Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation

Riis, Thomas; Schwemer, Sebastian Felix

Published in:
Journal of Internet Law

Publication date:
2019

Document version
Early version, also known as pre-print

Citation for published version (APA):
Riis, T., & Schwemer, S. F. (2019). Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation. *Journal of Internet Law*, *22*(7), 1–21.

Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation

Thomas Riis &
Sebastian Felix Schwemer

University of Copenhagen Faculty of Law
Legal Studies Research Paper Series, paper no. 2019-64

–Forthcoming in Journal of Internet Law 1/2019–

Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation

Thomas Riis* and Sebastian Felix Schwemer†

1. INTRODUCTION

The regulation of online content is as topical as never before: both, intermediaries on the application layer of the internet, such as online platforms[1] like Facebook, Twitter or YouTube, as well as intermediaries on the infrastructure layer, such as internet access service providers or domain registries[2], are at the epicenter of the debate.

In the European Union, the European Commission –in its function as legislative initiator– has over the recent years put forward a variety of different legislative and non-legislative solutions to answer the question how to tackle illegal content online. In this article, we look at one particular trend: the proactive takedown of content by automated technological means. There is no uniform notion or description applied. Rather the phenomenon is circumscribed as 'proactive measures', 'content recognition technologies', or 'using automated means to detect, identify and expeditiously remove or disable access to' content.

The purpose of implementing such measures is to make enforcement more efficient on online platforms and on the internet in general by using intermediaries as tools because they have the technical possibilities of monitoring and addressing online infringing activities. However, in this case, efficiency comes at a cost.

One concern is that such measures, typically, are part of private procedures and the use and impact of these procedures is usually subject to a significant lack of transparency unless specific regulation is adopted to that effect. This impedes evaluating just how effective and widespread the procedures are; assessing how they work in terms of accuracy; and monitoring their adherence to general standards of fair process. It is also difficult to assess how this system affects right holders, internet service providers and internet users in general. Rights enforcement through automated proactive takedown is a way to resolve disputes between parties (i.e. the right holder, the internet service provider and the internet user(s) concerned).

Another concern relates to the standards of due process. The summary nature of automated take down measures makes them comparable to provisional (sometimes protective)

* Professor, Centre for Information and Innovation Law (CIIR), University of Copenhagen. Contact author: thomas.riis@jur.ku.dk.

† Ph.D., Industrial PostDoc, Centre for Information and Innovation Law (CIIR), University of Copenhagen and Danish Internet Forum (DIFO). Contact author: sebastian.felix.schwemer@jur.ku.dk.

[1] On online actors as addressees of European regulation *see* European Parliament resolution of 15 June 2017 on online platforms and the digital single market (2016/2276(INI)). Critical on the uniform notion of online platforms *see e.g.* A. Savin, "Regulating internet platforms in the EU – The Emergence of the 'Level playing Field'," 34(6) *Computer Law & Security Review* 1215 (2018).

[2] *See* S.F. Schwemer, "On Domain Registries and Website Content," 26(4) *International Journal of Law and Information Technology* 273 (2018).

measures such as *ex parte* preliminary injunctions. However, there is no requirement for automated measures to offer procedural safeguards comparable to those usually related to the granting of a preliminary injunction. Disregarding due process creates a risk of automated measures being abused.[3] As emphasized by William Patry, this technique is notoriously inaccurate.[4]

A final and related concern is the risk over over-enforcement. As a commercial profit seeking entity, an internet service provider minimizes cost, and one way to do that is to avoid litigation and other disputes. Hence, an internet service provider is more likely to apply an algorithm that takes down too much rather than too little.[5]

First, the article tracks the different proposals of automated content-takedown measures. Then it briefly identifies some common issues in the context of the European safe harbor regime and the existing notice-and-takedown system. It argues that the policy trend towards algorithmic content regulation is problematic: firstly, there is only little known about the workings of algorithmic content enforcement at this point. Secondly, the legislator appears to prefer soft law and industry self-regulation over legislative intervention based on secondary law. Thirdly, the reliance on algorithmic content regulation represents a departure from the traditional intermediary liability regime.

2. EU INITIATIVES REGARDING PRO-ACTIVE, AUTOMATED MEASURES BY INTERMEDIARIES

Over the recent years, the European lawmaker has put forward a variety of different regulatory solutions to tackle illegal content online. In the following, let us look at three examples for suggested pro-active measures of intermediaries proposed by the European Commission: 1) in the field of copyright, 2) broadly for online platforms for all forms of illegal content and terror content, and 3) lastly for terrorist content.

