Council of the European Union
General Secretariat

Interinstitutional files:
2018/0331(COD)

Brussels, 25 February 2020

WK 1935/2020 INIT

LIMITE

CT
ENFOPOL
COTER
JAI

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a Regulation on preventing the dissemination of terrorist content online - comments by Member States

Delegations will find in Annex comments by Member States on the above mentioned proposal which were received in February 2020.

TABLE OF CONTENTS

Article XX

Specific measures

[Merging of Articles 3, 6 and 9]

1. Hosting service providers shall include in their terms and conditions, and apply, provisions to address the misuse of their service for the dissemination of terrorist content online.

2. Where a hosting service provider is exposed to terrorist content, it shall take specific measures to protect their services against the dissemination of terrorist content.

   Those measures may include, in particular, one or more of the following:

   (a) easily accessible and user-friendly mechanisms for users to report or flag to the hosting service provider alleged terrorist content;

   (b) mechanisms to detect, identify and expeditiously remove or disable access to content that is considered terrorist content;

   (c) mechanisms addressing the reappearance of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content.

3. Any specific measure or measures that a hosting service provider takes pursuant to paragraph 2 shall meet all of the following requirements:

   (a) they shall be effective in mitigating and managing the level of exposure to terrorist content;

   (b) they shall be targeted and proportionate, taking into account, in particular, the seriousness of the level of exposure to terrorist content as well as the financial strength of the hosting service provider;

   (c) they shall be applied taking full account of the rights and legitimate interest of the users, in particular users' fundamental rights to freedom of expression and of information, to respect for private life and to protection of personal data;

   (d) they shall be applied in a diligent and non-discriminatory manner;

   (e) where they involve the use of automated tools, appropriate safeguards shall be provided to ensure accuracy and to avoid the removal of information that is not terrorist content, in particular through human oversight and verification.

4. For the purposes of paragraph 2, a hosting service provider shall be considered to be exposed to terrorist content, where the competent authority of the Member State of its main establishment has informed the hosting service provider, through a decision based on objective factors, such as the hosting service provider having received two or more removal orders in any given 12 month period, that it considers the hosting service provider to be exposed to terrorist content.

Commented [h1]: Will there be a similar reference as provided in Art. 18.1 (a), previously referring to Art. 3 (2)?

Commented [h2]: Problematic for AT linked to Para 4

Commented [h3]: AT suggests to change "may" to "shall" (or to another term expressing a stricter obligation for the HSP)

Commented [h4]:
AT sees the new provision in connection with Para 2 critical. The new provision shifts the responsibility rather on the authority instead of the HSP. Furthermore, the threshold of having received two removal orders is quite high. Para 2 shall not be linked to a threshold at all or at least not to such a high threshold.
(a personal proposal how to work further could be to introduce a further clarification/specification of objective factors (receipt of a certain number of referrals, according to a threat assessment, ...))

5. After having received the decision referred to in paragraph 4 and, where relevant, paragraph 6 a hosting service provider shall report to the competent authority on the specific measures it has taken and that it intends to take in order to comply with the requirement of paragraph 2 and 3. It shall do so within three months of receipt of the decision and thereafter on an annual basis.

6. Where, based on the reports referred to in paragraph 5 and, where relevant, any other objective factors, the competent authority considers that the measures that a hosting provider has taken do not meet the requirements of paragraphs 2 and 3, the competent authority shall address a decision to the hosting service provider requiring it to adjust those measures or to take certain additional measures so as to ensure that those requirements are met.

7. A hosting service provider may, at any time, request the competent authority to review and, where appropriate, adjust or revoke the decisions referred to in paragraphs 4 and 6. The competent authority shall, within a reasonable time period after receiving the request, take a reasoned decision based on objective factors on the request and inform the hosting service provider accordingly.

8. Any requirement to take measures pursuant to this Article shall not entail a general obligation on hosting services providers to monitor the information which they store, nor a general obligation to actively seek facts or circumstances indicating illegal activity.

Compromise proposal on "public"

Art. 1

Para. 1:

This Regulation lays down uniform rules to prevent the misuse of hosting services for the dissemination **to the public** of terrorist content online. It lays down in particular [etc.]

Commented [h1]: Similar to IT we wonder whether "to the public" is needed in this context

Para. 2:

This Regulation shall apply to hosting service providers offering services in the Union, irrespective of their place of main establishment, **which disseminate information to the public.**

Commented [h2]: Similar to IT we wonder whether "to the public" is needed in this context

Art. 2

Para. 1:

'hosting service provider' means a provider of information society services consisting of the storage of information provided by and at the request of the content provider [***rest deleted***]

Para. 6:

'dissemination to the public' means the making available of information, at the request of the content provider, to a potentially unlimited number of persons.

Recitals

(10) In order to effectively tackle terrorist content online, while ensuring respect for the private life of individuals, this Regulation should apply to providers of information society services which store and disseminate to the public information provided by a recipient of the service at his or her request, irrespective of whether this activity is of a mere technical, automatic and passive nature. The concept of "storage" should be understood as holding data in the memory of a physical or virtual server. Providers of "mere conduit" or "caching" services as well as of other services provided in other layers of the internet infrastructure, which do not involve such storage, such as registries and registrars as well as providers of domain name systems (DNS), payment or distributed denial of service (DdoS) protection services therefore fall outside the scope of this Regulation.

(10a) The concept of "dissemination to the public" should entail the making available of information to a potentially unlimited number of legal or natural persons that is, making

the information easily accessible to users in general without further action by the content provider being required, irrespective of whether those persons actually access the information in question. Accordingly, the mere possibility to create groups of users of a given service does not, in itself, mean that this Regulation does not apply. However, the Regulation does not apply to closed groups consisting of a finite number of pre-determined persons. Interpersonal communication services, as defined in *[the Telecommunications Code (Dir. 2018/1972)]* such as emails or private messaging services, fall outside the scope of this Regulation. Information should be considered stored and disseminated to the public within the meaning of this Regulation only where such activities are performed upon direct request by the content provider. Consequently, providers of services such as cloud infrastructure, which are provided at the request of other parties than the content providers and only indirectly benefit the latter, should not be covered by this Regulation. By way of example, included in the scope of this Regulation are providers of social media, video, image and audio-sharing, as well as file-sharing and other cloud services, in as far as those services are used to make the stored information available to the public at the direct request of the content provider. Where a service provider offers several services, some of which fall within the scope of this Regulation, this Regulation should be applied only in respect of the services that fall within its scope.

(10b) Terrorist content is often disseminated to the public through services provided by service providers established in third countries. In order to protect users in the Union and to ensure that all service providers operating in the Digital Single Market are subject to the same requirements, this Regulation should apply to all providers of relevant services offered in the Union, irrespective of their country of main establishment. The determination as to whether a service provider offers services in the Union requires an assessment whether it enables legal or natural persons in one or more Member States to use its services and has a substantial connection to that Member State or Member States, in particular an establishment that is relevant to the provision of those services or, in the absence thereof, other specific factual criteria pointing to such a substantial connection. However, the mere accessibility of a service provider's website or of an email address or of other contact details in one or more Member States, taken in isolation, should not be a sufficient condition for the application of this Regulation.

From: Dimana DOYNOVA <dimana.doynova@bg-permrep.eu>

Sent: Monday, February 17, 2020 4:43 PM

To: Marijan.Jelinek@mvep.hr; kmamic@mup.hr; [DL] JAI TWG <twg@consilium.europa.eu>

Cc: imaleksandrov.14@mvr.bg

Subject: BG comments - TCO

Dear Colleagues,

Following the discussions at our last JHA Counsellors meeting on 13 February, please find below the comments I received from Sofia, which concern the new merged article on specific measures:

- In para 4 we prefer to delete the requirement for the competent authority to issue a decision. Instead, we think, it would be better to strengthen the objective factors. If there are clear objective criteria that define when a hosting service provider is exposed to terrorist content, a decision issued by the competent authorities will not be necessary - providers will be automatically obliged by the Regulation to take the respective specific measures. An objective factor for us, for example, could be if the HSP has received 3 or more removal orders in the last 12 months.

- In para 7 we support the proposal *"within a reasonable time period"* to be replaced with *"within a month"* or even better *"within 40 days"*.

For the rest of the proposals discussed at the meeting last week, we could be flexible.

