The European Commission's Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online

Gavin Robinson

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

In September 2018, the European Commission presented a draft Regulation on preventing the dissemination of terrorist content online. The proposal builds on EU-level initiatives to foster the voluntary cooperation of service providers in stopping the dissemination of terrorist content online, and it echoes ongoing national developments which go a step further in imposing obligations – underpinned by considerable fines – on service providers. This article describes the main features of the proposal and highlights some of the policy challenges, legal questions, and technological concerns it is likely to face on the road to adoption.

AUTHOR

Gavin Robinson

Postdoctoral Researcher, Criminal law & IT law
Université de Luxembourg

CITE THIS ARTICLE

Robinson, G. (2018). The European Commission's Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2018-024

Published in eucrim 2018, Vol. 13(4) pp 234 – 240

https://eucrim.eu

ISSN:

I. Introduction

At the informal European Council summit in Salzburg on 19th and 20th September 2018, the European Commission presented a draft Regulation on preventing the dissemination of terrorist content online.[1] The proposal builds upon EU-level initiatives to foster the voluntary cooperation of service providers in stopping the dissemination of terrorist content online, chiefly the cross-sectoral EU Internet Forum and the work of Europol's Internet Referral Unit (IRU). It also echoes ongoing national developments which go a step further in imposing obligations – underpinned by considerable fines – on service providers to hastily remove illegal content and prevent re-uploading, such as the German *Netzwerkdurchsetzungsgesetz (NetzDG)*, passed in June 2017. The Regulation would apply to "hosting service providers" (HSPs), defined as "a provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to third parties" (Art. 2(1)).[2] Another prerequisite is that HSPs offer services in the Union, irrespective of their place of main establishment (Art. 1(2)).

The draft Regulation, which is strongly supported by both France and Germany, takes a four-pronged approach to terrorist content online:

- At the "light touch" end of the regulatory spectrum it seeks to establish EU-wide general duties of care on HSPs to take "appropriate, reasonable and proportionate actions […] against the dissemination of terrorist content and to protect users from terrorist content" (Art. 3);
- It would enshrine a framework of practical arrangements for HSPs' own assessment of terrorist content once "referred" to them by national competent authorities or the relevant Union body (Europol) (Art. 5), discussed below under II.;
- It introduces removal orders, to be issued by national competent authorities, which must be complied with within one hour (Art. 4). This is the proposal's flagship measure, and is discussed below under III. In addition to the tight deadline, the removal order comes with the most bite of the measures foreseen in the draft Regulation: whilst HSPs in breach of the quasi-totality of the obligations anchored in the draft Regulation risk incurring penalties, a "systematic failure to comply" with removal orders specifically shall be subject to financial penalties of up to 4% of the HSP's latest yearly global turnover (Art. 18(4));
- It seeks to erect a compliance framework aiming to ensure that HSPs develop and take proactive measures, "including by using automated tools", in order to protect their services against the dissemination of terrorist content (Art. 6). The development and use of proactive measures, discussed below under IV., are subject to rather terse obligations relating to transparency (Art. 8) and safeguards (Art. 9).

II. Referrals

The inclusion of a referral mechanism in the draft Regulation reflects increasingly intensive co-regulatory efforts undertaken by EU, national and industry actors in recent years. Most notably, 2015 saw two key developments:

- First, the European Commission launched the EU Internet Forum to bring together the internet industry and Member States, as well as Europol, the Radicalisation Awareness Network and the European Strategic Communications Network in order to tackle the spread of terrorist content online;

https://doi.org/10.30709/eucrim-2018-024

- Second, Europol itself established internally the so-called EU Internet Referral Unit (IRU) to actively scan the internet for terrorist content and refer it to host platforms. The Commission reports that "over 50,000 decisions for referrals across over 80 platforms in more than 10 languages have been made since 2015", whilst five Member States have since set up their own IRUs.[3]