2.1. Copyright: Article 13 of the proposed Directive on copyright in the Digital Single Market – The case of sharing platforms

On 14 September 2016, the European Commission presented its proposal for a Directive on copyright in the Digital Single Market.[6] The proposed Directive addresses a broad variety of issues, where a modernization of the copyright framework was deemed necessary in order to enable a digital single market.[7]

In the chapter on certain uses of protected content online, Article 13(1) stipulates, that

[3] *E.g.* N. Suzor and B. Fitzgerald, "The Legitimacy of Graduated Response Schemes in Copyright Law," 34(1) *University of New South Wales Law Journal* 25 (2011); Special Rapporteur (Frank La Rue), Report on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, UN Doc. A/HRC/17/27 (May 16, 2011) 12.

[4] W. Patry, "Moral Panics and the Copyright Wars," (London: Oxford University Press, 2009) 13. *See also* P.K. Yu, "The Graduated Response," 62 Florida Law Review 1373, 1395 et seq. (2010).

[5] *Cf.* C. Salung Petersen and T. Riis, "Private enforcement of IP law by internet service providers: notice and action procedures" in T. Riis (Ed.), "User Generated Law: Re-construction Intellectual Property Law in a Knowledge Society" (Cheltenham: Edward Elgar Publishing, 2016), ch.10, 242 et seq.

[6] European Commission, Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, Brussels 14 September 2016, COM(2016) 593 final 2016/0280(COD).

[7] For recent developments in relation to the access to copyright protected works see S.F. Schwemer, "Licensing and Access to Content in the European Union" (Cambridge: Cambridge University Press, 2019).

> *"Information society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users shall, in cooperation with rightholders, take measures to ensure the functioning of agreements concluded with rightholders for the use of their works or other subject-matter or to prevent the availability on their services of works or other subject-matter identified by rightholders through the cooperation with the service providers. Those measures, such as the use of effective content recognition technologies, shall be appropriate and proportionate."*

The proposed Article 13 aims at providing right holders with a stronger negotiation position vis-à-vis big online platforms. It aims to address what has by music right holders been described as 'value gap': the alleged imbalance between the revenue that platforms, for example Youtube and Facebook, extract from user-uploaded content, and the revenue that finds its way back to right holders. The problem of the value gap arises by the widespread practice of users where large numbers of copyright protected work are made available on the sharing platform without authorization. The sharing platforms' business model benefits to a certain extent from copyright infringements by its users; however, the platforms themselves are not liable for the infringements pursuant to safe harbor provisions of the E-Commerce Directive[8] (see in detail below).

The proposed Article 13 stipulates that in both, instances where licensing agreements have been concluded and in instances where no licensing agreements have been concluded, certain online platforms need "to take measures", such as the use of "effective content recognition technologies". Recital 39 of the Proposal clarifies that

> *"Collaboration between information society service providers storing and providing access to the public to large amounts of copyright protected works or other subject-matter uploaded by their users and rightholders is essential for the functioning of technologies, such as content recognition technologies. In such cases, rightholders should provide the necessary data to allow the services to identify their content and the services should be transparent towards rightholders with regard to the deployed technologies, to allow the assessment of their appropriateness. The services should in particular provide rightholders with information on the type of technologies used, the way they are operated and their success rate for the recognition of rightholders' content. Those technologies should also allow rightholders to get information from the information society service providers on the use of their content covered by an agreement."*

The suggested solution to the value gap problem was thus to put certain (not very clear) obligations on the sharing platforms to prevent copyright infringements by the platforms' users. The solution is problematic because it implies general obligations on the sharing platforms. According Article 15(1) of the E-Commerce Directive, Member States shall not impose a general obligation on providers, when providing the services, to monitor the information, which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. Basically, the proposed provision attempts to expand the liability of sharing platforms without amending the wording of the E-Commerce Directive that explicitly exempt *i.a.* such service providers from liability.

In the scholarly community, the Proposal by the European Commission has been ill received and led to several statements addressing various fundamental legal issues.[9] On 25 May

[8] 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 [2000] OJ L178.

[9] *See e.g.* S. Stalla-Bourdillon et al., "Open Letter to the European Commission - On the Importance of Preserving the Consistency and Integrity of the EU Acquis Relating to Content Monitoring within the Information Society," Sep. 30, 2016, available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2850483*; "The Copyright Directive is failing" (Open Letter to Members of the European Parliament and the Council of the European Union),

2018, the European Council presented its agreed negotiating agreement.[10] The Council solved the conflict with the liability exemptions of the E-Commerce Directive by suggesting that the mere fact that a sharing platform gives the public access to copyright protected works uploaded by its users, constitutes a 'communication to the public', which is covered by the right holders' exclusive rights. In this way, the sharing platforms are considered directly liable for the users' copyright infringements and the E-Commerce Directive only exempts from contributory liability.