Best regards,

Dimana

Dimana Doynova

JHA Counsellor

Permanent Representation of the Republic of Bulgaria to the EU

Square Marie-Louise 49, Brussels 1000

Phone: +322 230 9422

GSM: +32475634039

Compromise proposal on "public" CZ comments

Art. 1

Para. 1:

This Regulation lays down uniform rules to ~~prevent~~ address the misuse of hosting services for the dissemination **to the public** of terrorist content online. It lays down in particular [etc.]

Commented [HPM1]: to respect already agreed text

Para. 2:

This Regulation shall apply to hosting service providers offering services in the Union, irrespective of their place of main establishment, **which disseminate information to the public**.

Art. 2

Para. 1:

'hosting service provider' means a provider of information society services consisting of the storage of information provided by and at the request of the content provider **[*rest deleted*]**

Para. 6:

'dissemination to the public' means the making available of information, at the request of the content provider, to a potentially unlimited number of persons.

Recitals

(10) In order to effectively tackle terrorist content online, while ensuring respect for the private life of individuals, this Regulation should apply to providers of information society services which store and disseminate to the public information provided by a recipient of the service at his or her request, irrespective of whether this activity is of a mere technical, automatic and passive nature. The concept of "storage" should be understood as holding data in the memory of a physical or virtual server. Providers of "mere conduit" or "caching" services as well as of other services provided in other layers of the internet infrastructure, which do not involve such storage, such as registries and registrars as well as providers of domain name systems (DNS), payment or distributed denial of service (DdoS) protection services therefore fall outside the scope of this Regulation.

Commented [HPM2]: Concrete elaboration on criteria relevant for including or excluding various types of providers of information society services should be added, as it is necessary for better orientation of both industry and officials in practice

(10a) The concept of "dissemination to the public" should entail the making available of information to a potentially unlimited number of legal or natural persons that is, making the information easily accessible to users in general without further action by the content

provider being required, irrespective of whether those persons actually access the information in question. Accordingly, the mere possibility to create groups of users of a given service does not, in itself, mean that this Regulation does not apply. However, the Regulation does not apply to closed groups consisting of a finite number of pre-determined persons. Interpersonal communication services, as defined in *[the Telecommunications Code (Dir. 2018/1972)]* such as emails or private messaging services, fall outside the scope of this Regulation. Information should be considered stored and disseminated to the public within the meaning of this Regulation only where such activities are performed upon direct request by the content provider. Consequently, providers of services such as cloud infrastructure, which are provided at the request of other parties than the content providers and only indirectly benefit the latter, should not be covered by this Regulation. By way of example, included in the scope of this Regulation are providers of social media, video, image and audio-sharing, as well as file-sharing and other cloud services, in as far as those services are used to make the stored information available to the public at the direct request of the content provider. Where a service provider offers several services, some of which fall within the scope of this Regulation, this Regulation should be applied only in respect of the services that fall within its scope.

(10b) Terrorist content is often disseminated to the public through services provided by service providers established in third countries. In order to protect users in the Union and to ensure that all service providers operating in the Digital Single Market are subject to the same requirements, this Regulation should apply to all providers of relevant services offered in the Union, irrespective of their country of main establishment. The determination as to whether a service provider offers services in the Union requires an assessment whether it enables legal or natural persons in one or more Member States to use its services and has a substantial connection to that Member State or Member States, in particular an establishment that is relevant to the provision of those services or, in the absence thereof, other specific factual criteria pointing to such a substantial connection. However, the mere accessibility of a service provider's website or of an email address or of other contact details in one or more Member States, taken in isolation, should not be a sufficient condition for the application of this Regulation.

Commission suggestion for compromise text on Article 8a

CZ comments

2) Article 8a

Article 8a
Transparency obligations for competent authorities

1. Competent authorities shall publish annual transparency reports relating to their activities under this Regulation. Those reports shall include at least the following information in relation to the year covered:
(a) the total number of removal orders issued in accordance with Article 4 and the number of instances in which the removal orders led to the removal of or disabling of access to terrorist content and the number of instances in which they did not;
(b) the total number of referrals issued in accordance with Article 5 and number of instances in which the referrals led to the removal of or disabling of access to terrorist content and the number of instances in which they did not;
(c) the total number of decisions imposing [proactive/specific] measures taken in accordance with Article 6(4) and a description of categories/types of the measures imposed;
(d) the total number of instances in which removal orders and decisions imposing [proactive/specific] measures were subject to administrative or judicial remedies and information on the final outcome of the relevant proceedings.
(e) The total number of final decisions imposing penalties, including a description of the type of penalty imposed.

2. The transparency reports referred to in paragraph 1 shall not contain information that may affect ongoing activities for the prevention, detection investigation or prosecution of terrorist offences or national security interests.

Commented [HPM1]: similar to (2), no elaborations on specific measures applied to particular HSP

Commented [HPM2]: i.e. where no regular remedies (appeals) are possible. Such cases appear in the statistics just once.

Comments CZ:

Article XX

Specific measures

[Merging of Articles 3, 6 and 9]

1. Hosting service providers shall include in their terms and conditions, and apply, provisions to address the misuse of their service for the dissemination of terrorist content online.

2. Where a hosting service provider is exposed to terrorist content, it shall take specific measures to protect their services against the dissemination of terrorist content.

   Those measures may include, in particular, one or more of the following:

   (a) easily accessible and user-friendly mechanisms for users to report or flag to the hosting service provider alleged terrorist content;

   (b) mechanisms to detect, identify and expeditiously remove or disable access to content that is considered terrorist content;

   (c) mechanisms addressing the reappearance of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content.

3. Any specific measure or measures that a hosting service provider takes pursuant to paragraph 2 shall meet all of the following requirements:

   (a) they shall be effective in sufficiently mitigating ~~and managing~~ the level of exposure to terrorist content;

   (b) they shall be targeted and proportionate, taking into account, in particular, the impact of the service, the seriousness of the level of exposure to terrorist content as well as the financial strength of the hosting service provider;

   (c) they shall be applied taking full account of the rights and legitimate interest of the users, in particular users' fundamental rights to freedom of expression and of information, to respect for private life and to protection of personal data;

   (d) they shall be applied in a diligent and non-discriminatory manner;

   (e) where they involve the use of automated tools, appropriate safeguards shall be provided to ensure accuracy and to avoid the removal of information that is not terrorist content, in particular through human oversight and verification.

4. For the purposes of paragraph 2, a hosting service provider shall be considered to be exposed to terrorist content, where the competent authority of the Member State of its main establishment has informed the hosting service provider, through a decision based on objective factors, such as the hosting service provider having received ~~two or more~~ several removal orders in any given ~~12-month period~~ calendar year, that it considers the hosting service provider to be exposed to terrorist content.

Commented [HPM1]: Could give the wrong idea that certain non-zero level of incidence of terrorist content is positive.

Commented [HPM2]: Global services have obviously more potential for misuse and misuse causes more damage.

Commented [HPM3]: "capabilities and resources" would be more general and still appropriate, since some HSPs (NGOs etc.) may have personnel available to moderate platforms but no resources to buy some software or IT expertise to develop or implement new solutions.

Commented [HPM4]: CZ strongly welcomes that automated filters are not imposed but are available (CZ Constitution prohibits ex ante censorship)

Commented [HPM5]: This should really be part of risk assessment (impact and number of removal orders/referrals) and not a simple number. Would lead to proportionality issues

Commented [HPM6]: Focus on removal orders gives the HSPs reason to sue competent authorities for sending removal orders instead of referrals and courts likely will require a) objective differences or b) referrals first

Commented [HPM7]: This makes the regulation less burdensome, more predictable both for HSPs and competent authorities and simplifies compliance.

5. After having received the decision referred to in paragraph 4 and, where relevant, paragraph 6 a hosting service provider shall report to the competent authority on the specific measures it has taken and that it intends to take in order to comply with the requirement of paragraph 2 and 3. It shall do so within three months of receipt of the decision and thereafter on an annual basis.

6. Where, based on the reports referred to in paragraph 5 and, where relevant, any other objective factors, the competent authority considers that the measures that a hosting provider has taken do not meet the requirements of paragraphs 2 and 3, the competent authority shall address a decision to the hosting service provider requiring it to adjust those measures or to take certain additional measures so as to ensure that those requirements are met.

7. A hosting service provider may, at any time, request the competent authority to review and, where appropriate, adjust or revoke the decisions referred to in paragraphs 4 and 6. The competent authority shall, within a reasonable time period after receiving the request, take a reasoned decision based on objective factors on the request and inform the hosting service provider accordingly.

