schemes generally permit the censoring of speech merely on the basis of a private complaint and/or the assessment of a private service provider, in a departure from the general principle that free expression in the public sphere should only be suppressed by a court of law after

235. *Law No. 2004-575, art. 6-I(5).*

236. *UK Defamation Act 2013 < http://www.legislation.gov.uk/ukpga/2013/26/contents/enacted> (accessed 10 August 2015).*

237. *ECtHR, Delfi AS v. Estonia, application no. 64569/09, 18 March 2015, para. 117.*

proper consideration in a normally adversarial process. Furthermore, and as already noted, the proposal would hold "electronic portals" liable for defamatory third-party comments even in the absence of any notification by affected persons.

It is true that, in the *Delfi* case, the ECtHR Grand Chamber accepted a legal regime of post-publication liability despite the absence of any private notification—or more precisely, it found that the Estonian portal should have removed the impugned comments on its own motion and "without delay", irrespective of whether anyone had complained about them. However, the Court's holding was based on the specific circumstances of the case, which involved statements that "mainly constituted hate speech and speech that directly advocated acts of violence."[238] Thus, the Court added, "the establishment of their unlawful nature did not require any linguistic or legal analysis since the remarks were *on their face manifestly unlawful*."[239]

The above suggests that the Grand Chamber's approach might well be different in cases involving more complex disputes, including most libel and privacy infringement cases, where the legal questions underlying the lawfulness (or not) of the challenged statements are typically less clear cut and require careful judicial consideration. It is worth recalling here that Art. 625/a of the Albanian Civil Code requires the courts to consider no less than eleven separate elements of fact and law in resolving moral damage cases.

The ECtHR Grand Chamber itself conceded in *Delfi* that a notice-and-takedown system as contained in the e-Commerce Directive, "[i]f accompanied by effective procedures allowing for rapid response, … can in the Court's view function in many cases as an appropriate tool for balancing the rights and interests of all those involved."[240] In other words, service providers may be required to adopt special scrutiny and act proactively to remove third-party content – in the absence of notification by affected parties and without any judicial involvement -- only where such content is extreme and "manifestly unlawful." In contrast, the Bregu proposal is open-ended in its scope, covering any and all statements alleged to infringe upon a person's "honour, personality or reputation."

6. ISSUES WITH SELF-REGULATION

As noted in the introduction to this section, the efforts of Albanian online news sites to adopt and enforce ethical standards for user-generated content are relatively rudimentary. There is no indication that the sites employ, for example, any automatic filtering for vulgarities and in general there is little editing or moderation post publication.

An often quoted explanation for this state of affairs is the precarious finances of most online news sites and their inability to employ properly staffed moderation teams. Even the leading online news sites, which can receive thousands of user comments on a daily basis, operate with dedicated teams of no more than 4-5 editorial staff, some of which act as part-time moderators for user comments.[241]

238. *Ibid., para. 117*
239. *Ibid (emphasis added)*.
240. *Ibid., para. 159.*
241. *Rrapo Zguri, ibid..*

There are very few sites, belonging primarily to the major TV stations, that are able to deploy full-time moderators and advanced UGC technology.[242] Basic technological solutions are also lacking: for example, most sites do not offer an easy option to report abusive comments or notice-and-takedown mechanisms. Partly for this reason, the legal remedies provided for in the Albanian ECA seem to go largely unused by persons affected by defamatory or otherwise illegal speech.

Financial or technological restraints cannot explain, however, certain basic failures of the online news and opinion sites. Thus – with the exception of Shqiptarja.com/A1 Report, which has developed and posted a detailed and sophisticated code of journalistic ethics – sites only tend to offer the most basic UGC guidelines for their user community.

In general, user comments contain significantly more offensive speech than professionally produced content. Objectionable language tends to be driven by the country's highly polarized politics; there is relatively little hate speech based on race, ethnicity or religion and it is, for the most part, limited to fringe opinion sites and the social media.[243] Interestingly, online-only news sites seem to maintain a healthier comment environment than mainstream media sites, which are more politicized.[244] Anecdotal evidence suggests that a relatively small number of users, using multiple anonymous accounts and perhaps acting at the behest of political actors, is responsible for a disproportionately large amount of offensive speech.