Notwithstanding this increased voluntary activity, the Commission now posits that "referrals alone will not be able to achieve the necessary impact – particularly with regards [sic] to volume and speed of response",[4] necessitating also the introduction of removal orders and the development of proactive measures, discussed below under III. and IV. As such, the principal attraction of formalising the referral mechanism in a Regulation is represented by the attendant fines which it would require;[5] the firm application of as-yet-undefined penalties is envisaged specifically in relation to HSPs' "assessment of and feedback on referrals" (Art. 18(1)(c)). Although referrals are to be assessed not against provisions in EU or national law but against service providers' own terms and conditions (Art. 5(5)),[6] and as a rule the idea remains that it is HSPs which shall decide whether or not to take action, the pressure which HSPs are likely to come under from competent authorities sits uneasily with the term "voluntary consideration" (Art. 5(2) and Art. 2(8)). The choice of wording is all the more regrettable since HSPs "shall, as a matter of priority, assess the content […]" (Art. 5(5)), meaning that HSPs' consideration of putative referred terrorist content is actually not voluntary but mandatory, with sanctions hovering over them in case of poor performance.

In assessing referrals from national competent authorities or from Europol, HSPs will have to grapple with the Regulation's definitions of terrorist content. According to Art. 2(5) of the draft Regulation, "terrorist content" means one or more of the following information:

> "(a) inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed;
>
> (b) encouraging the contribution to terrorist offences;
>
> (c) promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541;
>
> (d) instructing on methods or techniques for the purpose of committing terrorist offences."

The Commission presents the inclusion of the last three categories, which are broader than the corresponding provisions in the 2017 Directive on combating terrorism,[7] as a step to provide clarity to HSPs and competent authorities and as a basis for more effective preventative action,[8] given the variable nature of content used for radicalisation purposes. In this context, the Commission refers to real-life cases:[9] (1) a Danish schoolgirl found guilty in 2017 of attempted terrorism having tried to make bombs to be used in attacks against her former school (radicalised via internet and chat contacts within a few months); (2) *Daesh's* tactics to "groom" young children (using cartoons); and (3) the attack on the Thalys train in 2015 that was provoked in the preceding moments by a "call to arms" on a YouTube audio file. Yet the examples of terrorist content cited all ostensibly feature an element that was not taken up by the definition in the draft Regulation: intent. This has raised concerns that any communication of terrorist-related content will be automatically deleted, irrespective of the context of its use (i.e. for confrontation, reporting, research or historical purposes).[10] Without offering an explicit justification, the draft not only "draws on" (cf. recital 9), but also goes beyond the wording of the takedown obligation in the Directive on combating terrorism.[11]

With that said, the converse would have seen HSPs tasked with assessing the intentions of content providers, thereby adding a further level of complexity to their task of identifying the content *per se* as terrorist, meaning *inter alia* "the nature and wording of the statements, the context in which the statements were made and their potential to lead to harmful consequences, thereby affecting the security and safety of per-

sons".[12] Faced with this heavy responsibility, HSPs as well as competent authorities are suitably reminded of the importance of freedom of expression and information, "one of the values on which the Union is founded".[13] Digital rights campaigners, however, are unlikely to be reassured by much of the supporting argumentation put forward by the Commission.

In explaining its decision to broaden the definition of terrorist content to include recruitment and training for terrorism, the Commission draws attention to safeguards including (domestic) "judicial reviews of removal orders and the possibility to issue a counter-notice, as well as measures taken to mitigate the possibility of erroneous removals when deploying proactive measures".[14] Yet as regards referrals, which are non-binding, available redress is in fact limited to (private) complaint mechanisms (Art. 10). Moreover, the fact that HSPs' assessments are to be facilitated by the prior appraisal of Europol and national authorities (which may be of a judicial, administrative, or most pertinently law enforcement nature) "with particular expertise to identify whether or not the content could potentially constitute terrorist content as defined by law" is proffered as a "safeguard" against erroneous removals.[15] This reasoning seems to presuppose – and depend on – high levels of trust in the competent authorities.

III. Removal Orders

Under the proposal, national competent authorities may also issue removal orders to HSPs. Member States are free to assign this task to either administrative, law enforcement or judicial authorities.[16] In contrast to referrals (see II.), HSPs must comply with removal orders within one hour of reception (Art. 4(2)). Thus, the provider can only decide whether to remove the relevant content or to block access thereto.[17] Removal orders sent to HSPs shall contain, *inter alia,* a statement of reasons explaining why the content is considered terrorist content by reference to the definitions used in the draft Regulation, information enabling the identification of the content referred (typically a URL), and information about redress available to both the HSP and to the content provider.