8. Any requirement to take measures pursuant to this Article shall not entail a general obligation on hosting services providers to monitor the information which they store, nor a general obligation to actively seek facts or circumstances indicating illegal activity.

Commented [HPM8]: Direct link to e-commerce directive should be added

Article 2
Definitions

For the purposes of this Regulation, the following definitions shall apply:
(1) 'hosting service provider' means 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; **as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[1], which is of a type listed below**

(a) **social network means an information society service that allows to the registred members to create a profile, share information, data and communicate;**

(b) **cloud computing service means an information society service that enables access to a scalable and elastic pool of shareable computing resources;**

(c) **online marketplace means an information society service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council[2] to conclude online sales or service contracts with traders either on the online marketplaces website or on a trader's website that uses computing services provided by the online marketplace;**

This adjustment should also apply to the recital 10.

Rationale

The Czech Republic proposes the definition of the definition in Article 2 (1) to the specific types of the hosting service providers indicated in rec. 10 of the draft regulation, it does not seem desirable to impose on all service providers an obligation to cover only a few specific types of hosting service providers.

[1] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

[2] Directive 2013/11/EU of the European Parliament and of the Council of 21 May on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/ES (Directive on consumer ADR) (OJ L 165, 16.6.2013, p. 63).

From: JAI INTERNAL SECURITY
To: ADSERBALLE Anne Cecilie
Subject: FW: TCO - proposals for the JHA-Counsellors meeting on Friday 31 January
Date: mercredi 5 février 2020 09:49:43
Attachments: image001.png

Email received to Internal Security mailbox (below)

From: Martin Bank Nutzhorn Villaume
Sent: Wednesday, February 5, 2020 9:29 AM
To: JAI INTERNAL SECURITY
Cc: Marijan.Jelinek@mvep.hr
Subject: SV: TCO - proposals for the JHA-Counsellors meeting on Friday 31 January

Dear all,
DK acknowledges and appreciates the Presidency's efforts to reach a compromise with the EP on the TCO-proposal.
DK can be flexible with regard to the Commission's draft compromise proposals on Article 1 and Article 2, the suggested Article on specific measures and Article 8a.
Furthermore, DK supports the Presidency's decision to ask the EP to draft a compromise proposal regarding the cross-border effect of removal orders. DK will be happy to assist in finding a suitable solution to this very important issue.
Best,
Martin

MARTIN BANK NUTZHORN VILLAUME / MABAJE@UM.DK
COUNSELLOR / JUSTICE AND HOME AFFAIRS
DIRECT (+32) (0) 2 233 08 11 / MOBILE (+32) (0) 497 05 84 33
PERMANENT REPRESENTATION OF DENMARK TO THE EU
RUE D'ARLON 73 / B-1040 BRUSSELS
PHONE (+32) (0) 2 233 08 11 / EU.UM.DK
HOW WE PROCESS PERSONAL INFORMATION

Please consider the environment before printing this message

Fra: JAI INTERNAL SECURITY <jai.internal.security@consilium.europa.eu>
Sendt: 31. januar 2020 10:17
Emne: TCO - proposals for the JHA-Counsellors meeting on Friday 31 January

Dear all,
On behalf of the Presidency, and with a view to the JHA-Counsellors' meeting on Friday (and the technical meeting with the EP on Monday 3 February), please find attached three proposals form the Commission: a proposal on proactive measures (merging Articles 3, 6 and 9), a proposal on "public", and a proposal on Article 8a.
Kind regards,
Secretariat JAI.1

From: ADSERBALLE Anne Cecilie
To: BRITTAIN Elizabeth
Subject: FW: written comments on TCO
Date: lundi 17 février 2020 09:10:29
Attachments: Compromise proposal on Article 3, 6 and 9.docx
Compromise public_clean.docx
Art 8a Commission suggestion for compromise text.docx

From: Liina Pello
Sent: Wednesday, February 5, 2020 12:19 PM
To: Marijan.Jelinek@mvep.hr; kmamic@mup.hr; [DL] JAI TWG
Cc: Anni Aleksandrov ; Birgit Paal
Subject: written comments on TCO

Dear partners

Our initial thoughts regarding compromise proposals are added to enclosed files.

We would like to point out, that leaving cloud services outside the scope of the TCO will raise the risk that cloud services could then be misused for distribution of terrorist content. We suggest all information society service providers, that make any information or content available to the public, including content that is accessible through public or semi-public URL, or that is password-protected, should fall within the scope of the regulation. We want to avoid exclusion of closed groups, using one/the same password to access and disseminate the (terrorist) content, as this would affect the operational chain and even reduce the ability to react on terrorist content, which is not in accordance with the aim of the regulation.

We find it useful to clarify, does terms and conditions on para 2 art XX (Specific measures) apply only for HSPs established in the EU MSs or it applies also to non-EU established HSPs? We are not sure it is possible to impose this regulation on HSP-s established in third countries, which does not provide services to significant number of EU users or has a substantial connection to EU MS/MSs.

With regards to the definition of competent authority we strongly hold the position that a Member State must decide at its own discretion what kind of authority should be authorized to issue Orders. There should be the possibility to appoint different authorities to do different tasks. This actually guarantees better compliance with fundamental rights – that is, if the competent authority issuing removal orders and the competent authority enforcing the penalties and overseeing the implementation of proactive measures are different. It is our opinion that to the greatest extent possible the MS should be free to choose the competent authority depending on their size or legal system. This is not just a matter of principle, especially for smaller MS.

Kind regards

Liina Pello
Adviser
+372 612 5040/+372 58865352
Estonian Ministry of the Interior

Compromise proposal on "public"

Art. 1

Para. 1:

This Regulation lays down uniform rules to prevent the misuse of hosting services for the dissemination **to the public** of terrorist content online. It lays down in particular [etc.]

Para. 2:

This Regulation shall apply to hosting service providers offering services in the Union, irrespective of their place of main establishment, **which disseminate information to the public.**

Art. 2

Para. 1:

'hosting service provider' means a provider of information society services consisting of the storage of information provided by and at the request of the content provider **[*rest deleted*]**

Para. 6:

'dissemination to the public' means the making available of information, at the request of the content provider, to a potentially unlimited number of persons.

Commented [AA1]: Should we not consider "make available" or "enable access to" instead of "disseminate"? We feel that "to disseminate" something requires an extra effort to spread the information and could thus be more limiting

Recitals

(10) In order to effectively tackle terrorist content online, while ensuring respect for the private life of individuals, this Regulation should apply to providers of information society services which store and disseminate to the public information provided by a recipient of the service at his or her request, irrespective of whether this activity is of a mere technical, automatic and passive nature. The concept of "storage" should be understood as holding data in the memory of a physical or virtual server. Providers of "mere conduit" or "caching" services as well as of other services provided in other layers of the internet infrastructure, which do not involve such storage, such as registries and registrars as well as providers of domain name systems (DNS), payment or distributed denial of service (DdoS) protection services therefore fall outside the scope of this Regulation.

(10a) The concept of "dissemination to the public" should entail the making available of information to a potentially unlimited number of legal or natural persons that is, making

Commented [AA2]: It is not clear weather our ambition is to leave the (bigger) messaging groups in our out? EE supports having bigger closed groups in the scope. If we want to be sure they are in, the text probably needs a bit more work. We do not want this regulation to limit the current powers of authorities when it comes to TCO or cause unnecessary disputes with the HSP-s.

the information easily accessible to users in general without further action by the content provider being required, irrespective of whether those persons actually access the information in question. Accordingly, the mere possibility to create groups of users of a given service does not, in itself, mean that this Regulation does not apply. ~~However, this Regulation does not apply to closed groups consisting of a finite number of pre-determined persons.~~ Interpersonal communication services, as defined in *[the Telecommunications Code (Dir. 2018/1972)]* such as emails or private messaging services, fall outside the scope of this Regulation. Information should be considered stored and disseminated to the public within the meaning of this Regulation only where such activities are performed upon direct request by the content provider. Consequently, providers of services such as cloud infrastructure, which are provided at the request of other parties than the content providers and only indirectly benefit the latter, should not be covered by this Regulation. By way of example, included in the scope of this Regulation are providers of social media, video, image and audio-sharing, as well as file-sharing and other cloud services, in as far as those services are used to make the stored information available to the public at the direct request of the content provider. Where a service provider offers several services, some of which fall within the scope of this Regulation, this Regulation should be applied only in respect of the services that fall within its scope.