Furthermore, the Council deleted the reference to "effective content recognition technologies" and proposes an alternative safe harbor regime for certain online platforms: in instances where a platform does not have the necessary licenses, it is according to Article 13(4) shielded from liability provided that

> *"(a) it demonstrates that it has made best efforts to prevent the availability of specific works or other subject matter by implementing effective and proportionate measures, in accordance with paragraph 5, to prevent the availability on its services of the specific works or other subject matter identified by rightholders and for which the rightholders have provided the service with relevant and necessary information for the application of these measures; and*
>
> *(b) upon notification by rightholders of works or other subject matter, it has acted expeditiously to remove or disable access to these works or other subject matter and it demonstrates that it has made its best efforts to prevent their future availability through the measures referred to in point (a)."*

In other words, the Council still requires "implementing effective and proportionate measures", without further clarification, though.[11]

Finally, on 12 September 2018, the European Parliament found its compromise text, after the Legal Committee's compromise text in June 2018 failed to pass. The European Parliament's text deleted all references to automated technologies stipulating in Article 13 (2a):[12]

> *"Member States shall provide that where right holders do not wish to conclude licensing agreements, online content sharing service providers and right holders shall cooperate in good faith in order to ensure that unauthorised protected works or other subject matter are not available on their services. Cooperation between online content service providers and right holders shall not lead to preventing the availability of non-infringing works or other protected subject matter, including those covered by an exception or limitation to copyright."*

The proposed Article 13 is highly controversial which the substantial amendments of the provision by the European Council and the European Parliament as well as the public and academic opposition testify to. Arguably, the most controversial feature of the proposed Article 13 comes with uncertainty as to the legal effect of the provision. It is clear that Article 13 imposes an obligation on the sharing platforms, but it is not clear whether that is an obligation to cooperate in good faith with right holders, an obligation to ensure that unauthorized protected works or other subject matter are not available on their services, or both.

April 26, 2018, available at *https://www.create.ac.uk/wp-content/uploads/2018/04/OpenLetter_EU_Copyright_Research_Centres_26_04_2018.pdf.* In the context of Article 11, *see* "Academics Against Press Publishers' Right", available at *https://www.ivir.nl/academics-against-press-publishers-right/.*

[10] European Council, "Agreed negotiating mandate", Brussels, May 25, 2018, ST 9134 2018 INIT.

[11] Additional safeguards were introduced *i.a.* in the recitals, where for example code sharing platforms, online marketplaces and other actors are envisaged to be exempted from the novel regime.

[12] European Parliament, "Copyright in the Digital Single Market ***I, Amendments adopted by the European Parliament on 12 September 2018 on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market (COM(2016)0593 – C8-0383/2016 – 2016/0280(COD))".

2.2. Illegal content online

The proposed Directive on copyright in the Digital Single Market aims exclusively at copyright infringement. Other EU measures have a broader and more general scope of application.

2.2.1. Commission Recommendation (EU) 2018/334

On 1 March 2018, the European Commission issued its Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online.[13] The Recommendation, a legal act of the Union but without binding effect on its addressees (cf. Article 288 TFEU), is addressed broadly towards Member States and hosting service providers.[14]

In Chapter 2 on "General recommendations relating to all types of illegal content", the Recommendation stipulates under point 18 on "proactive measures" that:

> *"Hosting service providers should be encouraged to take, where appropriate, proportionate and specific proactive measures in respect of illegal content. Such proactive measures could involve the use of automated means for the detection of illegal content only where appropriate and proportionate and subject to effective and appropriate safeguards, in particular the safeguards referred to in points 19 and 20."*

In the context of the Recommendation, illegal content refers to "any information which is not in compliance with Union law or the law of a Member State concerned" (point 4(b) Recommendation (EU) 2018/334). Whereas the Commission's proposed Article 13 in the context of copyright from two years earlier simply referred to "(...) measures, such as the use of effective content recognition technologies", the Recommendation appears to be more reluctant. Automated means for the detection of illegal content are only suggested under certain safeguards. The call for encouragement mentions the 'appropriateness' of measures three times.

Chapter 3 of the Recommendation is dedicated to specific recommendations relating to terrorist content that apply in addition to the general recommendations set out in Chapter 2. Point 36 suggests the adoption of "proportionate and specific proactive measures, including by using automated means, in order to detect, identify and expeditiously remove or disable access to terrorist content". Point 37 additionally suggests taking such measures to also prevent the re-submission of content that has previously been removed.

