EURACTIV

REGULATING AGAINST RADICALISATION

EVENT REPORT | FEB.-MAR. 2019
http://eurac.tv/9Q2a

With the support of

CISPE.cloud

EURACTIV

REGULATING AGAINST RADICALISATION

EVENT REPORT | FEB.-MAR. 2019
http://eurac.tv/9Q2a

In a period tarnished by terrorist attacks across the continent, the EU is seeking to clamp down on the dissemination of terrorist content online, which is often seen as an effective method of radicalisation.

The regulation on preventing the dissemination of terrorist content online was presented by the Commission towards the end of 2018, as a means to oblige hosting services to detect, identify and remove terrorist content, without encroaching on fundamental rights, such as freedom of expression and information.

The legislation is seen as a legacy-maker for the outgoing Security Chief Sir Julian King, and there are many who would like to see talks tied up in Parliament as soon as possible, following the Council's adoption of their negotiating position in December.

However, a number of challenges lie ahead.

This special report, published ahead of a high-level event hosted by the rapporteur for the legislation, MEP Daniel Dalton, looks into some of the finer details of the measures that have come under scrutiny. Such include the length of the time-limited order, the scope of the regulation, and whether the restrictions could ever lead to a censorship of the web.

Contents

Up to 400 online platforms hosting terrorist content, Commission says

By Samuel Stolton | EURACTIV.com

Iraqi soldiers display a flag belonging to the Islamic State (IS) as they take up position on the roof of a house in the formerly IS held district of Muthana in eastern Mosul, northern Iraq on 08 January 2017. [EPA/AHMED JALIL]

Between 200 and 400 online platforms are currently hosting content that could lead to terrorist radicalisation, the European Commission has said.

Speaking at a Brussels event on Wednesday (6 March), Hans Das, head of unit for terrorism and radicalisation in the Commission's DG Home, said that while terrorist content has traditionally been disseminated across larger platforms, it is now being spread more widely over lesser-known sites.

The event, hosted by the Cloud Infrastructure Service Providers trade association, CISPE, took place as European Parliament regulators debate the finer details of the Commission's plans to regulate against the appearance of online terrorist content.

Das described as 'essential to the plans' the notion of obliging platforms to enact proactive measures as a means to ensure that previously removed content does not reappear online.

"There is so much terrorism propaganda online that is being recycled so quickly… It would be totally irrational to put the burden of proof on law enforcement agencies and the courts," he said.

"Do we really want our police authorities to be spending their time chasing up each and every version of a video that comes online and then issuing removal orders to companies?"

"Companies need to take responsibility in this area. There are a number of technological solutions already developed," Das added.

Dr Hany Farid, a senior adviser for Counter Extremism Project (CEP), recently told EURACTIV that most platforms were unwilling to assume their civic responsibilities, which could soon backfire for them.

Continued on Page 5

Continued from Page 4

Farid is a world-leading authority on computer forensics and developer of a hashing software capable of identifying and quickly removing violent images, video, and audio content online, the eGLYPH technology.

"We are at where we are today because of the sheer unwillingness of the platforms to cooperate with wider social concerns," he said.

"The scale of extremist content online is phenomenal."

Farid said he would not be surprised if the platforms' failure to counter the spread of terrorist content started to hit their revenues.

"Advertisers are going to start to turn away," he said. "They won't want to be associated with businesses that allow the dissemination of such offensive material."

Meanwhile, the Romanian Presidency of the EU believes that young people are the most at risk of radicalisation.

Speaking on Wednesday, Mihai Niţoi of the Romanian Presidency said that "no one is safe from the threat [of online terrorist content]," and that the priority of the Council was always to "diminish the availability" of material that would fall under the scope of the regulation, especially for young people, who, he said, are being specifically targeted.

However, there are some who feel that the measures on the table are misaligned.

Jens-Henrik Jeppesen of the Centre for Democracy and Technology (CDT) said on Wednesday that "many free expression groups have issues" with how the referral procedure for content that breaches the regulation would take place under the new plans, fearing that legitimate political debate may become stifled in the cause of restricting online material.