From the content providers' perspective, the draft Regulation provides that HSPs are in turn to supply them with "information" regarding the removal or blocking of content (Art. 11(1)) and (upon request of the content provider) reasons for such action (Art. 11(2)). However, these obligations may be suspended for up to four weeks where the competent authority decides for reasons of public security, such as the prevention, investigation, detection and prosecution of terrorist offences, that no information on removal or blocking should be disclosed. Although the instrument would require HSPs to establish (private) mechanisms allowing content providers to complain and request the reinstatement of content removed or blocked pursuant to a referral or via proactive measures (Art. 10), this – understandably – does not apply to content removed or blocked by HSPs pursuant to a non-negotiable one-hour removal order.

Rapidity is the order of the day not only as regards HSPs' responses to removal orders; it also characterises the recent policy-making flurry at EU level. The proposal for a Regulation comes hot on the heels of the Commission's March 2018 Recommendation on measures to effectively tackle illegal content online. It encouraged Member States to develop their response to all types of illegal content, *inter alia,* through systems of notices to HSPs, informing content providers and counter-notices, transparency and safeguards, and the cooperation of HSPs with national competent authorities, with "trusted flaggers", and amongst themselves.[18] Indeed, most of the core provisions of the draft Regulation have been fleshed out from the Commission's earlier specific recommendations relating to terrorist content, which featured *inter alia* a ban on terrorist content in HSPs' terms of service, referrals, proactive measures, cooperation and the one-hour rule:[19]

https://doi.org/10.30709/eucrim-2018-024

> "Hosting service providers should assess and, where appropriate, remove or disable access to content identified in referrals, as a general rule, within one hour from the moment at which they received the referral."

Should the draft Regulation enshrine the one-hour rule in EU law, this will represent a real change of gear compared to the existing general, open-ended obligation on Member States to "take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence" (Art. 21 of Directive (EU) 2017/541 on combating terrorism). The deadline for implementation of the Directive passed on 8 September 2018 – less than a fortnight before the draft terrorist content Regulation was unveiled – with the Commission stating that 15 Member States had notified it of measures giving effect to their Art. 21 obligation in their domestic systems.[20] Arguably, an evaluation of national measures taken pursuant to Art. 21 would be essential to gauging the added value of the Directive, as well as "its impact on fundamental rights and freedoms, including on non-discrimination" (Article 29, Directive on combating terrorism). The distant deadline for the Commission's added value report, however, is 8 September 2021.

In opting to respond to Member State pressure with a proposal for a Regulation[21] before any such evaluation of the Terrorism Directive has occurred, the Commission may also have been swayed by its experience of chasing up the slow and patchy implementation of Art. 25 of Directive 2011/92/EU. This provision stipulates that Member States *shall* on the one hand take the necessary measures to ensure the prompt removal of, and *may* on the other hand take measures to block access to, web pages containing or disseminating child pornography.[22]

The draft Regulation covers the main practical matters on the procedure for removal/blocking orders, e.g. nomination of HSP points of contact or legal representatives, framework for interaction between HSPs and competent authorities, provisions on language etc., but, as noted above, controversially[23] leaves open a key aspect to the Member States: the choice of competent authority. The Commission itself notes that in the majority of national systems a takedown order may come only from a judicial body within criminal proceedings. Some Member States, however, provide for administrative orders – subject to appeal before a court – and in a few Member States even law enforcement authorities can issue removal orders and refer content to service providers.[24]

This flexibility stands in contrast to the one-hour rule, which applies only to removal orders, is far tighter than existing provisions in national law mandating, for instance, removal within 24 or 48 hours,[25] and is justified by the Commission by reference to the speed at which terrorist content is claimed to spread across online services.[26] The preference for such a short window for removal or blocking goes hand-in-hand with the Commission's choice to eschew an "all illegal content" approach – deemed "unnecessary and disproportionate"[27] – and focus instead on terrorist content as a priority, at least for now.