When comparing the two scenarios in Chapter 2 and 3, it appears that the Commission has fewer concerns as to the use of automated content recognition technologies when it comes to terrorist content. It is thus noteworthy that the Recommendations provisions on safeguards and protection against abusive behavior (points 19–21) is placed in Chapter 2, which applies to all types of illegal content, and that no similar provisions are found in Chapter 3 on terrorist content. One of the safeguards in Chapter 2 concerns the situation where hosting service providers use automated means in respect of content that they store, effective and appropriate. In such cases safeguards should be provided to ensure that decisions taken concerning that content, in particular decisions to remove or disable access to content considered to be illegal

[13] European Commission, Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online [2018] OJ L63/50.

[14] Such a hosting service provider is defined in point 4 (a) of Recommendation (EU) 2018/334 as "(...) a provider of information society services consisting of the storage of information provided by the recipient of the service at his or her request, within the meaning of Article 14 of Directive 2000/31/EC, irrespective of its place of establishment, which directs its activities to consumers residing in the Union".

content, are accurate and well-founded. Furthermore, such safeguards should consist, in particular, of human oversight and verifications, where appropriate and, in any event, where a detailed assessment of the relevant context is required in order to determine whether or not the content is to be considered illegal content (point 20).

Recital 24 of Recommendation (EU) 2018/334 clarifies that the proactive measures described are to be seen in addition to notice-and-action mechanisms. It further clarifies that the measures are "taken voluntarily by hosting service providers". Yet, in the same sentence it underlines that they "can also be an important element in tackling illegal content online". Furthermore,

> *"In connection to such proactive measures, account should be taken of the situation of hosting service providers which, because of their size or the scale on which they operate, have only limited resources and expertise and of the need for effective and appropriate safeguards accompanying such measures."*

So, whereas the measures are suggested to be voluntary on the one side, the Commission discourages hosting service providers that lack the resources or expertise. But it can also be read as an additional encouragement of those that do.

2.2.2. The revised Audiovisual Media Services Directive

In May 2016, the European Commission proposed its revision for the Audiovisual Media Services Directive (AVMSD).[15] Also in the regime of the AVMSD, the curation or regulation of content is topical.

The AVMSD applies exclusively to an 'audiovisual media service' which, however, is defined broadly as a service which is under the editorial responsibility of a media service provider and the principal purpose of which is the provision of programmes, in order to inform, entertain or educate, to the general public by electronic communications networks. Such an audiovisual media service is either a television broadcast or an on-demand audiovisual media service (cf. Article 1(1)(a)(i) AVMSD). Accordingly, video-sharing platforms that are subject to Article 13 of the proposed Directive on copyright in the Digital Single Market are also audiovisual media services within the meaning of the AVMSD.

In the Commission's proposal, Article 28a(1) on a provision applicable to video-sharing platform services, it stipulates:

> *"Without prejudice to Articles 14 and 15 of Directive 2000/31/EC, Member States shall ensure that video-sharing platform providers take appropriate measures to:*
>
> *(a) protect minors from content which may impair their physical, mental or moral development;*
>
> *(b) protect all citizens from content containing incitement to violence or hatred directed against a group of persons or a member of such a group defined by reference to sex, race, colour, religion, descent or national or ethnic origin."*

[15] European Commission, Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, Brussels, May 25, 2016, COM/2016/0287 final, 2016/0151 (COD).

In Article 28a(2) the proposal further defines appropriate measures, related to e.g. the services' terms and conditions, reporting and flagging mechanisms and parental control systems. Whereas the proposed Directive on copyright in the Digital Single Market imposes obligations on video-sharing platforms in respect of copyright infringements, the proposed amendments to AVMSD imposes obligations on video-sharing platforms in respect of other types of illegal content.

It is specified in the preamble of the proposed Directive that video-sharing platform providers typically determine the organization of the content on the platform, namely programmes or user-generated videos, including by automatic means or algorithms. Therefore, those providers should be required to take appropriate measures to protect minors from and protect all citizens from incitement to violence or hatred directed against a group of persons or a member of such a group defined by reference to sex, race, colour, religion, descent or national or ethnic origin (recital 28).

On 2 October 2018, the European Parliament voted in favor of a number of amendments to the Commission's proposal. According to the text of Parliament, the legislation does not include any automatic filtering of uploaded content, but the rules should create a transparent, easy-to-use and effective mechanism to allow users to report or flag content.