The European Parliament's rapporteur for the file, ECR MEP Daniel Dalton, said that on the scope of the plans, "there is an issue of whether cloud infrastructure services should be included or not."

"My opinion is that there is a distinction between consumer cloud services, like Dropbox, and cloud infrastructure services," he added.

The Secretary-General of CISPE, Francisco Mingorance, rallied for this issue, saying that the regulation, as it stands, "targets the wrong player" in not providing a specific legal carve-out for cloud infrastructure service providers.

"Our industry provides the underlying foundation for businesses to manage their data and build their own systems," he said.

"We have no foresight or supervision over the nature of the content that is eventually delivered to the public. We are not responsible for putting the content in front of people."

Moreover, Mingorance suggested that there may be issues surrounding data protection if cloud infrastructure services came under the scope of the plans, as such firms "would have to access the content in order to read it and understand whether it comes under the definition as of terrorist content."

EURACTIV pressed the European Commission's Hans Das as to why such services were not given an exclusion clause from the outset.

"Our strategy from the beginning was to cover all the relevant services in the fight against online terrorist content, he said"

"However, I believe that the wording of the text could be further refined for clarity. We do need clearer definitions on the scope," Das added.

Mingorance chimed in after hearing the Commission's response.

"Our industry is a relatively new sector," he said. "In my experience, there are difficulties with understanding the specificities of cloud service infrastructure providers and our competences."

INTERVIEW

‘Small platforms’ are the target of online terrorist content regulation, MEP says

By Samuel Stolton | EURACTIV.com

The EU is taking regulatory measures to clamp down on the dissemination of terrorist content online. In the European Parliament, the file is being dealt with by the Civil Liberties Committee, with MEP Daniel Dalton leading the report. EURACTIV sat down with Dalton to discuss the finer details of the plans.

Daniel Dalton is a British MEP for the European Conservatives and Reformists (ECR). He spoke to EURACTIV’s Samuel Stolton.

How do you define online terrorist content?

We have to be very careful here because there are things that are clearly terrorist content and content that is political expression. So to me, we’ve already got the definition. And that’s the one contained within the 2017 terrorism directive.

However, the challenge here is that the directive doesn’t define what content is, it defines what terrorism

Continued on Page 7

Continued from Page 6

is, with reference to "seriously intimidating a population, unduly compelling a government or an international organization to perform or abstain from performing any act, or seriously destabilizing or destroying the fundamental political structure of a country…"

I think that these are good pointers for how we should define online terrorist content.

Why is this content regarded as particularly dangerous?

Many people who are at risk of radicalization are being targeted online. Whether it's watching videos or learning about certain parts of an ideology that has eventually led to terrorist acts, most of this happens online.

At the same time, there are practical problems, when you have things such as bomb-making guides, for example, that are available on the web.

There are many reasons why this content should be regarded as dangerous, but the most important one is the fact that these types of content clearly does play a role in radicalization.

How do you respond to those who fear this regulation could result in a form of censorship?

Well, of course, there is the worry that legitimate free speech may get caught up in this, which is a worry I share and we will certainly be looking to make sure that we can tighten the regulation up to be certain that this doesn't happen.

On top of that, we are facing similar issues as to those faced in the Copyright debate, such as things like upload filters and content monitoring.

How much faith do you have in the platforms dealing with this content themselves, without the need for regulation?

It's clear that the platforms are not doing enough. There's lots of content out there that shouldn't be out there. And it's not only the political institutions that recognize the need for something to be done. If you talk to most people outside of the Brussels bubble, they would say that platforms have a huge responsibility to make sure that terrorist content is taken down.

Now, from what I understand, it's not necessarily the big platforms that have the problem. Many of them are doing their own voluntary and proactive measures as it is now. But there are quite a few smaller platforms who are either inundated with offending content, or they are basically not responding to the authorities' requests for the removal of content.

So I think it's fair enough for the commission to set out a framework which allows the content authorities to have more teeth when they're trying to liaise with these platforms and take down content, which shouldn't be on there.

And how small are these platforms that we're talking about here?

Very small outfits, we're talking about one or two man bands. Websites that most people have probably not heard of, but are hosting a huge amount of terrorist content. These sites are the target of the regulation.