The immediate imperative to act at national level is of course constituted by the increasing use of HSPs to disseminate terrorist content. The main driver for EU action on an Art. 114 TFEU legal basis, meanwhile, is the hindrance to the effective exercise of freedom of establishment and freedom to provide services across the Union which may result from the legal uncertainty caused by a deepening "fragmentation" of national responses to the removal or disabling of access to illegal content in general (as already envisaged in the e-commerce Directive)[28] and terrorist content in particular (as recently mandated by the Terrorism Directive). Here too, there is fertile ground for debate over the coming months as to the true necessity of EU action – and not only from a freedom of expression perspective. Notably, whereas one might expect the anchoring of such a forceful rule as the one-hour window in a Regulation to receive solid backing from law enforcement circles, national law enforcement authorities are in fact cited by the Commission as favouring the continuation of self-regulatory initiatives, "allowing industry to take the lead … whilst working closely with them".[29]

https://doi.org/10.30709/eucrim-2018-024

On the HSP side, the Commission also cites input from "companies" to the effect that diverging legislation is a serious concern and smaller companies are likely to suffer the most from 28 different sets of rules.[30] This position call for two remarks. First, although it seems undeniable that the functioning of the "country of origin" principle would likely be undermined by the continued proliferation of national removal order systems with differing assessments of terrorist content (e.g. compliance with regulatory requirements in one Member State ensuring access to all others, only for one or several of those other Member States to remove or block access to content), the added value of the draft Regulation in this specific respect would seem to depend on levels of cohesiveness between competent authorities which are high enough to produce similarity between the decisions they take.[31] This may raise workability concerns, particularly given the likely varying nature of competent authorities and the open-ended definition of terrorist content they are to be mandated to apply. Second, with regard to impact on smaller HSPs, achieving readiness to respond to one-hour takedown orders could indeed affect small companies even more compared to the status quo – although this is, in principle, to be factored into sanctioning decisions.[32] In these respects, we can expect industry to call for further clarification and substantiation in the near future.

IV. Proactive Measures

Perhaps the most novel section of the draft Regulation entails a duty on HSPs to take proactive measures to protect their services against the dissemination of terrorist content (Art. 6). HSPs are to report to the competent authority[33] on "the specific proactive measures […] taken, including by using automated tools, with a view to:

- preventing the re-upload of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content;
- detecting, identifying and expeditiously removing or disabling access to terrorist content".[34]

Should the competent authority deem such measures to be insufficient, the HSP is bound to cooperate with it in order to establish "key objectives and benchmarks as well as timelines for their implementation" (Art. 6(3)). Where no agreement can be reached, the taking of specific proactive measures can be imposed on HSPs by the competent authority (Art. 6(4)). Penalties for HSPs which fail to report on proactive measures, or to adopt such measures following a decision imposing them, are to be set out at national level (Art. 18(1)(d)).

This mini-compliance framework for the automated detection and removal of terrorist content channels a fairly recent but major growth in political pressure[35] as well as industry activity, chiefly in the form of a pooled "hash database".[36] The extent to which such initiatives and the technologies they employ are truly effective at accurately identifying terrorist content (as distinct from removing vast swathes of content)[37] raises a set of thorny issues which are likely to play out in the months to come, particularly given the European Parliament's position on the importance of transparency in the use of algorithms. In this context, the EP recently called on the Commission and the Member States to "examine the potential for error and bias in the use of algorithms in order to prevent any kind of discrimination, unfair practice or breach of privacy".[38]

Counterbalancing its provisions designed to foster the uptake of proactive measures, the draft Regulation stipulates standard GDPR-era obligations on HSPs. These include the provision of a meaningful explanation of such tools in their terms and conditions, the publication of transparency reports (including "information" and absolute figures on action taken and complaint procedures) and the provision of safeguards to ensure that decisions taken concerning stored content are "accurate and well-founded". Safeguards shall consist, in particular, of "human oversight and verifications where appropriate and, in any event, where a detailed

https://doi.org/10.30709/eucrim-2018-024

assessment of the relevant context is required in order to determine whether or not the content is to be considered terrorist content" (Art. 9). Beyond the European Parliament's calls for caution, it is worth noting the concerns voiced by *David Kaye*, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, a few weeks before publication of the draft Regulation. In his report, *Kaye* makes specific reference to the application of artificial intelligence (AI) tools to online content and states:[39]

> "Even when algorithmic content moderation is complemented by human review – an arrangement that large social media platforms argue is increasingly infeasible on the scale at which they operate – a tendency to defer to machine-made decisions (…) impedes interrogation of content moderation outcomes, especially when the system's technical design occludes that kind of transparency".