2.3. New Regulation on terrorist content

In Jean-Claude Juncker's State of the Union speech from 12 September 2018, it was announced that the recommendations from March 2018 "have brought positive results, overall progress has not been sufficient."[16] The Recommendation sets out voluntary operational measures to ensure faster detection and removal of illegal content online, to reinforce the cooperation between companies, trusted flaggers and law enforcement authorities, and to increase transparency and safeguards for citizens and it includes specific suggestions to ensure increased protection against terrorist content online. One of the suggestions in respect of terrorist content concerns faster detection and effective removal which implies that internet companies should implement proactive measures, including automated detection, to effectively and swiftly remove or disable terrorist content and stop it from reappearing once it has been removed.[17]

Now, the Commission has left its soft law approach and proposed a Regulation on terrorist content.[18] The proposed Regulation institutes a duty of care obligation for all platforms to ensure they are not misused for the dissemination of terrorist content online. Article 3 (1) stipulates, on the one hand, that hosting service providers shall take appropriate, reasonable and proportionate actions in accordance with the regulation, against the dissemination of terrorist content and to protect users from terrorist content. On the other hand, they shall act in a diligent, proportionate and non-discriminatory manner, and with due regard to the fundamental rights of the users and take into account the fundamental importance of the freedom of expression and information in an open and democratic society. It is further specified that hosting service providers shall, where appropriate, take proactive measures to protect their services against the dissemination of terrorist content (Article 6(1)), including by deploying automated detection tools.

---

[16] European Commission, "State of the Union 2018: Commission proposes new rules to get terrorist content off the web", Sep. 12, 2018, available at *http://europa.eu/rapid/press-release_IP-18-5561_en.htm.*

[17] *Id.*

[18] European Commission, Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, Sep. 12, 2018, COM(2018) 640 final, 2018/0331 (COD).

In Article 9, the proposed Regulation introduces safeguards specifically aimed at the use and implementation of the proactive measures mentioned in Article 6. Where hosting service providers use automated tools in respect of content that they store, they shall provide effective and appropriate safeguards to ensure that decisions taken concerning that content, in particular decisions to remove or disable content considered to be terrorist content, are accurate and well-founded (Article 9(1)). Furthermore, safeguards shall consist, in particular, of human oversight and verifications where appropriate and, in any event, where a detailed assessment of the relevant context is required in order to determine whether or not the content is to be considered terrorist content (Article 9(2)).

Strong safeguards to protect content which is not terrorist content from erroneous removal, are needed because automated removal tools are radical measures, which can malfunction and be misused. Until recently, the EU legislator was reluctant to recommend and adopt such proactive measures. Notably, in terms of one of the most serious online crimes related to child sexual abuse material, Article 25 of the Directive on combating the sexual abuse and sexual exploitation of children and child pornography from 2011 builds upon "Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory."[19] In other words, proactive measures are not introduced from its outset.

3. THE TRADITIONAL SAFE HARBOR REGIME OF THE E-COMMERCE DIRECTIVE

As seen in the section above, the use of proactive measures is prominently featured in recent regulatory proposals. Almost for two decades, Section 4 of the E-Commerce Directive has provided the basis for a partly harmonized EU regime on intermediary liability for so-called 'information society services' in situations of mere conduit (Article 12), caching (Article 13), and hosting (Article 14), while Article 15 establishes that there is no general monitoring obligation. Articles 12-14 exempt intermediaries from liability in cases where the users of the intermediary's platform, network etc. infringe the rights of others. The provisions on liability exemptions are considered a precondition for the development of popular and valuable online services and platforms in the EU. It is a distinct feature of the EU liability regime that the EU harmonized rules do not establish the contributory liability of the intermediaries. Articles 12-15 harmonize solely the exemptions from contributory liability. It is the national law of each Member State that establishes the standard of contributory liability which means that if an intermediary is not found to be contributory liable under national law, the harmonized liability exemptions are not relevant. Accordingly, it is possible that the same intermediary providing the same service in all EU Member States is found to be contributory liable in one Member State but not in another.[20]

In 2016, the European Commission concluded that the existing intermediary liability regime is fit for purpose, but that regulatory action was needed to tackle the proliferation of

[19] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L335.

[20] Joined Cases C-236/08 to C-238/08 (*Google AdWords*), ECLI:EU:C2010:159 at para 107.

illegal content online.[21] Nordemann concludes in his report commissioned by European Parliament that the provisions on liability exemption "seem to be sufficiently flexible to adopt to new business models, which also make them in general future proof."[22] For the present purpose, it suffices to have a closer look at Articles 14 and 15.