Commented [AA3]: Is the number considered finite if after the initial creation of the group more people join? According to Telecommunications Code finite number of persons means *that the persons initiating or participating in the communication determine the recipient(s)*. Is this to be understood that in case throughout time new people join, but the people who join are determined by the participants in the group or the persons initiated the group, we are talking about a finite number of persons?

Commented [AA4]: If a terrorist e-mail is sent to 100 000 persons (e.g. newsletter), it is out of the scope?

(10b) Terrorist content is often disseminated to the public through services provided by service providers established in third countries. In order to protect users in the Union and to ensure that all service providers operating in the Digital Single Market are subject to the same requirements, this Regulation should apply to all providers of relevant services offered in the Union, irrespective of their country of main establishment. The determination as to whether a service provider offers services in the Union requires an assessment whether it enables legal or natural persons in one or more Member States to use its services and has a substantial connection to that Member State or Member States, in particular an establishment that is relevant to the provision of those services or, in the absence thereof, other specific factual criteria pointing to such a substantial connection. However, the mere accessibility of a service provider's website or of an email address or of other contact details in one or more Member States, taken in isolation, should not be a sufficient condition for the application of this Regulation.

Commented [AA5]: We are not sure it is possible to impose this regulation on HSP-s established in third countries.

Article XX

Specific measures

[Merging of Articles 3, 6 and 9]

Commented [AA1]: *Recital 10a states that the Regulation should also apply to hosting service providers established outside the Union but offering services within the Union […]* We are not sure it is possible to impose this regulation on HSP-s established in third countries.

1. Hosting service providers shall include in their terms and conditions, and apply, provisions to address the misuse of their service for the dissemination of terrorist content online.

2. Where a hosting service provider is exposed to terrorist content, it shall take specific measures to protect their services against the dissemination of terrorist content.

   Those measures should include [at least] one or more~~may include, in particular, one or more~~ of the following:

Commented [AA2]: We would prefer a stronger wording - at least one of these measures should be mandatory (e.g. point a)

   (a) easily accessible and user-friendly mechanisms for users to report or flag to the hosting service provider alleged terrorist content;

   (b) mechanisms to detect, identify and expeditiously remove or disable access to content that is considered terrorist content;

   (c) mechanisms addressing the reappearance of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content.

3. Any specific measure or measures that a hosting service provider takes pursuant to paragraph 2 shall meet all of the following requirements:

   (a) they shall be effective in mitigating and managing the level of exposure to terrorist content;

   (b) they shall be targeted and proportionate, taking into account, in particular, the seriousness of the level of exposure to terrorist content as well as the financial strength of the hosting service provider;

   (c) they shall be applied taking full account of the rights and legitimate interest of the users, in particular users' fundamental rights to freedom of expression and of information, to respect for private life and to protection of personal data;

   (d) they shall be applied in a diligent and non-discriminatory manner;

   (e) where they involve the use of automated tools, appropriate safeguards shall be provided to ensure accuracy and to avoid the removal of information that is not terrorist content, in particular through human oversight and verification.

4. For the purposes of paragraph 2, a hosting service provider shall be considered to be exposed to terrorist content, where the competent authority of the Member State of its main establishment has informed the hosting service provider, through a decision based on objective factors, such as the hosting service provider having received two or more

removal orders in any given 12 month period, that it considers the hosting service provider to be exposed to terrorist content.

5. After having received the decision referred to in paragraph 4 and, where relevant, paragraph 6 a hosting service provider shall report to the competent authority on the specific measures it has taken and that it intends to take in order to comply with the requirement of paragraph 2 and 3. It shall do so within three months of receipt of the decision and thereafter on an annual basis.

6. Where, based on the reports referred to in paragraph 5 and, where relevant, any other objective factors, the competent authority considers that the measures that a hosting provider has taken do not meet the requirements of paragraphs 2 and 3, the competent authority shall address a decision to the hosting service provider requiring it to adjust those measures or to take certain additional measures so as to ensure that those requirements are met.

7. A hosting service provider may, at any time, request the competent authority to review and, where appropriate, adjust or revoke the decisions referred to in paragraphs 4 and 6. The competent authority shall, within a reasonable time period after receiving the request, take a reasoned decision based on objective factors on the request and inform the hosting service provider accordingly.

8. Any requirement to take measures pursuant to this Article shall not entail a general obligation on hosting services providers to monitor the information which they store, nor a general obligation to actively seek facts or circumstances indicating illegal activity.

Commented [LP3]: Does terms and conditions on Para 2 apply only for HSPs established in the EU MSs or it applies also to non-EU established HSPs? We are not sure it is possible to impose this regulation on HSP-s established in third countries, which does not provide services to significant number of EU users or has a substantial connection to EU MS/MSs.

Commented [AA4]: The wording of this para is too broad and could give opportunities for HSPs not acting in good faith to unreasonably prolong taking action.

Commission suggestion for compromise text on Article 8a

Commented [AA1]: This article is OK for us

2) Article 8a

Article 8a
Transparency obligations for competent authorities

1. Competent authorities shall publish annual transparency reports relating to their activities under this Regulation. Those reports shall include at least the following information in relation to the year covered:
(a) the total number of removal orders issued in accordance with Article 4 and the number of instances in which the removal orders led to the removal of or disabling of access to terrorist content and the number of instances in which they did not;
(b) the total number of referrals issued in accordance with Article 5 and number of instances in which the referrals led to the removal of or disabling of access to terrorist content and the number of instances in which they did not;
(c) the total number of decisions imposing [proactive/specific] measures taken in accordance with Article 6(4) and a description of the measures imposed;
(d) the total number of instances in which removal orders and decisions imposing [proactive/specific] measures were subject to administrative or judicial remedies and information on the outcome of the relevant proceedings.
(e) The total number of decisions imposing penalties, including a description of the type of penalty imposed.

2. The transparency reports referred to in paragraph 1 shall not contain information that may affect ongoing activities for the prevention, detection investigation or prosecution of terrorist offences or national security interests.

From: ADSERBALLE Anne Cecilie
To: "KAARLEP Agne"; "Emese.KOTTASZ@ec.europa.eu"; WERNERT Severine
Subject: FW: TCO - comments
Date: lundi 3 février 2020 14:37:50

From: Puiro Johanna SM
Sent: Monday, February 3, 2020 1:58 PM
To: ADSERBALLE Anne Cecilie ; Marijan Jelinek ; JAI INTERNAL SECURITY ; Mamic Krešimir
Cc: Mari Hämäläinen
Subject: TCO - comments

Dear all,

I would like to wish you all the best with the TCO file! I know how challenging this file is!

Below you will find FI comments. Main concern is related to specific/proactive measures.

1. Merging Articles 3, 6 and 9

In general, Finland can support the idea of merging Articles 3, 6 and 9. Attached you will find FI text proposal.

It is unclear whether the COM proposes to delete articles 3 and 9 entirely or just take para 2 of Article 3 to the new para 1 of Article 6. It seems that all the content in Article 9 would be found in new Article 6.

Finland would like to get clarification of the aim of the new Article 6 as proposed by the Commission. In the COM original proposal and Council GA, the starting point was that the HSP's should take their societal responsibility (recital 3) to protect their services from the misuse by terrorists. It was understood that the aim was to involve the industry to act. Now this new compromise proposal will shift the burden. The industry does not have to do anything, except having terms and conditions on terrorist content, before applying e.g. flagging systems or disable access to terrorist content.

Article 6 para 1: Now in the COM compromise proposal all HSP's should "include in their terms and conditions, and apply, provisions to address the misuse of their service for the dissemination of terrorist content online". What consequences are there in case a HSP does not do that. In Art 17 GA a penalty is foreseen in case a HSP infringes its obligation to have these terms and conditions. EP wishes to delete this provison (AM 132). So will there be a penalty? EP also wishes to require that before issuing a penalty, there must be a systematic and persistent breach (AM 131). Will that amendment be accepted as well. What will suffice the a systematic and persistent breach of not having terms and conditions as required. Is the Regulation clear and precise here? A more minor remark: Maybe it would be could to add the word "public" also in this paragraph in accordance with the Presidency proposal to Art 1 and 2.

Article 6 paras 2 and 3: In general, making the provisions of specific measures more clear and targeted is good. It would be good to know, is para 2 an exhaustive list of measures? Should these measures be given as examples and put them in a recital. We do not know what type of effective measures will be available in the near future.