This is also why the amendment was made on the 'proactive measures' point, which, in the Commission's original proposal, called for hosting service providers to take steps to protect their services against the dissemination of online terrorist content.

My take on this issue is a little different: I think that we should focus on voluntary measures and the interaction between competent authorities and platforms. We should be honing in on the platforms that consistently fail to comply and that have no voluntary measures in place of their own.

In terms of the moderation of online terrorist content, isn't there the risk that individuals employed in roles that require the reviewing of content could be affected by engaging with gratuitous and graphic content for hours daily?

I guess the inference you're making here is that potentially people who are moderating the content themselves could be radicalised.

Frankly, I don't know how we solve that. The fact that the content exists in the first place, means that it is liable to radicalize, potentially, anyone who comes into contact with it.

Arguably, if one person is looking at it, to take it offline and ensure that millions of people don't look at it, well that's clearly a good thing. Which is justification for doing something about it in the first place.

The Commission's proposal calls for offending content to be removed within "one hour from receiving the removal order." Your amendment includes an adage to this point: "depending on the size and means of the hosting service provider." Do you think this one-hour time order is achievable?

I'll be tabling some more amendments on this issue, because I don't think my position was quite right, at that moment.

The aim I have is that the one hour should come at the end of the process. i.e. that you've had a referral in the first place, and the competent authority has then contacted the platform, they've had a discussion, and the platform is refusing to comply. Only at that stage, in my opinion, should the one-hour

Continued on Page 8

Continued from Page 7

order come in.

In terms of the 'size' of the hosting provider – that amendment is included to cover one-man outfits who cannot practically respond to such orders within such a short timeframe.

But in this case, an item of terrorist content may have been online for two or three weeks before the order is issued. If the objective of this regulation is to remove online terrorist content as swiftly as possible, don't you think any time-limited order should be from the moment that the content is uploaded?

Well, that may require technologies such as upload filters, which I am completely against. For me, the one hour is more an enforcement tool for the authorities, rather than justification for saying content such as this should only be online for one hour.

This is about giving the competent authorities the teeth to go after platforms that are not living up to their responsibilities.

Moving on to another amendment that has been made to the Commission's original text, what's your take on the scope of the restrictions? In the draft report, you say that the regulation should only cover terrorist content that has been available to 'the public' and not 'third parties.'

To me, the moral obligations should be on the platform disseminating the information to the public, not on an infrastructure service that might be hosting the content.

Ultimately, it's the platform that is taking the editorial decision to put up that material to people or to leave the offending content online.

The whole objective of the legislation, that you're trying to allow platforms to live up to their moral responsibility to keep terrorist content offline is compromised by the fact that businesses that don't put terrorist content up, but who only host it for someone else, could be targeted. This is a moral hazard issue, why are you going after the people who are not actually responsible for disseminating the content?

Moreover, from what I understand, it's virtually impossible for cloud infrastructure service providers to identify individual pieces of content that may violate any restrictions.

How badly would cloud service infrastructure providers be affected should they be included in the scope?

Well, as I understand it, because it's technically impossible for them to identify specific pieces of content, they may be required to shut down entire websites. This would lead to making the business model for cloud service infrastructure providers unfeasible. Customers may turn away.

Was it an oversight, then, that the Commission included cloud infrastructure service providers in the original scope?

Possibly. The Commission said in Committee that they didn't mean to include those types of cloud infrastructure services. I suspect they were thinking more about consumer cloud services, like Dropbox, for example, who I think should be covered. Others may not agree with me on this point, because material within Dropbox is only disseminated to private groups. But you can have a private group with 10,000 members, which is more Twitter followers than I have.

So for me, consumer cloud services should be included, but cloud hosting services shouldn't. This is a distinction that we've tried to make in the draft report.

PROMOTED CONTENT / OPINION

DISCLAIMER: All opinions in this column reflect the views of the author(s), not of EURACTIV.COM Ltd.

Terrorist legislation: the EU is on the right track but isn't there yet

By Alban Schmutz - CISPE Chairman and Vice President Strategic Development and Public Affairs at OVH

"New EU terr laws: almost there?"