The Commission considered several options with regard to the use of automated tools: deferring to companies' own risk assessment; mandatory uptake of measures limited to the prevention of re-uploading of known terrorist content; and mandatory uptake of "appropriate proactive measures, including by using automated detection tools".[40] Despite the above-mentioned misgivings, which can also be found amongst EU Member State governments,[41] the Commission has chosen the most far-reaching option. It does so whilst acknowledging[42] that should proactive measures inadequately distinguish between unlawful and lawful conduct, this may risk undermining, *inter alia,* freedom of information in contravention of settled EU law.[43] This tense relationship with standing CJEU case law barring the imposition of systematic ISP (internet service provider) filtering for copyright breaches is also reflected in the wording of recital 16 to the draft Regulation. That recital states that whilst on the one hand it is up to HSPs to determine what proactive measure should be put in place, on the other hand "(t)his requirement should not imply a general monitoring obligation". Should the co-legislators concur with those judges who have remarked that the use of automated processes is "pushing in the direction" of a general monitoring obligation,[44] we may yet see a return in the final text to one of the more limited policy options evoked in the Commission's Impact Assessment.

Lastly, a less immediately obvious legal tangle may await the proposal in general, and its drive toward proactive measures in particular. Art. 7 of the draft Regulation obliges HSPs to preserve terrorist content which has been removed or disabled as a result of a removal order, a referral or proactive measures. With a preservation period set at six months (extendable), the potential ramifications of this framework are bound to attract comparisons to the (annulled) Data Retention Directive – especially insofar as the obligation not only covers the targeted terrorist content per se but also extends to "related data removed as a consequence of the removal of the terrorist content" (Art. 7(2)).

The term "related data" is not defined in the main text of the draft Regulation, but subscriber data and access data are given as examples in recital 20. This is unlikely to quell fears of over-preservation by HSPs and will likely fuel calls for a more precise wording. Moreover, whatever data is preserved by HSPs as being in their estimation "likely to have a link with terrorist offences" (recital 21) may be used for the prevention, detection, investigation and prosecution of terrorist offences (Art. 7(1)(b)). Depending on definitions in place in national systems, these purposes may open broad channels of access to large amounts of data generated by the customers of HSPs. In turn, this approach triggers concerns regarding profiling, particularly in light of the CJEU's language on the use of non-content data to draw "very precise conclusions concerning the private lives of the persons whose data has been retained"[45] and lead to "the feeling that (users') private lives are the subject of constant surveillance".[46]

V. Outlook

For the reasons evoked in this overview, the strong political support for swift regulatory action on terrorist content online, which is reflected in the Commission's draft Regulation, is sure to be tested as the proposal progresses through the EU's legislative procedure – in particular by pressure from the Internet industry and digital rights groups.

Taken as a whole, the proposal envisages the transformation of extant co-regulation and voluntary self-policing by hosting service providers (HSPs) into a framework of obligations (to respond to referrals; to comply with removal orders; to implement proactive measures) bolstered by sit-up-and-take-notice sanctions. To deliver on this vision, the dossier will have to navigate doubts as to the necessity of taking such action at EU level. This may be accompanied by principled objections on grounds of freedom of expression. The initiative will also encounter narrower concerns over its potential impact on smaller HSPs and over key matters of scope and legal certainty – right down to the broadly termed definition of "terrorist content" provided therein.

With the EU Council having agreed its negotiating position on the proposal in early December 2018,[47] the ball is now squarely in the European Parliament's court. Given that the next elections to the Parliament are scheduled for late May 2019, we can expect the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) to finalise its report on the proposal before then. We may have to wait until the fourth quarter of 2019, however, to see interinstitutional talks begin.