3.1. Liability of intermediary service providers: Hosting Article 14

According to Article 14 of the E-Commerce Directive a service provider whose service consists of the storage of information provided by a recipient of the service, is not liable for the information stored at the request of a recipient of the service. However, the exemption is conditioned on:

> *"(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or*
>
> *(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."*

The E-Commerce Directive regime for hosting providers including online platforms has led to the establishment of notice-and-takedown mechanisms.[23] The notice to the online platform by an infringed right holder provide the online platform with actual knowledge of the illegal activity or information and the online platform's takedown mechanism ensures the expeditious removal of the information.

It is a condition for liability exemption that the information is provided by the user of the platform and is uploaded on the request of the user. This indicates the crucial condition that the platform has a purely passive role in distributing the information. Along the same lines, the CJEU, in joined Cases C-236/08 to C-238/08 (*Google AdWords*)[24], emphasized that it follows from recital 42 in the preamble to E-Commerce Directive that the exemptions from liability cover only cases in which the activity of the information society service provider is 'of a mere technical, automatic and passive nature'. This implies that that service provider 'has neither knowledge of nor control over the information which is transmitted or stored'. Accordingly, in order to establish whether the liability of a referencing service provider (i.e. Google) may be limited under Article 14, it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and

---

[21] European Commission, "Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe," Brussels, May 25, 2016, COM(2016) 288 final.

[22] J.B. Nordemann, "Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?", Study commissioned by European Parliament, Policy Department A: Economic and Scientific Policy (2017) 18, available at *http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614207/IPOL_IDA(2017)614207_EN.pdf.*

[23] On notice-and-takedown procedures, *see e.g.* K. Wallberg, "Notice and takedown of counterfeit goods in the Digital Single Market: a balancing of fundamental rights" 12(11) *Journal of Intellectual Property Law & Practice* (2017); K. Erickson and M. Kretschmer, "'This Video is Unavailable': Analyzing Copyright Takedown of User-Generated Content on YouTube" 9 JIPITEC 3, available as pre-print at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144329*; D. Keller, "Empirical evidence of "over-removal" by internet companies under intermediary liability laws", (The Center for Internet and Society at Stanford Law School, Oct. 12, 2015), available at *http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws.*

[24] Cases C-236/08 to C-238/08 (*Google AdWords*).

passive, pointing to a lack of knowledge or control of the data which it stores.[25] Hence, the distinction between passive distribution and the platform's active use of the information is delicate and cannot be described in general term but relies on the specific circumstances of the case.

To escape liability, the platform must not have 'actual knowledge of illegal activity or information' and it is not quite clear how strict this condition is. If the platform has a reasonable substantiated suspicion that the content is illegal, does that amount to 'actual knowledge' within the meaning of the liability exemption? The question should probably be answered in the negative. In Case C-324/09 (*eBay*), the CJEU found that "it is sufficient, in order for the provider of an information society service to be denied entitlement to the exemption from liability provided for in Article 14 of [the E-Commerce] Directive, for it to have been aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question and acted in accordance with Article 14(1)(b) of [the E-Commerce] Directive."[26] The Court added that Article 14 must be interpreted as covering every situation in which the provider concerned becomes aware, in one way or another, of such facts or circumstances.[27]

Another aspect of the term 'actual knowledge' is whether this refers to 'general knowledge' or exclusively to 'specific knowledge'. A sharing platform, such as YouTube, has the general knowledge that a large amount of the content uploaded by its user is illegal, but the platform does not have the specific knowledge of what content this applies to. Liability on the basis of general knowledge would compel a platform to institute measures to monitor the information which they transmit or store and that would violate the prohibition against such a general obligation in Article 15 of the E-Commerce Directive. Hence, 'actual knowledge' must equate 'specific knowledge'.

In most situations in practice, platforms will become aware of illegal content by notifications from the right holders. In such cases, and provided that the content is illegal, the platform is liable if it does not expeditiously remove the content. However, it is normally impossible, or at the best very onerous, for the platform to decide whether the content actual is illegal and therefore, to be on the safe side, the platform will have incentives to remove all notified content including legal content and that creates a chilling effect. The risk of misuse of notifications is probably the reason why the CJEU has modified the notion of awareness by notification by stating in the Case C-324/09 (*eBay*) that

> *"although such a notification cannot automatically preclude the exemption from liability provided for in Article 14, given that notifications of allegedly illegal activities or information may turn out to be insufficiently precise or inadequately substantiated, the fact remains that such notification represents, as a general rule, a factor of which the national court must take account when determining, in the light of the information so transmitted to the operator, whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality."*[28]

3.2. No general obligation on platforms to monitor: Article 15

[25] *Id.* at paras. 113-114. Similar in Case C-324/09 (*eBay*) ECLI:EU:C:2011:474, para 113.
[26] Case C-324/09 (*eBay*), para 120.
[27] *Id.* at para 121.
[28] *Id.* at para 122.