Exposed to terrorist content (para 2 and 4): COM proposal would be a remarkable change to the original COM proposal and reasoning behind it. The new COM proposal would mean that the obligation to take specific measures would only begin after the HSP has received 2 or more removal orders in 12 months. The burden to follow the content online would be shifted to the authorities. The HSP's, whose business this is, would not have to do anything to address the misuse before getting this decision. This paragraph is a major change to the GA. In recital 3 it is currently stated "online service providers have particular societal responsibllities to protect their services from misuse by terrorists". With this new paragaraph it seems that this responsibility begins only after the authorities have detected this illegal content. Furthermore, the 2 removal

orders would have to be issued by the host Member State. To give an example, if Ireland has not issued any removal orders to Google, in the past 12 months, Google does not have to take specific measures. The starting point of the Regulation was that the MS against which the terrorist threat is directed to is best in place to detect it. So, there might be a HSP located in Finland but having as target audience Greece. What is the likelihood of Finnish authorities following the Greek content on the services of that HSP identifying content as terrorist content.
Para 5: FI This para is ok. However, one might wish to add a maximum time period for this reporting, such as 3 years for example.

2. Word "PUBLIC"

Recitla 10 a: According to the Recital: "Information should be considered stored and disseminated to the public within the meaning of this Regulation only where such activities are performed upon direct request by the content provider." Perhaps it is not necessary to include the word "direct". That is not included in the E-commerce either, where "information service" is defined:

> Directive 98/34/EC is amended as follows:
>
> 2. Article 1 is amended as follows:
> (a) the following new point shall be inserted:
> '2. **"service"**, any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at **the individual request** of a recipient of services.

- "at the individual request of a recipient of services" means that the service is provided through the transmission of data on individual request

3. Transparency obligations for the HSP Article 8 a

These can be accepted in case the MS will keep the freedom to choose their national authorities.

Best regards,
Johanna Puiro

Note de commentaires

Commentaires de la France sur le projet de règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne – suite de la réunion des conseillers JAI TCO du 31 janvier 2020.

Suite à la réunion des conseillers JAI TCO du 31 janvier 2020, la Présidence a invité les États membres à faire part de leurs commentaires s'agissant des compromis diffusés dans la perspective de ladite réunion. Ceux-ci portaient sur trois points :

- Une proposition de reformulation s'agissant des articles 3, 6 et 9, fusionnés en un seul traitant des mesures spécifiques ;
- Une précision de l'article 1 sur la notion de « diffusion au public » ;
- Une nouvelle rédaction s'agissant des obligations de transparence des autorités compétentes.

D'une manière générale, les compromis proposés vont dans le bon sens et viennent réaffirmer certains principes fondamentaux.

S'agissant des mesures spécifiques :

La nouvelle rédaction proposée au sujet des mesures spécifiques nous convient. Les autorités françaises saluent donc le travail de rédaction de la Présidence, consacrant l'aspect obligatoire de ces mesures tout en préservant l'équilibre avec le respect des droits fondamentaux. Sous réserve de la prise en compte des éléments ci-après, elles émettent donc un avis favorable à cette proposition de compromis.

- point 2 du document joint : les autorités françaises proposent de remplacer la phrase "*it shall take specific measures to protect their services against the dissemination of terrorist content*" par "*It shall take specific measures to make sure their services are not used to disseminate terrorist content*". Elles proposent également de remplacer "*Those measures **may** include, in particular, one or more of the following*" par "***must***" ou "***shall***".

- point 4 : les autorités françaises s'interrogent sur l'absence de référence à la plateforme de signalement de contenus illicites (IRU) d'Europol qui est amenée à jouer un rôle de plus en plus important dans la lutte contre les contenus illicites en ligne au niveau européen.

- point 5 : les autorités françaises font remarquer que le délai de « trois mois » ne permettra pas de respecter le délai dit "*golden hour*". Un délai d'une durée maximale d'un mois serait plus approprié.

- point 7 : les autorités françaises proposent de remplacer "*within a reasonable time period*" par "*within a month*" en miroir du point 5.

S'agissant de la notion de diffusion au public :

S'agissant de la rédaction proposée pour la notion de « diffusion au public », les autorités françaises estiment qu'il s'agit là d'une bonne base de négociation mais que celle-ci gagnerait à être précisée. Les autorités françaises considèrent que la formule "*to a potentially unlimited number of persons*" telle qu'elle figure à l'article 2 paragraphe 6 et dans le cadre du considérant 10a) pose difficulté ; cette formule génère de la confusion dans la mesure où elle peut suggérer que la notion de diffusion publique se limite à des cas de diffusion qui s'adresseraient nécessairement à l'intégralité du public de l'Internet.

En effet, cette rédaction pourrait être interprétée comme signifiant que le seul fait que certaines limites aient été apportées à la visibilité d'un contenu induirait que ce contenu ne puisse jamais être considéré comme public. De telles limites peuvent avoir été prévues par l'hébergeur (nombre de personnes dans un groupe) ou par l'utilisateur (diffusion restreinte au cercle d'amis, ou aux amis d'amis, etc.).

L'appréciation du caractère public de la diffusion doit ainsi être pouvoir être appréciée au cas par cas, compte tenu notamment des paramétrages de visibilité et de l'audience potentielle. À titre d'exemple, la jurisprudence française a pu considérer que les contenus postés sur un mur *Facebook* ouvert aux seuls « amis » ne sont pas publics dès lors qu'ils sont accessibles uniquement à un nombre limité de personnes agréées par le titulaire de compte (Cour d'appel de Versailles, 3ème ch, 18 juin 2015, 13-03453), **mais qu'en revanche, lorsqu'il est également accessible aux « amis des amis », dont le nombre est incontrôlable**, et qui ne constituent pas une communauté d'intérêts, les contenus sont publics. (Cour d'appel de Douai, 11 septembre 2014 n°14/02540).

L'intérêt de cette approche est d'éviter que le texte aboutisse par exemple à écarter du champ d'application des messageries comme *Telegram* ou *Rocketchat*, ou une plateforme qui viendrait à décider que la visibilité du contenu est limitée à x personnes, alors que ce nombre est extrêmement élevé.

Autre exemple, un groupe constitué sur l'application de messagerie *Telegram* peut accueillir jusqu'à 230 000 participants et peut être rejoint en suivant un simple lien hypertexte, sans agrément des modérateurs du groupe. Le créateur d'un groupe peut en outre le rendre public et les échanges seront ainsi visibles par d'autres utilisateurs, sans que ces derniers ne soient membres du groupe. Un utilisateur de *Telegram* peut également créer un canal, qui fonctionne comme l'équivalent d'une plateforme, en ce qu'il permet de partager un contenu à un nombre illimité de destinataires.

Les autorités françaises considèreraient donc utile de supprimer dans la définition et le considérant 10a les termes « *to a potentially unlimited number of persons* », de supprimer les 3e et 4e phrases du considérant 10a proposé et d'ajuster ce dernier pour préciser d'autres critères pouvant être utilisés pour apprécier au cas par cas le caractère public ou non d'une diffusion. À titre d'exemple, aux fins d'appréciation de celui-ci, on peut citer le nombre restreint de personnes agréées, la communauté d'intérêt que forment ou non les membres d'un groupe sur une plateforme telle que *Facebook*, l'accessibilité du contenu aux seules personnes agréées par le titulaire du compte.

Les autorités françaises proposent donc d'amender la proposition de compromis comme suit :

Compromise proposal on "public"

Art. 1
Para. 1:
This Regulation lays down uniform rules to prevent the misuse of hosting services for the dissemination ***to the public*** *of terrorist content online. It lays down in particular [etc.]*
Para. 2:
This Regulation shall apply to hosting service providers offering services in the Union, irrespective of their place of main establishment, ***which disseminate information to the public.***
Art. 2
Para. 1:
'hosting service provider' means a provider of information society services consisting of the storage of information provided by and at the request of the content provider ***[rest deleted]***
Para. 6:
'dissemination to the public' means ~~the~~ making ~~available of~~ information ***easily accessible to any users without further action by the content provider being required, irrespective of whether one or more users actually access the information in question~~ ~~, at the request of the content provider, to a potentially unlimited number of persons.~~***

Recitals

(10) In order to effectively tackle terrorist content online, while ensuring respect for the private life of individuals, this Regulation should apply to providers of information society services which store and disseminate to the public information provided by a recipient of the service at his or her request, irrespective of whether this activity is of a mere technical, automatic and passive nature. The concept of "storage" should be understood as holding data in the memory of a physical or virtual server. Providers of "mere conduit" or "caching" services as well as of other services provided in other layers of the internet infrastructure, which do not involve such storage, such as registries and registrars as well as providers of domain name systems (DNS), payment or distributed denial of service (DdoS) protection services therefore fall outside the scope of this Regulation.

