EDiMA

EDiMA examples document on the Regulation on preventing the dissemination of terrorist content online

In our effort to ensure that the Regulation can have an effective impact on the problem at hand, EDiMA has compiled an initial list of questions we still have regarding the practical transposition of the Regulation as well as examples we believe highlight the shortcomings and unintended consequences of the Regulation as it was proposed.

Scope: the problematic inclusion of all hosting service providers (HSPs)

- Any business that operates online has to store the data it uses, and most of them rely on the cloud infrastructure to do so, which enable their everyday operation and work.
- **Question:** Does the current text mean that when a company is sharing a file to another entity e.g. their accountants, the government or posting something on their website, the cloud providers have to monitor all their exchanges, in case the company spreads terrorist content to the other entity?

- **Question:** What happens if a cloud service provider (CSP) receives a request to take down one comment on a website or platform running on their service? Currently, the only technical solution is for the provider to shut down the entire service which could then mean that major sites e.g. BBC, messaging apps like Snapchat and public institutions could be removed from the CSP altogether.

- **Question:** What would the impact on SMEs be if B2B services are included?

Definitions:

- The current definition is very broad and would even cover a wide array of services including such niche areas such as map applications.
  Question: Does the text mean that companies would be expected to monitor every comment that is posted on a map somewhere in the world just in case potential terrorist content is included?

Competent authorities: the issue of the lack of coordination

- **Question:** What happens if two competent authorities contact a company regarding one piece of content, but both disagree on what action is required (taking it down, restricting access or keeping it up) what is the company expected to do? What are the implications regarding the liability of the company for taking the correct action within the very short turn-around time?

- **Question:** What happens if in their transposition of article 6 ask companies to put in place different, incompatible, or conflicting proactive measures? Does each company have to develop different technological solution for each country? This would of course lead to fragmentation of the DSM and the Internet at large?

EDiMA

Fundamental rights and data protection

- **Question:** What does it mean to inform law enforcement of terrorist offences? Does are companies being asked to disclose personal information about someone posting a piece of content, if doubt exists, without following due legal process?

- **Question:** How does this proposal square with the e-evidence proposal, which places a higher threshold on disclosure?

- **Question:** What happens if Member States disagree on whether a particular group is a terrorist organization and therefore ask companies to take a different position/action regarding content originating from this source?

- **Question:** What happens if we are referred content from a group that is registered in a Member State as a political party?

- **Question:** How should we react if we are forced to prevent the reuploading of each piece of terrorist content removed? Does it mean that we have to automatically take down all the news content, or academic or activists posts that use that content to debunk it.

A need for more flexibility to accommodate existing solutions

- Article 14 on points of contact as it stands is restrictive and nonpractical as it would force platforms to significantly adjust their systems to be compatible with the proposal[1].
- **Question:** How does the proposal take into account current best practices which required considerable stakeholder investment and engagement to get off the ground e.g. some HSPs allow police officers and agencies to register and submit data requests through their system, which saves time and provides for a much more efficient way of dealing with individual requests?

The importance of encouraging industry initiatives to support the whole ecosystem

- As Professor Maura Conway has found, the significant disruption of IS Twitter activity has further pushed the group to other platforms. Many of these services are operated by smaller companies, who do not have the resources to deploy the sort of technology Twitter is able to leverage.
  Since the beginning of 2018, Twitter has worked with several companies to pilot a process whereby when Twitter identifies a URL being shared by accounts that are removed for the promotion of terrorism, the company operating the service being linked to is made aware of the content on their service. By actioning unique URLs of source material, this means that any link across any platform will no longer produce content. For example, where one terrorist manual is removed by a file hosting service, every link to that manual anywhere on the internet will no longer work. As such, the impact of this project could be substantial. Twitter has been expanding this project to include more companies, helping more companies to deal with both existing content and new content going forward.
  Question: How will the proposal make it possible to stay on top of shifting content from one platform to another and how will it support smaller actors to comply?

[1] The current wording of article 14 (Points of Contact) would require Hosting service providers to establish a point of contact for receipt of removal orders and referrals by electronic means. This would mean that platforms would have to set up an email address where authorities would refer their removal orders.