It follows from Article 15(1) of the E-Commerce Directive that Member States shall not impose a general obligation on providers, who benefit from the liability exemptions, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

One particular issue is how these various proactive measures could be reconciled with Article 15. It prohibits 'general obligations' and not obligations as such. In that respect, one important question is how to distinguish between prohibited general monitoring obligations and specific monitoring duties, which may be imposed on providers in conformity with Article 15(1).[29]

The CJEU has in two decisions decided that a national court must not order an intermediary a general obligation to implement effective filtering technologies. Case C-70/10 (*Scarlet Extended*)[30] concerned a Belgian court that ordered an internet service provider (Scarlet Extended SA) that provided services such as downloading or file sharing, to bring an end to copyright infringements by making it impossible for its customers to send or receive in any way files containing a musical work in the national collecting society's (SABAM) repertoire by means of peer-to-peer software. Scarlet Extended claimed that it was impossible for it to comply with that injunction since the effectiveness and permanence of filtering and blocking systems had not been proved and that the installation of the equipment for so doing was faced with numerous practical obstacles. In addition, Scarlet Extended claimed that complying with the order would constitute a violation of Article 15 of the E-Commerce Directive. The CJEU held that the injunction imposed on Scarlet Extended concerned requiring it to install the contested filtering system would oblige it to actively monitor all the data relating to each of its customers in order to prevent any future infringement of intellectual property rights. Thus, the order would require Scarlet Extended to carry out general monitoring contrary to Article 15(1).[31] The CJEU applied a similar reasoning and result in Case C-360/10 (*Netlog*).[32]

3.3. Will platforms using pro-active measures lose their safe harbor?

The *Scarlet Extended* and *Netlog* judgments suggest that rules that impose obligations on intermediaries to implement pro-active measures will be in conflict with Article 15 of the E-Commerce Directive.

Another issue of particular interest is to what extent intermediaries would lose their safe harbor by implementing such proactive measures voluntarily. The train of thought here is that, firstly, given the use of proactive measures, the intermediaries could qualify as active and thus fall outside the scope of the safe harbor. Secondly, that they will have more information on the activities taking place on their platform or in their network and, consequently, in many more situations are considered to 'be aware' of illegal activities.[33]

The preamble of Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online clarifies the European Commission's stance in this respect. The Commission has set out its view that taking such voluntary proactive measures does not automatically lead to the hosting service provider concerned losing the benefit of the liability exemption

[29] *See* J.B. Nordemann, cited *supra* n.22 at 16.
[30] Case C-70/10 (*Scarlet Extended*) ECLI:EU:C:2011:771.
[31] Case C-70/10 (*Scarlet Extended*), para 40.
[32] Case C-360/10 (*Netlog*).
[33] A. Kuczerawy, "The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?", (KU Leuven, CITIP Blog, April 24, 2018), available at *https://www.law.kuleuven.be/citip/blog/the-eu-commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5/*.

provided for in Article 14 of the E-Commerce Directive.[34] Obviously, voluntarily use of proactive measures will not *de jure* limit the scope of Article 14, however, the implementation of such measures will *de facto* take away a substantial part of the intermediaries' safe harbor protection to a degree that depends on the effectiveness of the measures.

3.4. Intersection to fundamental rights

The increasing use of proactive measures, either voluntary or by means of law creates a risk of infringing *i.a.* the freedoms of information and privacy.

In the *Scarlet Extended* case[35], the CJEU also evaluated whether such an obligation to implement filtering technologies would violate fundamental rights. When considering ordering an internet service provider to install filtering technologies to protect copyright holders, national courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures and such a fair balance was not struck in the specific case.

The Court referred to the facts that (1) the installation of the contested filtering system involves monitoring all the electronic communications made through the network of the Scarlet Extended; (2) that monitoring has no limitation in time; and (3) is intended to protect not only existing works, but also future works that have not yet been created at the time when the system is introduced. Accordingly, the filtering system would result in a serious infringement of the freedom of Scarlet Extended to conduct its business, cf. Article 16 of the EU Charter of Fundamental Rights. The CJEU further referred to that the order would require Scarlet Extended to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions laid down in Article 3(1) of the Enforcement Directive[36], which requires that measures to ensure the respect of intellectual property rights should not be unnecessarily complicated or costly.[37]

Moreover, the Court found that the filtering system would involve a systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is send. Those information are protected personal data because they allow those users to be precisely identified and, hence, the filtering system will also infringe the users' right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the EU Charter respectively. In addition, another infringement of the freedom of information occurs, potentially, if the filtering system cannot not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications.[38]

