Council of European National Top-Level Domain Registries

Brussels, Belgium
1 September 2020

CENTR Comment on the public consultation on the Digital Services Act

Introduction

CENTR is providing its response to the European Commission's public consultation[1] on the Digital Services Act (DSA). The document below represents only the questions deemed to be relevant for CENTR members' input on which there was a consensus amongst volunteers who helped drafting the response.

CENTR response

C. Activities which could cause harm but are not, in themselves, illegal

4 In your personal experience, how has the spread of harmful (but not illegal) activities online changed since the outbreak of the COVID-19 pandemic? Please explain.

3000 character(s) maximum

CENTR answer:

Country-code top-level domain registries (ccTLDs) are responsible for maintaining the internet infrastructure, the Domain Name System. ccTLDs manage a country-specific top-level domain which is usually reserved to sovereign states, e.g. .si or .fr.

ccTLDs are one of the key actors responsible for the resolution of domain name queries when a website in their domain name zone (namespace) is requested. In addition, ccTLDs maintain a registration database, used to collect and access the contact information of domain name holders (via WHOIS). ccTLDs, as technical operators of the internet infrastructure, are not considered to be 'online intermediaries' under the current valid e-Commerce Directive. Their role is operating an essential service ('operators of essential services' under the NIS Directive) for the benefit of society.

As a key actor within the technical community of the internet, CENTR, the association of European ccTLDs such as .de or .pt, would like to provide its view on evaluating the illegality of online content. The wording of the question suggests

[1] The full questionnaire is available here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services/public-consultation

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium

Phone: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org

www.centr.org

that digital service providers are already equipped with sufficient knowledge and resources to reliably distinguish between harmful and illegal content. Such assumptions are overzealous.

Online misconduct touches upon numerous legal areas: from hate speech to slander, to intellectual property rights infringement, to child sexual abuse material. In many of these areas the border between legal and illegal activity is not clear-cut, and subject to different interpretations across the Member States. An appropriate and proportionate evaluation of the content is necessary to determine whether it is legal or not. In addition, evaluating the legal classification of given content poses a challenge to all digital services, both in terms of increased risk of liability and valid legal powers to act upon it without the involvement of public authorities.

With COVID-19, claiming that disinfectants kill the virus is legal but can be harmful (i.e. people drinking bleach), but claiming that colloidal silver can cure the virus could possibly go against national and EU legislation and thus be illegal. Purely technical operators like ccTLDs lack the legal powers, in addition to resources, and expert legal and technical knowledge to be able to establish the (il)legality of content and provide legal certainty for end-users. Nor should they be required to.

During COVID-19, ccTLDs have not encountered any significant levels of abusive behaviour within their namespaces due to a close collaboration with public authorities who do the relevant content analysis within their given powers to do so. ccTLDs are not able to provide an assessment of whether levels of harmful content have increased (in comparison to illegal content), since the illegality of content is established by public authorities who can in return mandate a corresponding technical action from ccTLDs.

The following questions are targeted at organisations.

3 What is your experience in flagging content, or offerings of goods or services you deemed illegal to online platforms and/or other types of online intermediary services? Please explain in what capacity and through what means you flag content.

3000 character(s) maximum

CENTR answer:

Country-code top-level domain registries (ccTLDs) do not host any content and no content passes through their infrastructure. ccTLDs do not have a special authority or any specific technical advantage to effectively judge the legality of content online.

ccTLDs are responsible for operating and maintaining the Domain Name System (DNS). The DNS is a well-established network control protocol at the heart of the internet infrastructure – commonly thought of as the "phone book of the internet". It provides a neutral function to translate user-friendly domain names into numeric IP addresses. ccTLDs hold information necessary for users to navigate the internet but do not store or enhance content.

As ccTLDs are technical operators that do not have control over the content of websites, they rely on close cooperation with public authorities in responding to abuse online. In estimating the real harm and risk to the public, only competent public authorities can assess whether the activity on a website is illegal or not and has the mandate to act accordingly.

As such the content eventually needs to be flagged to public authorities. In most Member States we notice a range of different notification channels. This often makes it difficult for the consumer to identify the correct notification

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

channel. CENTR, the association of European ccTLDs such as .de or .pt, believes a harmonised approach towards notification procedures by consumers to public competent authorities across the EU would be most helpful.

Each ccTLD registry has adopted its own policies and processes to ensure they are acting as responsible actors within the internet ecosystem. The approach of each ccTLD registry differs to reflect their size, type of organisation, relationship with their government and expectations of their local internet community, in addition to the limits of national jurisdiction.

While they have limited options, some ccTLDs are proactively addressing criminal activity and so-called technical or "infrastructure abuse" (e.g. algorithmically registered botnets, malware, phishing, etc). There is no universally accepted definition of what constitutes infrastructure abuse, hence, the level of action taken depends on the operator.

10 What sources do you use to obtain information about users of online platforms and other digital services – such as sellers of products online, service providers, website holders or providers of content online? For what purpose do you seek this information?

3000 character(s) maximum

CENTR answer:

Country-code top-level domain registries (ccTLDs) manage a registration database that is used to collect and access the contact information of domain name holders. Access to certain registration data is managed via the so-called WHOIS protocol that allows a user to retrieve various pieces of information about a domain name. The registry collects data to be able to contact the holder in case of dispute, technical problems, changes to the Terms and Conditions (T&C), missing payments, etc. ccTLD T&C usually explicitly require the domain holder to provide correct data and contact details upon registration and keep this information up-to-date. Providing false or incorrect data may be a violation of the T&C or in conflict with national legislation and can lead to the deletion or suspension of a domain name.

ccTLDs put a lot of time and effort into the maintenance of their registration database. This not only improves the quality of the registration WHOIS data, but also may have an indirectly positive impact on less abusive behaviour online, as it is unlikely that those with bad intentions would register a domain name using their correct personal information.