A number of possible self-regulatory solutions appear obvious in the current state of affairs. Some would be relatively inexpensive technological solutions, such as adopting Albanian-language automatic filters to flag obscene language to website moderators, and reporting mechanisms for abusive commentary. More detailed guidelines for UGC are needed as well as a greater effort to enforce such standards through dedicated moderators and the takedown of objectionable comments. Failing that, online news sites can except growing public pressure in the coming years to force them to rein in abusive comments, including through new laws and legal proceedings.

The authorities -- and in particular specialized agencies such as the Electronic and Postal Communications Authority and the Data Protection Commissioner -- should also do more to educate the public about already available remedies in Albanian law against online defamation, infringement of privacy and other unlawful content. These include the hardly used notice-and-takedown system of the Albanian ECA.

7. TRANSNATIONAL ENFORCEMENT

The Albanian authorities have shown self-restraint in (not) seeking to directly enforce Albanian law against transnational hosts and other online service providers. In fact, there have been no known efforts of such a nature to date, excluding the possible use of mutual legal assistance procedures or other inter-governmental mechanisms.

---

242. The website of Top Channel, for example, has only allowed user comments since the summer of 2014, using Disqus software. However, the site does not appear to encourage user comments, which are relatively sparse.

243. Ilda Londo, Hate Speech in Online Media in Southeast Europe (Albania section), Tirana: Albania Media Institute, 2014 <http://www.institutemedia.org/Documents/PDF/Hate%20speech%20in%20online%20media%20in%20SEE.pdf> (accessed 10 August 2015).

244. Ibid.

No official data are available on this topic. However, the transparency reports of major global providers like Google and Facebook are informative. According to the Google Transparency Reports, there have been zero requests by Albanian authorities to Google for content removal since the start of relevant reporting by the search engine in December 2009. In 2014, Google reported the first two requests by Albanian authorities for user data, involving three user accounts; both requests were denied.[245]

The national authorities have been more active in requesting user data from Facebook, which is not surprising given the social network's popularity in the country. In 2013 and 2014 – the only period for which Facebook has made such data available to date -- there were a total of 32 requests for user data involving 61 accounts, with a 66.5% average rate of "some data produced" by Facebook.[246] There was a spike in user data requests in the second half of 2014 (16 requests involving 34 accounts), but the data production rate went down to 25% for that period, from 75-83% in the three prior reporting periods.[247] This indicates a possible trend toward more aggressive use of the Facebook self-policing mechanism by the Albanian government.

In contrast, during the same two-year period, Facebook reported zero content restriction requests – typically, requests to delete specific unlawful content posted by its users -- from Albania, whether by the authorities or any other local source. This suggests that no government agencies, NGO watchdogs or legal professionals engage in systematic or even sporadic monitoring of hate speech or other unlawful online publications involving users under the Albanian jurisdiction. Such passivity stands in contrast to the efforts of both governmental and NGO entities in many European countries, which seek to work with – and sometimes in open confrontation against -- major service providers to find innovative solutions to the problem of harmful speech online.[248] While such efforts are sometimes controversial from a free speech perspective, it can be seen as a missed opportunity by Albanian actors to make use of the main global OSPs' self-policing mechanisms as a cheaper and simpler alternative to law enforcement or private litigation.

8. CONCLUSIONS WITH POLICY RECOMMENDATIONS

Against the background of European best practices in online content regulation, the study considered in particular a pending legislative proposal in Albania which seeks to introduce "liability for online publication of comments that infringe upon a person's honour, personality or reputation" on providers of "electronic portals". The study's assessment of the proposal concludes that it conflicts with the graduated and differentiated approach promulgated by the relevant CoE standard-setting instruments, vastly exceed the ECtHR interpretation in the *Delfi* judgement and would clash with the

245. Cf. <http://www.google.com/transparencyreport/userdatarequests/AL/> (accessed 10 August 2015). Google does not provide specific reasons for denial of such requests.

246. Cf. <https://govtrequests.facebook.com/country/Albania/2014-H2/> (accessed 10 August 2015). Facebook does not provide details for requests filed by specific governments, but includes this general explanation: "The vast majority of these requests relate to criminal cases, such as robberies or kidnappings. In many of these cases, these government requests seek basic subscriber information, such as name and length of service. Other requests have asked for IP address logs or actual account content." Cf. <https://govtrequests.facebook.com/about/> (accessed 10 August 2015).