4. CONCLUSION

When we look at the emerging tendency of the European lawmaker to encourage the use of proactive filtering mechanisms, it is obvious that this is an envisaged solution for many forms of illegal content. First suggested in relation to copyright in the Proposal for a Directive on

[34] Recommendation (EU) 2018/334, Recital 26.
[35] Case C-70/10 (*Scarlet Extended*).
[36] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L195/16.
[37] Case C-70/10 (*Scarlet Extended*), paras. 45-49.
[38] Case C-70/10 (*Scarlet Extended*), paras. 50-54.

copyright in the Digital Single Market in September 2016, the idea is found to be the appropriate response broadly to illegal content (Recommendation) and terrorist content (Proposal for Regulation).

It is safe to say that the European institutions have either departed or are about to depart from their traditional stance on the role of Internet intermediaries in light of illegal online content. Article 13 of the proposed Directive on copyright in the digital single market represents a change in strategy with its carve-out from the E-Commerce Directive's safe harbor rule in the copyright sphere. The advocacy for proactive measures in the Commission's Recommendation further underlines this trend.

Especially the voluntary and self-regulatory aspects are problematic.[39] Voluntary implementation of proactive measures, inadvertently, reduces intermediaries' safe harbor protection. Furthermore, harms in respect to fundamental rights that the CJEU emphasized in the *Scarlet Extended* and *Netlog* judgments may also occur.

A specific problem relates to Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online because it is issued by the European Commission and has not gone through the European Parliament and European Council, thus albeit it is weaker, the instrument lacks to a certain extent democratic legitimacy.

The implementation of voluntary measures may also gradually influence the standard of liability. According to the CJEU in Case C-324/09 (*eBay*), exemption of liability as a host under Article 14 of the E-Commerce Directive requires that an intermediary should not have been aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question.[40] When more and more intermediaries implement voluntary proactive measures there is a risk that, at a certain time, a court will find that a diligent economic operator will implement proactive measures. In this way, the exemption from liability under Article 14 can be eroded.

Proactive measures must be considered to be blunt instruments. Firstly, due to the risk of the intermediary of being liable for the users' infringement, the intermediaries are expected to adjust the systems so that they rather take down too much than too little. Secondly, at the present state of technology, proactive measures are not smart enough to distinguish between lawful and unlawful content in all cases. When popular microblogging platform Tumblr started to algorithmically enforce a strict adult content policy in December 2018, it led to the flagging of much non-adult content and public ridicule. This could for instance be problematic the case for parodies in the form of memes because in the individual cases, it is very difficult and complicated to decide if a meme is covered by the copyright exception in the Infosoc Directive for parodies.[41] The issue is further complicated by the fact that the application of statutory exceptions to copyright varies from one Member State to another. Moreover, in some Member States certain works fall within the public domain or can be posted online free of charge by the authors concerned.[42]

It follows from the *Scarlet Extended* and *Netlog* judgments that an order to implement filtering systems that remove legal content may violate the freedom of information pursuant to Article 11 of the EU Charter. However, private entities have more freedom to implement

[39] See also G. Frosio, "Why keep a dog and bark yourself? From Intermediary Liability to Responsibility" Centre for International Intellectual Property Studies Research Paper No. 2017-11.
[40] Case C-324/09 (*eBay*), para 120.
[41] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2011 on the harmonisation of certain aspects of copyright and related rights in the information society, Article 5(3) lit. (k).
[42] Case C-70/10 (*Scarlet Extended*).

such measures without being in conflict with fundamental rights. The finding of the CJEU in the *Scarlet Extended* and *Netlog* judgments that an order to implement filtering technologies violates Article 15 of the E-Commerce Directive and fundamental rights, in principle, must also be considered applicable to other rules that create an obligation to implement proactive measures.[43]

Against this background, the various provisions on proactive measures such as in the proposed Directive on copyright in the Digital Single Market, the proposed Regulation on terrorist content and the Recommendation are problematic. Relying on mythical algorithms to solve content issues might appear appealing. But just as a sailor prepares its boat to leave its safe harbor, regulatory intervention –whether based on self-regulation, soft or hard law– needs to be a thorough endeavor based on a careful balancing of interests and transparent information about the workings of these mechanisms.

[43] Position Statement of the Max Planck Institute for Innovation and Competition on the Proposed Modernisation of European Copyright Rules (2017), PART G, paras. 15 et seq., available at *https://www.ip.mpg.de/fileadmin/ip-mpg/content/stellungnahmen/MPI_Position_Statement_PART_G_incl_Annex-2017_03_01.pdf.*