Last autumn, the European Commission's proposed Regulation to remove and proactively monitor terrorist content online sent shockwaves through Europe's cloud infrastructure community. Alban Schmutz explains why.

Alban Schmutz is CISPE Chairman and Vice President Strategic Development and Public Affairs at OVH.

When the Commission announced its proposed Regulation on Preventing the dissemination of terrorist content online, one thing was immediately clear: it was targeting the wrong players.

It made no sense to include cloud infrastructure in its scope. Since then, real progress has been made in tightening the wording and scope of the Regulation to ensure it can work as effectively as possible—but more remains to be done, and the clock is ticking.

It is technically impossible for Europe's cloud infrastructure companies to comply, yet they were covered. Cloud infrastructure services are used for other companies to build and run their business on top of it. As we made crystal clear last year, it is not possible for cloud infrastructure

Continued on Page 10

Continued from Page 9

providers to take down a specific piece of content without compromising lawful content and interfering with their customers' private data.

The legislation is mainly designed for social media platforms and online content sharing services but, unintentionally, captures other hosting service providers.

The organizations represented by CISPE (Cloud Infrastructure Services Providers in Europe) take care of the underlying infrastructure and not the content. We do not remove specific content, we are the processors not the controllers. It's not what we do.

So while our members do, of course, support the aim of the Regulation, and recognize this is a highly sensitive issue, we believe that cloud infrastructure should not fall under its scope. In addition, issues remain around security, data privacy and fundamental rights related, for example, to filtering obligations. Some provisions are at odds with the e-Commerce Directive.

SINCE LAST DECEMBER, HOWEVER, WE'VE SEEN ENCOURAGING MOVEMENT IN THE RIGHT DIRECTION.

For example, the draft report from the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) recognized that cloud infrastructure services should not be within the scope of the Regulation, as this may lead to a conflict with principles of privacy and undermine the provision on cloud infrastructure services.

As rapporteur Daniel Dalton MEP said in a LIBE committee meeting (04/02/2019), "I don't think that cloud infrastructure services should be included… I'm not talking here about consumer cloud services such as Dropbox, but more the cloud infrastructure services that are used by businesses to host data that's used on websites. They don't control or filter the data, and they have no technical means of removing specific content."

The IMCO committee (Internal Market and Consumer Protection) elaborated on the exclusion: services at other layers of the Internet infrastructure than the application layer (meaning to address cloud infrastructure services).

Meanwhile, the CULT committee (Culture and Education) clarified the definition of hosting service providers to exclusively cover hosting providers that enable their users to make content available to the public instead of 'third parties'—which we believe is helpful.

SO PROGRESS HAS BEEN MADE. WE'RE ALMOST THERE BUT IT'S NOT QUITE ENOUGH. KEY CLARIFICATIONS AND IMPROVEMENTS ARE STILL REQUIRED TO MAKE THE REGULATION AS CLEAR AND UNAMBIGUOUS AS IT NEEDS TO BE.

As a result, we are calling on MEPs to introduce a properly robust definition of cloud infrastructure in Article 2 of the Regulation and explicitly exclude such services.

Ensuring exclusion within Article 2 of the Regulation will provide consistency across member states in their interpretation of cloud infrastructure services and so avoid loopholes.

It would prevent a situation in which different interpretations co-exist across the EU, with the risk of 28 or more national competent authorities misstepping into imposing automated proactive measures on cloud infrastructure services—or even companies claiming to have cloud infrastructure services when they do not.