(10a) The concept of "dissemination to the public" should entail ~~the making available of information to a potentially unlimited number of legal or natural persons that is~~, making the information easily accessible to ***any*** *user* ~~***in general***~~ *without further action by the content provider being required, irrespective of whether* ~~***those persons***~~ *one or more users actually access the information in question.* ***While in many cases, the dissemination of terrorist content to a group of individuals approved by the account holder on a social network and bound by a community of interest should not be considered as public dissemination, the mere possibility to create groups of users of a given service does not, in itself, mean that this Regulation does not apply. The public nature of the dissemination shall be assessed on a case by case basis.*** ~~***However, the Regulation does not apply to closed groups consisting of a finite number of pre-determined persons.***~~ *Interpersonal communication services, as defined in [the Telecommunications Code (Dir. 2018/1972)] such as emails or private messaging services,* ***should in principle*** *fall outside the scope of this Regulation* ***as it relates to private correspondance. However, such services should be included in the scope of the Regulation when a content is made available to the public at the direct request of the content provider.*** *Information should be considered stored and disseminated to the public within the meaning of this Regulation only where such activities are performed upon direct request by the content provider. Consequently, providers of services such as cloud infrastructure, which are provided at the request of other parties than the content providers and only indirectly benefit the latter, should not be covered by this Regulation. By way of example, included in the scope of this Regulation are providers of social media, video, image and audio-sharing, as well as file-sharing and other cloud services, in as far as those services are used to make the stored information available to the public at the direct request of the content provider. Where a service provider offers several services, some of which fall within the scope of this Regulation, this Regulation should be applied only in respect of the services that fall within its scope.*

(10b) Terrorist content is often disseminated to the public through services provided by service providers established in third countries. In order to protect users in the Union and to ensure that all service providers operating in the Digital Single Market are subject to the same requirements, this Regulation should apply to all providers of relevant services offered in the Union, irrespective of their country of main establishment. The determination as to whether a service provider offers services in the Union requires an assessment whether it enables legal or natural persons in one or more Member States to use its services and has a substantial connection to that Member State or Member States, in particular an establishment that is relevant to the provision of those services or, in the absence thereof, other specific factual criteria pointing to such a substantial connection. However, the mere accessibility of a service provider's website or of an email address or of other contact details in one or more Member States, taken in isolation, should not be a sufficient condition for the application of this Regulation.

S'agissant des obligations de transparence des autorités compétentes :

Enfin, les autorités françaises accueillent favorablement la rédaction proposée à l'article 8a, obligations de transparence des autorités compétentes.

NOTE
from the Hungarian delegation to Terrorism Working Party (TWP)

Subject: Proposal for a Regulation on preventing the dissemination of terrorist content online

Specific comments regarding the draft compromise proposal by the Presidency issued on 31th of January 2020 on JHA COUNSELLORS meeting

Compromise proposal on "public"

We can be flexible in order to reach the compromise on these provisions but we would like to emphasize that in our view if this change would be accepted (especially in the recitals) then hosting providers could not be obliged to remove terrorist contents circulated within closed user groups. Terrorist propaganda contents are in many cases hidden behind a fully legal, innocuous looking public front page and they are available for download only after a registration. This would substantially hinder the effectiveness of the TCO Regulation.

In our view, the text of the new proposal regarding the recitals still does not solve the problem outlined above, since the definition interprets public access only to subscriptions to the service as a whole, and not to the content with specific authentication within the service.

Commission suggestion for compromise text on Article 8a

Hungary can support the compromise text proposal regarding Article 8a.

Specific measures [Merging of Articles 3, 6 and 9]

- Regarding the first paragraph of the compromise proposal – formerly Article 3(2) – Hungary supports to keep the text of the general approach.
- Regarding the compromise proposal on the fourth paragraph Hungary share the concern that the new wording imposes additional burden on the competent authority. In our opinion we should strive to keep the balance regarding the obligations of the competent authorities.
- Regarding the further points of the compromise proposal on the Specific measures Hungary

can be flexible in order to reach the compromise.

From:	ADSERBALLE Anne Cecilie
To:	BRITTAIN Elizabeth
Subject:	FW: TCO - deadline for comments
Date:	lundi 17 février 2020 09:09:14
Attachments:	image002.gif image003.jpg 20200205 Articles 3 6 9 with IE comments.docx

From: Ian P. Mulholland
Sent: Wednesday, February 5, 2020 12:01 PM
To: 'MarijanJelinek@mvep.hr' ; 'kmamic@mup.hr' ; [DL] JAI TWG
Cc: Tara M. Storey ; Richard X. Troy ; EurAffairs ; Antoinette.Doran@dfa.ie; 'John.Keyes@dfa.ie'
Subject: RE: TCO - deadline for comments

Colleagues,

Please find attached our comments on the Commission proposal to merge Articles 3, 6, and 9 (in track-changes format, as requested).

In common with the concerns raised by several MS at the recent JHA Counsellors' meeting on 31 January 2020, we believe that the procedure outlined in paragraph 4 would be unreasonably onerous for competent authorities. We note that this paragraph suggests that the determination should be made based on objective factors, with an example given in the wording. We would suggest that, if objective factors can be established in the text, there is no need for a CA to have a role in this regard, as a HSP would unambiguously be deemed to be exposed to terrorist content based upon the Regulation, which is directly applicable.

We have proposed text to this effect in the tracked changes, along with other related amendments – as always we are aiming to be constructive and flexible. In this regard we welcome the initiative by the Presidency to break the deadlock in the negotiations, and hope that these efforts will be matched by the European Parliament.

Best regards,

Ian

Ian Mulholland
Oifigeach Riaracháin | Beartais Chibear-Shlándála
Administrative Officer | Cyber Security Policy
Acmhainní d'Ábhair ar Leith agus Beartais Fheidhmeacha | Ceartas Coiriúil
SMR and Applied Policy | Criminal Justice

An Roinn Dlí agus Cirt agus Comhionannais
Department of Justice and Equality
51 Faiche Stiabhna, Baile Átha Cliath 2, D02 HK52
51 St Stephen's Green, Dublin 2. D02 HK52

T +353 (0)1 602 8395 **M** +353 (0)87 349 4694 **Internal VOIP** 60 8395
E IPMulholland@justice.ie **W** www.justice.ie twitter.com/DeptJusticeIRL

From: John.Keyes@dfa.ie <John.Keyes@dfa.ie>
Sent: Monday 3 February 2020 14:25
To: Ian P. Mulholland <IPMulholland@justice.ie>
Cc: Tara M. Storey <TMStorey@justice.ie>; Richard X. Troy <RXTroy@justice.ie>; EurAffairs <EurAffairs@justice.ie>; Antoinette.Doran@dfa.ie
Subject: FW: TCO - deadline for comments

Hi Ian,

FYI

John

John Keyes
Criminal Justice & Data Protection Attaché | Justice & Home Affairs
Permanent Representation of Ireland to the European Union
Rue Froissart 50 | 1040 Brussels |John.keyes@dfa.ie | T: +32 (0) 22 823252 | GSM: +32 (0) 497 053796

From: JAI INTERNAL SECURITY <jai.internal.security@consilium.europa.eu>

Sent: Monday 3 February 2020 15:19
Subject: TCO - deadline for comments

Dear colleagues,

On behalf of the Presidency, we would like to remind you about the deadline - **Wednesday 5 February, 12h** - for possible comments to the Commission proposals presented at the JHA-Counsellors' meeting last Friday. We take the opportunity to inform you that at today's technical meeting with the EP, the Commission's proposal to merge Articles 3, 6 and 9 was initially welcomed.