247. Ibid.

248. One recent example of this approach has been the high-profile litigation of the Spanish Data Protection Authority leading to a judgment of the CJEU recognizing the right to have certain personal data removed from search engine results of one's name; CJEU, case C-131/12, Google Spain SL, Google Inc. v AEPD, Mario Costeja González, 13 May 2014, discussed infra at 2.2.4.

EU *aquis,* particularly with Art. 14 and 15(a) of the e-Commerce Directive.

In light of the above considerations, the necessity of a legislative intervention in Albania at this time, along the lines of the Bregu proposal, appears less than compelling. It may be more advisable, as in the Estonian *Delfi* case which was based on the general civil law defamation rules, to allow the courts to develop more nuanced rules in this field, under the guidance of the ECtHR. With the exception of England and Wales, which undertook in 2013 long-planned, comprehensive reforms of their defamation laws, no other EU member state to our knowledge has adopted specific laws for online defamation. This has allowed their court systems to gradually develop the case law, taking account of fast changes in technology, information ecosystems and societal attitudes.

If enacted this legislation would retrograde the advancements made with the 2012 reforms to the Albanian civil and criminal defamation laws introduce an unorganic and unbalanced measure directed against all content and hosting providers that is excessively restraining the freedom of expression online.

In particular, the study identifies the following shortcomings:

1. The definition of "electronic portal" to overly broad, thus capturing "passive" intermediaries contrary to European best practices and the EU aquis; the definition does also not allow for taking into account the defining characteristics of the service but automatically places the obligations of "active" intermediaries on all providers;
2. To the extent that "passive" intermediaries would be regulated the proposal contradicts with Art. 17 of the Albanian ECA which provides for a liability exception for hosting services analogue to Art. 14 of the EU e-Commerce Directive;
3. The obligation on portal administrators to prevent the publication of any offending third-party content amounts to a duty to monitor information contrary to the EU aquis;
4. The obligation would appear to apply horizontally to all providers of "electronic portals" irrespective whether they are established in Albania or abroad but the proposal does not include issues of jurisdiction or consider practicalities of extraterritorial enforcement.
5. This in turn can amount to a violation of Art. 3 (2) of the e-Commerce Directive because it would alter the requirements for providers established in another member state within the coordinated field of activities;
6. The general obligations for the content and the take-down procedure do not allow for a balancing exercise taking into account the type of speech, the role of the actors involved, the political relevance and public interest, among others, pursuant to the established case-law of the ECtHR;
7. The legislative proposal lacks procedural safeguards, in particular that courts should primarily assess whether online content is infringing third party's reputation, or at least which requirements the notice has to comply with and other rights and means to assess and protest the notice; and

In light of the above considerations, the study recommends the Albanian legislator not to adopt this

legislative proposal. It should be recalled that the Estonian *Delfi* case was based on the general civil law defamation rules and not on dedicated piece of legislation placing a general obligation on providers of hosting services for all published content, irrespective whether this is own or third party content and the provider's activities are passive intermediary or rather media/ "active" intermediary. In light of the fundamental right to the freedom of expression and the recommended nuanced approach Albanian decision-makers should allow the courts to develop case-law, under the guidance of the ECtHR, based on the criteria in Art. Art. 647/a of the civil code.

In order to communicate how the present legal framework applies to the situation of hosting providers it is recommended:

1. to disseminate this study widely to all stakeholders;
2. to organize a workshop for policy-makers and stakeholders covering the legislative status quo in Albania against the backdrop of European best practices and developments in the case law of the European courts; in particular the workshop should aim to convey the qualified requirements promulgated in the ECtHR Delfi-judgement;
3. to organize a workshop for judges on the case law of the ECtHR and the CJEU relevant to defamatory content online, in particular how both courts balance the infringement of individual's reputation and other rights with the freedom of expression online;
4. to promote self-regulation of hosting providers and assist with an overview of available measures
5. to educate the public about already available remedies in Albanian law against online defamation, infringement of privacy and other unlawful content. These include the hardly used notice-and-takedown system of the Albanian ECA.
6. to set-up a dedicated website to promote the public awareness of individual user's possible remedies against online defamation, infringement of privacy and other unlawful content. Inter alia, this website should provide an accessible overview over the mechanisms deployed by the most commonly used hosting providers in Albania and links to their reporting tools and notice-and-action schemes.