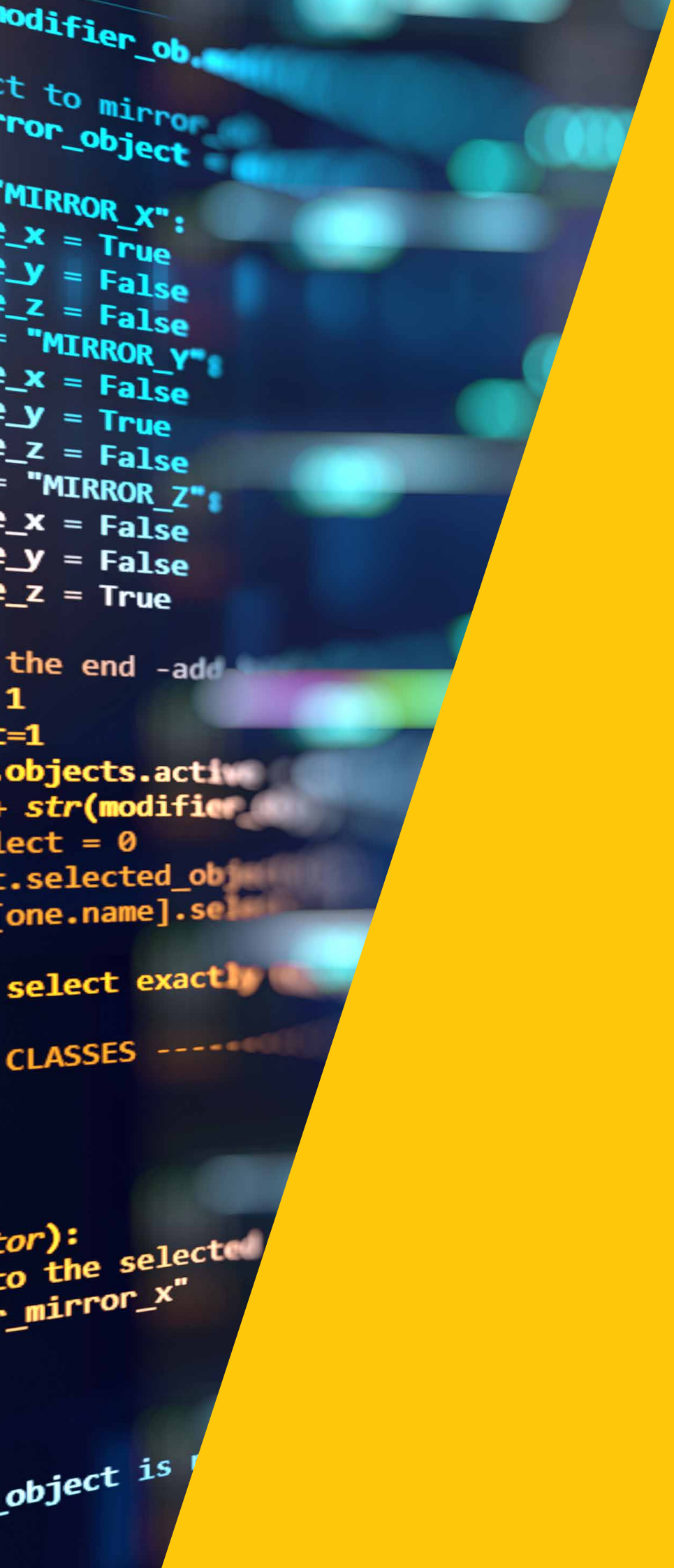
WE URGE LEGISLATORS TO TAKE THOSE LAST FEW IMPORTANT STEPS: TO EMBED THE NECESSARY EXCLUSIONS IN A LEGALLY BINDING ARTICLE RATHER THAN IN A NON-BINDING RECITAL, AND SO MAKE THIS REGULATION FIT FOR PURPOSE.

CISPE's original press release on the proposed EU Regulation on Terrorist Content Online is available here

The CISPE position paper on the proposed EU Regulation on Terrorist Content Online is available here

ABOUT CISPE

CISPE is the leading European trade association representing cloud infrastructure providers, supported by a majority of European SMEs and small-cap companies, working with business, consumers and EU institutions to address key industry issues and promote best practice in cloud provision, data protection and consumer choice. With more than 100 cloud services already declared under the CISPE GDPR Code of Conduct, its 30+ members provide services to many thousands of organizations and for millions of customers across the region. CISPE is open to all companies provided they declare at least one service under the CISPE Code of Conduct. Please get in touch – cispe.cloud



For information on
EURACTIV *Event Reports...*

Contact us

Davide Patteri
Public Affairs Senior Manager
davide.patteri@euractiv.com
tel. +32 (0)2 788 36 74

Samuel Stolton
Digital Affairs Editor
samuel.stolton@euractiv.com
tel. +32 (0)2 226 58 26