Kind regards,

Denisa KUPCAKOVA

General Secretariat of the Council
Directorate-General Justice and Home Affairs
Directorate Home Affairs
20-50-MN-78
Rue de la Loi/Wetstraat, 175 - B-1048 Bruxelles/Brussel - Belgique/België
Direct tel: + 32-2-281.64.06 | Mobile:
www.consilium.europa.eu | denisa.kupcakova@consilium.europa.eu

Article XX

Specific measures

[Merging of Articles 3, 6 and 9]

1. Hosting service providers shall include in their terms and conditions, and apply, provisions to address the misuse of their service for the dissemination of terrorist content online.

2. Where a hosting service provider is exposed to terrorist content, it shall take specific measures to protect their services against the dissemination of terrorist content.

   Those measures may include, in particular, one or more of the following:

   (a) easily accessible and user-friendly mechanisms for users to report or flag to the hosting service provider alleged terrorist content;

   (b) mechanisms to detect, identify and expeditiously remove or disable access to content that is considered terrorist content;

   (c) mechanisms addressing the reappearance of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content.

3. Any specific measure or measures that a hosting service provider takes pursuant to paragraph 2 shall meet all of the following requirements:

   (a) they shall be effective in mitigating and managing the level of exposure to terrorist content;

   (b) they shall be targeted and proportionate, taking into account, in particular, the seriousness of the level of exposure to terrorist content as well as the financial strength of the hosting service provider;

   (c) they shall be applied taking full account of the rights and legitimate interest of the users, in particular users' fundamental rights to freedom of expression and of information, to respect for private life and to protection of personal data;

   (d) they shall be applied in a diligent and non-discriminatory manner;

   (e) where they involve the use of automated tools, appropriate safeguards shall be provided to ensure accuracy and to avoid the removal of information that is not terrorist content, in particular through human oversight and verification.

4. For the purposes of paragraph 2, a hosting service provider shall be considered to be exposed to terrorist content, where ~~the competent authority of the Member State of its main establishment has informed the hosting service provider, through a decision based on objective factors, such as~~ the hosting service provider ~~having~~ has received two or more removal orders in any given 12 month period, ~~that it considers the hosting service provider to be exposed to terrorist content~~. Where a hosting service provider has been

exposed to terrorist content, it shall no longer be considered to be exposed to terrorist content following a 12 month period in which it has received fewer than two removal orders.

5. ~~After having received the decision referred to in paragraph 4 and, where relevant, paragraph 6 bA~~ hosting service provider that has been exposed to terrorist content shall report to the appropriate competent authority on the specific measures it has taken and that it intends to take in order to comply with the requirements of paragraph 2 and 3. It shall do so within three months of receipt of the decision and thereafter on an annual basis. Where a hosting service provider receives a decision referred to in paragraph 6 it shall report to the appropriate competent authority on the adjustments made or additional measures taken within three months.

6. Where, based on the reports referred to in paragraph 5 and, where relevant, any other objective factors, the competent authority considers that the measures that a hosting provider has taken do not meet the requirements of paragraphs 2 and 3, the competent authority shall address a decision to the hosting service provider requiring it to adjust those measures or to take certain additional measures so as to ensure that those requirements are met.

7. A hosting service provider may, at any time, request the competent authority to review and, where appropriate, adjust or revoke the decisions referred to in paragraphs ~~4 and~~ 6. The competent authority shall, within a reasonable time period after receiving the request, take a reasoned decision based on objective factors on the request and inform the hosting service provider accordingly.

8. Any requirement to take measures pursuant to this Article shall not entail a general obligation on hosting services providers to monitor the information which they store, nor a general obligation to actively seek facts or circumstances indicating illegal activity.

Commented [IPM1]: We believe that this paragraph would be unreasonably onerous for competent authorities. We note that this paragraph suggests that the determination should be made based on objective factors, with an example given in the wording. We would suggest that, if objective factors can be established in the text, there is no need for a CA to have a role in this regard, as a HSP would unambiguously be deemed to be exposed to terrorist content based upon the Regulation, which is directly applicable

Comments from the Netherlands on the proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online – 5 February 2020

The Netherlands supports the compromise proposals, and would like to highlight the following:

Article	Position
Art. 1 (1) Art. 1 (2)	We support the compromise of adding the word public.
Art. 2 (1) Art. 2 (6) Recital 10 Recital 10a Recital 10b	This compromise is in line with previous comments of the Netherlands about HSP's and the scope of the regulation. This regulation should only apply to HSP's which disseminate information to the public and thus to a potentially unlimited number of persons. It should not apply to e-mail, private messaging and other kinds of non-public forms of information and communication.
Merging of Art. 3, 6 and 9	We support the compromise proposal, except for paragraph 4. Paragraph 2c: strong support for the current wording ('addressing the reappearance'). This clarifies that the draft Regulation does not entail an obligation to filter content prior to its publication, as prohibited by the Dutch constitution, while leaving open that possibility for MS with different constitutional systems. Paragraph 4: we prefer a custom approach with regards to the choice to impose proactive measures or not. Paragraph 8: while we would prefer a direct reference to article 15(1) of Directive 2000/31/EC, we understand the reasoning for the current wording, as discussed in last counsellor's meeting. If the current wording remains, perhaps it could be clarified elsewhere (f.i. in a recital) that, regardless of the wording, the existing case law about Article 15(1) is applicable. This would ensure that the current wording does not imply a deviation from the e-commerce Directive.
Art. 8a	Support. Given the particularly important task of competent authorities and the potential effects of removal orders on the freedom of expression, transparency obligations of competent authorities are necessary.

Warsaw, 5th February 2020

Polish written comments concerning issues presented at the JHA-Counsellors' meeting on 31 of January 2020

On the proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online

Please find Poland's written comments on the draft compromise proposals, which were circulated by e-mail, after JHA Counsellors meeting on 31 of January 2020.

First document: Compromise proposal on "public"

We support compromise proposals in art. 1 and art. 2. We agree that the use of the word "public" better reflects the intentions that were behind the preparation of the draft regulation, i.e. terrorist content that goes into the public domain. This amendments also address issue that was raised in European Union Agency for Fundamental Rights opinion - on excessive interference with the right to freedom of expression and private life.

We do not object compromise text in recitals: 10, 10a, 10b. It is important to clearly define to which catalog of entities this regulation applies.

Second document: Specific measures [Merging of Articles 3, 6 and 9]

We support an idea to merge art. 3, 6 and 9.

We especially support compromise text in paragraph 2 and 3 of the new article – to enlist measures that are expected from hosting service provider. For Poland it is of particular importance to ensure that any measures introduced on service providers are effective, targeted and proportionate to the level of exposure of its services against terrorist content.

We support paragraph 8 as it ensures compliance with the Directive on electronic commerce 2000/31/EC. Article 15 (1) of this directive lays down the basic principle that EU Member States cannot impose a general obligation on internet intermediaries to monitor the information which they transmit or store.

Paragraph 7. We support the idea that hosting service provider should be able to appeal against decisions made by competent authority. The procedure for dealing with such complaints should include timeframe for examining it. It should also be made clear that hosting service provider can appeal against the decision to the court. The compromise proposal should be updated to include these two points.

We do not have any substantial objections toward the rest of the paragraphs in the new article.

Third document: Article 8a Transparency obligations for competent authorities

We support the idea to indicate transparency obligations for competent authorities.

We agree that transparency obligation, as it was indicated in paragraph 2, should not lead to exposing information that may affect ongoing activities for the prevention, detection investigation or prosecution of terrorist offences or national security interests.

We would like to point out that in case of point b of article 8a (reporting on the total number of referrals) it should be noted that European Parliament proposed to delete Art. 5 concerning referrals. Therefore before the final version of art. 8a can be accepted, we should decide whether we want to keep referrals as part of this Regulation.

From: Andreea RADUTU
To: JAI INTERNAL SECURITY
Cc: ADSERBALLE Anne Cecilie
Subject: RO comments TCO
Date: mercredi 5 février 2020 09:57:10
Attachments: image001.jpg

Dear colleagues,

Following your request regarding the TCO Regulation, with focus on article 1 and 2, the proposal on proactive measures (merging Articles 3, 6 and 9) and a proposal on Article 8a, we inform you that, at this moment, we agree with the current text and we have no further proposals and observations.