ANNEXES

Albania legislation relevant to online content regulation, in particular defamation laws, and hosting intermediaries liability for third party comments

1. BREGU PROPOSAL[249]

REPUBLIC OF ALBANIA

THE ASSEMBLY

DRAFT LAW

No _____ / 2015

ON AN ADDITION TO LAW NO 7850, DATED 29 July 1994 "CIVIL CODE OF THE REPUBLIC OF ALBANIA," AS AMENDED

Pursuant to Article 81(1) of the Constitution, and upon a proposal of a Member of Parliament,

THE ASSEMBLY

OF THE REPUBLIC OF ALBANIA

DECIDED

To make the following additions to Law No 7850, dated 29 July 1994 "Civil Code of the Republic of Albania," as amended:

Article 1

Article 617/1 with the following content shall be added after Article 617 of the Civil Code:

"Article 617/l

Liability for online publication of comments that infringe on a person's honour, personality or reputation

The administrator of an electronic portal, including official websites of printed or visual media, shall prevent publication of any comment that infringes on a person's honour, personality or reputation.

In case of failure to prevent publication of comments that infringe on a person's honour, personality or reputation, in accordance with the legal obligation set out in the first paragraph of this Article, the administrator of an electronic portal shall be held liable for damage caused.

If a comment that infringes on a person's honour, personality or reputation is classified for publication by the administrator of an electronic portal, he/she shall immediately delete it once notified by the person claiming that such comment infringes on his/her honour, personality or reputation. In case of failure to

249. *Draft legislation in Albanian <http://www.parlament.al/web/pub/pligj_m_bregu_21283_1.pdf>* (accessed 10 August 2015). Unofficial translation into English by the OSCE.

immediately delete the comment upon the request of the person whose honour, personality or reputation has been infringed, the administrator of the electronic portal shall be held liable for damage caused.

When the person who writes the comment is identifiable, the liability of the administrator of the electronic portal shall be solidary to that person's. When the person who writes the comment cannot be identified, the liability for damage caused shall rest only on the administrator of the electronic portal, who allowed the publication of the comment or failed to take necessary measures to ensure timely deletion thereof.

Damage caused under this Article shall be classified as non-property damage arising from infringement of a person's honour, personality or reputation.

Any clause posted on the electronic portal that exempts or limits the administrator's liability on published comments shall be invalid. Any electronic portal must publicly make available the full data of the administrators and modes of contact with him/her. The authority responsible for Electronic Communications shall forbid public access to any electronic portal that fails to abide by this obligation.

Article 2

Transitory provision

The administrator of an electronic portal, including official websites of printed or visual media, shall, within 30 days from the date the present law enters into force, publish his/her full data in the portal and provide full information on modes of contact with him/her. Means of contact with the administrator shall ensure recording of any request or complaint that the administrator may receive about comments that infringe on a person's honour, personality or reputation.

The competent authority for Electronic Communications shall monitor observation of this obligation and shall take measures to prevent public access to the electronic portal, when the full data of the administrator of the portal and modes of communication with him/her are not published.

Article 3

This law shall enter into force 15 days from its publication in the Official Gazette.

Approved on _____ / _____ / 2015

SPEAKER

ILIR META

Proposing MP
(signature)
MAJLINDA BREGU

2. PENAL CODE (IN EXTRACTS)[250]

Law No. 7895

CRIMINAL CODE OF THE REPUBLIC OF ALBANIA

Article 74/a

Computer dissemination of materials in favor of genocide or crimes against humanity

Offering in public or deliberately disseminating to the public through computer systems materials that deny, minimize significantly, approve of or justify acts that are genocide or crimes against humanity.

Article 119

Insult

Deliberate insult of the person constitutes a penal misdemeanour and is sentenced by fines from fifty thousand ALL up to one million ALL.

The same offense, when is committed publicly, injuring several persons and more than once, constitutes a penal misdemeanour and is sentenced by fines from fifty thousand ALL up to three millions ALL.

Article 119/a

Dissemination of racist or xenophobic materials through the computer system

Offering in public or deliberately disseminating to the public through computer systems materials with racist or xenophobic content constitutes a criminal contravention and is punishable by a fine or imprisonment up to two years.