---

1. COM(2018) 640 final.↩
2. Recital 10 of the draft gives as examples: "social media platforms, video streaming services, video, image and audio sharing services, file sharing and other cloud services to the extent that they make the information available to third parties and websites where users can make comments or post reviews".↩
3. SWD(2018) 408 final, "Impact Assessment", 140.↩
4. Impact Assessment, ibid.↩
5. The draft Regulation also advises that receiving a high number of referrals – or removal orders – indicates a high level of exposure to terrorist content, meaning proactive measures are more likely to be necessary (see e.g. recital 16).↩
6. By virtue of the aforementioned duties of care (and in a rather circular dynamic) such terms and conditions must include provisions to prevent the dissemination of terrorist content (Art. 3(2)).↩
7. "Member States shall take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence"; Art. 21 of Directive (EU) 2017/541 of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, *O.J.* L 88, 31.3.2017, p. 6.↩
8. See recital 9 of the draft Regulation.↩
9. Cf. Impact Assessment, op cit. (n. 3), 17.↩
10. *EDRi,* "EU's flawed arguments on terrorist content give big tech more power", 24 October 2018, <https://edri.org/eus-flawed-arguments-on-terrorist-content-give-big-tech-more-power/> accessed 3 January 2019.↩
11. Public provocation to commit a terrorist offence is defined non-exhaustively in the Directive on combating terrorism (op. cit. n. 7) as "the distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission of one of the offences listed in points (a) to (i) of Art. 3(1), where such conduct, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed, is punishable as a criminal offence *when committed intentionally*" (Art. 5; emphasis added).↩
12. Recital 9 taking up relevant ECtHR case law. Moreover, recital 9 mentions that "(t)he fact that material was produced by, is attributed to or disseminated on behalf of an EU-listed terrorist organisation or person constitutes an important factor in this assessment".↩
13. Recital 7.↩
14. Impact Assessment, op. cit. (n. 3), 103.↩
15. Impact Assessment, op. cit. (n. 3), 42. See also Annex 5, Impact on Fundamental Rights: "(W)hen referrals are issued by Europol, the fact that Europol is bound to act only within its mandate (…) makes it unlikely that any removal decision based on referrals would concern protected speech. The obligation on HSPs to assess the content flagged through referrals could have a significant impact on the freedom to conduct a business (…). The burden is alleviated by the high quality of the Europol and Member States (sic) referrals" (Impact Assessment, p. 104).↩
16. Cf. recital 13.↩
17. Cf. recital 13.↩
18. Recommendation (EU) 2018/334, *O.J.* L 63, 6.3.2018, 50. See also the subsequent European Council conclusions of 28 June 2018, at para. 13: "… welcomes the intention of the Commission to present a legislative proposal to improve the detection and removal of content that incites hatred and to commit terrorist acts".↩