Best regards,
Andreea Radutu

From: JAI INTERNAL SECURITY
Sent: Monday, 3 February 2020, 15:19
Subject: TCO - deadline for comments

Dear colleagues,
On behalf of the Presidency, we would like to remind you about the deadline - **Wednesday 5 February, 12h** - for possible comments to the Commission proposals presented at the JHA-Counsellors' meeting last Friday. We take the opportunity to inform you that at today's technical meeting with the EP, the Commission's proposal to merge Articles 3, 6 and 9 was initially welcomed.
Kind regards,
Denisa KUPCAKOVA

General Secretariat of the Council
Directorate-General Justice and Home Affairs
Directorate Home Affairs
20-50-MN-78
Rue de la Loi/Wetstraat, 175 - B-1048 Bruxelles/Brussel - Belgique/België
Direct tel: + 32-2-281.64.06 | Mobile:
www.consilium.europa.eu | denisa.kupcakova@consilium.europa.eu

SUBJECT	CONTRIBUTION FROM THE SPANISH DELEGATION

Considering the latest documents distributed in relation to the Regulation on the withdrawal of Terrorist Content *Online*, and to the JHA Councils meeting held on 13th February, this delegation states as follows:

1- Cross-border effect: we agree to be firm in the negotiation and to maintain the Council's position.

   However, as it seems to be a position currently blocked in the negotiation with the Parliament, alternative ways to unblock this situation are being considered, including in the procedure the competent authority in the State where the company has its head office, giving it the possibility to cancel or suspend the execution of the withdrawal order.

   For Spain, it would be essential to maintain the one-hour deadline and that it is not affected. The order would be sent both to the company (for which it should be enforceable), and to the competent authority, whose silence would be understood not to stall it, although it would have the possibility, in the event of a reaction, of cancelling or suspending it.

   Spain would be willing to consider such a solution, as a possible alternative to a total blockade with Parliament and within the framework of an overall final agreement to unblock the situation. Thus, perhaps at group level, it would be useful to reflect on the conditions under which this might be acceptable.

2- In relation to the consideration of "objective criteria", and based on the Commission's statement, we agree that receiving two withdrawal orders is an objective criterion, though there may be others such as receiving a certain number of *referrals*.

3- With regard to point 7: we agree that a deadline should be set, it can be negotiated whether a month or two, we could be flexible on this point.

4- It is important to us that the term "*promoting*" be maintained.

CORREO ELECTRÓNICO:
cgi@dgp.mir.es

COMISARÍA GENERAL DE INFORMACIÓN
C/ Julián González Segador s/n
28043 – MADRID
+34 915 822 133 | +34 915 822 160
+34 915 822 281

5- Regarding the concept of audience: we think that attempts to establish a definition on the criterion of the potential number of users are not progressing.

We therefore propose a new approach based on the criterion of access to content. If we speak of "*potentially unlimited number of persons*", it can be misleading, and furthermore, the focus should not be on the unlimited number or not, but on the form of access to this content[1].

We therefore propose an alternative wording to article 2, paragraph 6: "dissemination to the public" means making the information available to a plurality of users directly, at the request of the *content provider*.

By meaning "Directly" the user is not subject to any kind of identity verification[2].

Furthermore, in the *recitals*, paragraph 10, we propose to slightly modify the wording when the last line refers to the DdoS, since this is only one type of attack out of all the possible ones and we would prefer an all-encompassing wording: *providers of domain name systems (DNS), payment or ~~distributed denial of service (DdoS)~~ cybersecurity protection services therefore fall outside the scope of this Regulation.*

6- With regard to Europol and its involvement in these procedures: we believe that given the legal basis chosen for the Regulation, it is difficult to establish mandatory provisions for Europol.

Instead, we believe it is necessary for the Agency's Management Board to establish a procedure whereby Member States can exchange information on possible withdrawal orders, prior to their formal issuance to the competent authority; so that if a Member State has undertaken an investigation into the content to be withdrawn, it may give notice in time to assess whether it is appropriate to issue the formal order or to await possible results of the ongoing investigation.

---

[1] In this sense, it should also be remembered that the usual method for terrorists to enter Telegram groups is to share links for seconds in public spaces that usually give access to the group after several clicks, thus providing public access and therefore public content.
Rather, it would be private content if it is contained into a WhatsApp group, which is accessed because the group's administrator adds you.

[2] The content you access after clicking 23 links would be in this sense "directly accessible", as no one verifies our identity, access only depends on our patience. **And this is the usual method among terrorists.**

7- Finally, our experts insist that the term "*hosting service provider*" is not correct, since "*hosting*" makes reference to when "they rent a space for you to include the content you want, content to which the renter does not have access, and therefore he is not responsible", and is not covered by this Regulation.

Therefore, we consider the definition to be correct, but we propose to talk about *"online, Internet, or information society services*" instead of "*hosting service provider".*

Madrid, on 17th February 2020.

MINISTERIO
DEL INTERIOR

DIRECCIÓN GENERAL DE LA POLICÍA
CUERPO NACIONAL DE POLICÍA

Article XX

Specific measures

[Merging of Articles 3, 6 and 9]

Commented [KK1]: The proposal seems to have lost important points from Article 9 of the Council negotiating mandate (lines 176-178) and the proposed amendment 104 (lines 179-180) of the EP. It seems to Sweden that both safeguards and effective remedies are important features of the Regulation in this particular context. In particular, it is important that clear safeguards are provided should the Regulation enable automated tools to be imposed on hosting service providers when they do not meet the requirements of points 2 and 3

1. Hosting service providers shall include in their terms and conditions, and apply, provisions to address the misuse of their service for the dissemination of terrorist content online.

2. Where a hosting service provider is exposed to terrorist content, it shall take specific measures to protect their services against the dissemination of terrorist content.

   Those measures may include, in particular, one or more of the following:

   (a) easily accessible and user-friendly mechanisms for users to report or flag to the hosting service provider alleged terrorist content;

   (b) mechanisms to detect, identify and expeditiously remove or disable access to content that is considered terrorist content;

   (c) mechanisms addressing the reappearance of content which has previously been removed or to which access has been disabled because it is considered to be terrorist content.

3. Any specific measure or measures that a hosting service provider takes pursuant to paragraph 2 shall meet all of the following requirements:

   (a) they shall be effective in mitigating and managing the level of exposure to terrorist content;

   (b) they shall be targeted and proportionate, taking into account, in particular, the seriousness of the level of exposure to terrorist content as well as the financial strength of the hosting service provider;

Commented [KK2]: Moved to para 6

   (c) they shall be applied taking full account of the rights and legitimate interest of the users, in particular users' fundamental rights to freedom of expression and of information, to respect for private life and to protection of personal data;

   (d) they shall be applied in a diligent and non-discriminatory manner;

   (e) where they involve the use of automated tools, appropriate safeguards shall be provided to ensure accuracy and to avoid the removal of information that is not terrorist content, in particular through human oversight and verification.

4. For the purposes of paragraph 2, a hosting service provider shall be considered to be exposed to terrorist content, where the hosting service provider has received ~~competent authority of the Member State of its main establishment has informed the hosting service provider, through a decision based on objective factors, such as the hosting service provider having received~~ two or more removal orders in any given 12 month period, ~~that it considers the hosting service provider to be exposed to terrorist content.~~

Commented [KK3]: This burden should not be put on the competent authority, but rather the HSP. (These changes also require redrafting of parts of para 5.)

5. ~~After having receives the decision referred to in paragraph 4 and, where relevant, paragraph 5~~ a hosting service provider shall report to the competent authority on the specific measures it has taken and that it intends to take in order to comply with the requirement of paragraph 2 and 3. It shall do so within three months ~~of receipt of the decision~~ and thereafter on an annual basis.

Commented [KK4]: This will have to be deleted since we suggest changes in para 4.

6. Where, based on the reports referred to in paragraph 5 and, where relevant, any other objective factors, taking into account the seriousness of the level of exposurse to terrorist content as well as the financial strength of the host service provider, the competent authority considers that the measures that a hosting provider has taken do not meet the requirements of paragraphs 2 and 3, the competent authority shall address a decision to the hosting service provider requiring it to adjust those measures ~~or to take certain additional measures~~ so as to ensure that those requirements are met.

Commented [KK5]: This wording does not meet the requirement of legal clarity and foreseeability

7. A hosting service provider may, at any time, request the competent authority to review and, where appropriate, adjust or revoke the decisions referred to in paragraphs 4 and 6. The competent authority shall, within a reasonable time period after receiving the request, take a reasoned decision based on objective factors on the request and inform the hosting service provider accordingly.

8. Any requirement to take measures pursuant to this Article shall not entail a general obligation on hosting services providers to monitor the information which they store, nor a general obligation to actively seek facts or circumstances indicating illegal activity.