Article 119/b

Insulting due to racist or xenophobic motives through the computer system

Intentionally insulting a person in public, through a computer system, because of ethnicity, nationality, race or religion constitutes a criminal contravention and is punishable by fine or imprisonment up to two years.

250. Unofficial translation into English from Legislationline <http://www.legislationline.org/documents/section/criminal-codes> (accessed 10 August 2015).

Article 120

Defamation

Intentional dissemination of talks, and any other information knowing that they are false that injure the honour and dignity of the person, constitutes penal misdemeanour and is sentenced by fines from fifty thousand ALL up to one million and five hundred thousand ALL. The same offense, when is committed publicly, injuring several persons and more than once, constitutes a penal misdemeanour and is sentenced by fines from fifty thousand ALL up to three millions ALL.

3. CIVIL CODE OF ALBANIA (IN EXTRACTS)[251]

LAW Nr. 7850

ON THE CIVIL CODE OF THE REPUBLIC OF ALBANIA

Article 625, as amended

A person who has suffered non-pecuniary damage shall be entitled to compensation when:

…(b) his honor, personality or reputation has been harmed;

…(d) the memory of a dead person has been defamed. In such cases, the surviving spouse or relatives of the dead person to the second degree may request compensation of the non-pecuniary damage.

Article 647/a

Compensation of non-pecuniary damage to a person's honor, personality or reputation shall seek the reinstatement of the affected right, in proportion to the harm suffered and pursuant to the circumstances of each case. In determining civil liability and the quantum of non-pecuniary damage, courts shall consider the following, among other, considerations:

(a) The manner, form, and timing of the dissemination of the [relevant] utterances or conduct;

(b) The degree to which the author of the utterances has acted in compliance with standards of professional ethics

(c) The forms and degree of fault [dolus]

(ç) Whether the utterances include correct references to or quotations of utterances by a third person

(d) Whether the utterances are true, especially in cases of harm to reputation

(dh) Whether the utterances are related to the harmed person's private life and their relevance to matters of public interest

(e) Whether the utterances constitute opinions or contain only insignificant factual inaccuracies;

(ë) Whether the utterances are connected to matters of public interest, or to persons holding government positions or running for election;

(f) Any actions undertaken to prevent or reduce the degree of harm, such as the retraction of false statements, as well as any other measures taken by the author of the utterances to reinstate the honor, personality or reputation of the harmed person;

(g) Whether the author of the utterances has profited from their dissemination, as well the measure of such profit

(gj) Whether the amount of compensation awarded may significantly worsen the financial condition of the liable person.

251. *Own translation.*

4. ELECTRONIC COMMERCE ACT (EXCERPT)[252]

Law No. 10128 (as amended)

ELECTRONIC COMMERCE ACT OF THE REPUBLIC OF ALBANIA

Article 17

Hosting

1. In case when an information society service consists in saving/storing of information obtained by the service recipient, the service provider of the information society service is not responsible for the information saved upon request of the service recipient if the service provider:

2. Is not aware or cannot be aware of the illegal activity of the recipient or the content of information and as for damage claims, is not aware of the facts and circumstances from which illegal activity or information stems from; b) upon receiving this information acts immediately to remove or deactivate access to the information.

3. Point 1 of this article is not applicable when the service recipient acts on behalf or under the control of the service provider.

Article 18

Means of location of information

Service providers that generate, through electronic means, access to information for third parties shall not be liable for such information provided:

a) They are not, or cannot be, aware of the unlawful activities of the recipient [of the information] or the data contained in the information;

b) Upon obtaining knowledge of the fact of unlawful activity or data, they remove or disable access to such data.

Article 19

Interruption or prevention of contravention

Despite of what is provided by the dispositions of this law, in Articles 15, 16, 17 and 18, the service provider is obliged to stop or warn a violations if this is required by the court or the authority responsible in line with the legislation in power.

252. Own translation.

Article 20

Service Provider Obligations

1. the service provider of the information society services which are an object of this chapter do not have obligations to oversee the information they transmit or save, as well as for searching of facts or situations that demonstrate illegal activities.

2. The Service provider of the information society notifies immediately the responsible authorities in case there is reasonable doubt that the service user: a) are engaging in illegal activity b) have presented illegal information.

3. The service provider presents to the responsible authorities, upon their request and in line with the legislation in power, all the information that enables the identification of the recipient of the service.


COUNCIL OF EUROPE
CONSEIL DE L'EUROPE