https://doi.org/10.30709/eucrim-2018-024

19. Recommendation (EU) 2018/334, ibid, para. 35.↩
20. Impact Assessment, op cit. (n. 3), 9 and 116.↩
21. An amendment of the Terrorism Directive, for instance to broaden the activities/material covered therein from incitement to terrorism only to other offences (as proposed in the draft Regulation), was discarded by the Commission. It argued that "the focus on criminalisation of terrorist offences as opposed to purely preventative measures, the geographical limitations and limitations in terms of safeguards and other flanking measures (which would not have been possible under this legal basis) (…) would have had limited impact on the objective of preventing the dissemination of terrorist content" (Impact Assessment, op cit. (n. 3), 25).↩
22. See COM(2016) 872 final, where the Commission (at 12) stated that continued work was still required to ensure the "complete and correct implementation" of Art. 25 across the Member States – a full three years after the deadline of 18 December 2013, with the Commission having opened infringement proceedings against a total of 15 Member States.↩
23. In this regard, see the concerns raised by a coalition of 31 civil society organisations in a letter sent to EU Member States' Home Affairs Ministers on 4 December 2018, available at <https://edri.org/files/counterterrorism/20181204-CivilSociety_letter_TERREG.pdf> accessed 3 January 2019.↩
24. Impact Assessment, op cit. (n. 3), 9-10.↩
25. Impact Assessment, op cit. (n. 3), 116.↩
26. See also the "evidence summary" on terrorist content online (Annex 9, Impact Assessment, op cit. (n. 3), 138), referring to one example of UK Home Office analysis showing that a third of Daesh links are disseminated within the first hour.↩
27. Impact Assessment, op cit. (n. 3), 23.↩
28. Art. 14(3) of Directive 2000/31/EC,: "This article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information".↩
29. Impact Assessment, op cit. (n. 3), 116.↩
30. Impact Assessment, op cit. (n. 3), 10.↩
31. See e.g. Art. 13(1) of the draft Regulation: "Competent authorities in Member States shall inform, coordinate and cooperate with each other and, where appropriate, with relevant Union bodies such as Europol with regard to removal orders and referrals to avoid duplication, enhance coordination and avoid interference with investigations in different Member States".↩
32. Member States shall take into account *inter alia* "the financial strength of the legal person liable" in applying sanctions (Art. 18(3)(d)).↩
33. The "competent authority" may be different to that in charge of referrals and removal orders, see Art. 17.↩
34. Cf. Art. 6(2) of the Commission's proposal COM(2018) 640.↩
35. See the European Council conclusions on security and defence of 22 June 2017, point 2: "Building on the work of the EU Internet Forum, the European Council expects industry to establish an Industry Forum and to develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts. This should be complemented by the relevant legislative measures at EU level, if necessary". See also, subsequently to the Commission's proposal for a Regulation, European Parliament, Report on findings and recommendations of the Special Committee on Terrorism (2018/2044(INI)), 21 November 2018, 47: "underlines the need to achieve automatic detection and systematic, fast, permanent and full removal of terrorist content online on the basis of clear legal provisions including safeguards, and human review; […] welcomes the Commission' legislative proposal […]; calls on the co-legislators to urgently work on the proposal […]".↩
36. Under the aegis of the Global Internet Forum to Counter Terrorism, founded in June 2017 by the Big Four of Facebook, Microsoft, Twitter and YouTube. See <https://gifct.org/about/> accessed 3 January 2019.↩
37. Cf. the comment of D. Keller, "Inception Impact Assessment: Measures to Further Improve the Effectiveness of the Fight Against Illegal Content Online", 29 March 2018, available at SSRN: <http://dx.doi.org/10.2139/ssrn.3262950>, accessed 3 January 2019: "Technical filters cannot assess context or tell whether potentially terrorist content is actually illegal. No existing machine – be it a simple filter or the most advanced artificial intelligence – can review new material, or look at old material in a new context, and say with certainty whether it violates the law".↩
38. European Parliament, Report on online platforms and the digital single market (2016/2276(INI)), 31.5.2017, at 17 (Legal Affairs Committee) and 12 (full report).↩
39. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 29 August 2018, A/73/348, para. 15.↩
40. Impact Assessment, op. cit. (n. 3), 105.↩
41. Cf. Impact Assessment, op. cit. (n. 3), 120: "Regarding filtering, the (Dutch) government has indicated that this does not work adequately, since in case of terrorism unlawful content is not as evident as compared to e.g. child pornography, resulting in a disproportionate interference with the right to freedom of speech".↩
42. Impact Assessment, op .cit. (n. 3), 105.↩
43. CJEU, 24 November 2011, Case C-70/10, *Scarlet Extended SA v SABAM*, paras 50 *et seq.*↩
44. Impact Assessment, op .cit. (n. 3), 76.↩
45. CJEU, 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger*, para 27.↩
46. *Digital Rights Ireland,* ibid, para 37 and CJEU, 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB* and *Secretary of State for Home Department v Tom Watson and Others,* para 100. Cf. CJEU, 2 October 2018, Case C-207/16, *Ministerio Fiscal,* wherein a targeted request for access to data concerning a stolen mobile telephone was deemed to "not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned" (para 60).↩
47. Press release, "Terrorist content online: Council adopts negotiating position on new rules to prevent dissemination," 6 December 2018, <https://www.consilium.europa.eu/en/press/press-releases/2018/12/06/terrorist-content-online-council-adopts-negotiating-position-on-new-rules-to-prevent-dissemination/>, accessed 3 January 2019.↩