The actions and practices to maintain a high-quality database depend on factors specific to the registry, such as local legislation, size of the registry, the amount of registrations processed, etc. Some notable data verification examples include:

- High level screening of the data provided upon registration, to filter out obviously-false entries;
- Automated checks of provided data (for example, email address, phone number);
- Check of legal documentation provided by the registrant, in Member States where such requirement exists;
- Random verification of registration data of already-registered domain names;
- Verification of data in case of a complaint;

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

- Cross-checks of provided data with official databases (for example, valid postal code, existing phone number, company/organisation number or national identification number if such information is required upon registration).

It is important to note that many ccTLD registries have no direct contact with an individual or a company registering a domain name (i.e. domain name holder). Where this is the case, all contact, including providing and updating the registration data, goes via the registrar.

A registrar is a company that provides domain registration services to companies and individuals, directly or via a network of resellers. The registrar is accredited by one or more registries to offer domain names under their TLD. The registrar typically handles the registration process, whilst the registry manages the TLD of the requested name.

11 Do you use WHOIS information about the registration of domain names and related information?

Yes

No

I don't know

12 Please specify for what specific purpose and if the information available to you sufficient, in your opinion?

3000 character(s) maximum

CENTR answer:

Country-code top-level domain registries (ccTLDs) predominantly have a role of data controller and/or data processor when it comes to managing the WHOIS. The legal grounds for collecting WHOIS data are in accordance with the EU General Data Protection Regulation (GDPR) and other national data protection legislation corresponding to EU law. The most common ground for data processing among ccTLDs is for the "performance of a contract". The amount and specifics of publicly available WHOIS data depends on the jurisdiction and where applicable on national legislation. The majority of ccTLDs provide some form of access to non-public WHOIS data, primarily for law enforcement purposes and to the parties identified in a court order. The personal data processed by ccTLDs is strictly limited for the purposes identified in Article 6 of the GDPR.

The following questions are targeted at online intermediaries.

D. Transparency and cooperation

1 Do you actively provide the following information (multiple choice):

Information to users when their good or content is removed, blocked or demoted

Information to notice providers about the follow-up on their report

Information to buyers of a product which has then been removed as being illegal

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

2 Do you publish transparency reports on your content moderation policy?

Yes

No

3 Do the reports include information on:

Volumes of takedowns and account suspensions following enforcement of your terms of service?

Volumes of takedowns following a legality assessment?

Notices received from third parties?

Referrals from authorities for violations of your terms of service?

Removal requests from authorities for illegal activities?

Volumes of complaints against removal decisions?

Volumes of reinstated content?

Other, please specify in the text box below

4 Please explain.

5000 character(s) maximum

CENTR answer:

Country-code top-level domain registries (ccTLDs) do not host any content and no content passes through their infrastructure. Due to their very limited technical role and lack of effective control over the availability of online content, ccTLDs cannot be considered online intermediaries under the currently valid legislative framework in the EU. Nevertheless, ccTLDs are responsible actors within the internet ecosystem and are committed to contributing to a comprehensive and effective approach against illegal online content. Some ccTLDs regularly report on the amount of suspended domain names (e.g. on an annual basis) based on notifications from public competent authorities in clearly criminal cases (according to the local laws).

Hereby, it is important to note that these reports do not concern content moderation. These reports are related to domain name suspensions in clearly criminal cases, after an appropriate notification from a public competent authority responsible for the corresponding enforcement activity.

Examples include:

UK: https://www.nominet.uk/news/reports-statistics/

NL: https://www.sidn.nl/en/internet-security/transparency-report

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

5 What information is available about the automated tools you use for identification of illegal content, goods or services and their performance, if applicable? Who has access to this information? In what formats?

5000 character(s) maximum

CENTR answer:

The few country-code top-level domain registries (ccTLDs) that use automated tools to scan for potentially suspicious activity (e.g. fake webshops and/or phishing) provide regular public information about the use and effectiveness of these tools. These results are often presented in the form of publicly available research papers, public speaking commitments at different industry events and multistakeholder fora (e.g. ICANN, RIPE meetings), annual transparency reports, and/or informational resources (blog posts and FAQ) on ccTLD websites.

6 How can data related to your digital service be accessed by third parties and under what conditions?

Contractual conditions

Special partnerships

Available APIs (application programming interfaces) for data access

Reported, aggregated information through reports

Portability at the request of users towards a different service

At the direct request of a competent authority

Regular reporting to a competent authority

Other means. Please specify

7 Please explain or give references for the different cases of data sharing and explain your policy on the different purposes for which data is shared.

5000 character(s) maximum

CENTR answer:

Country-code top-level domain registries (ccTLDs) maintain authoritative name servers on the internet that hold DNS information about a particular domain. Each ccTLD maintains authoritative name servers for their managed TLD(s). Every authoritative name server provides information about all the delegations and complete DNS information (including IP addresses) about the section of the domain that is not delegated, which is called a zone. The DNS information provided by an authoritative name server on the internet is contained in a text file, called a zone file. In order for the domain-related services to be found on the internet and to be used, information about them must be in the zone file.

In addition to the information from the authoritative nameservers, ccTLDs also maintain the registration data (i.e. accessible via the WHOIS protocol).

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

The access to zone files is governed by each ccTLD, according to their own policies and needs from their local internet communities (incl. law enforcement agencies, governments and end-users). Some ccTLDs provide public access to their zone files (incl. as open data), others upon special agreements with interested parties (e.g. licences). APIs used for providing access to zone files also depend on the ccTLD but in any case, all of the APIs common amongst ccTLDs are based on open standards (e.g. AXFR, SFTP, HTTPS etc).

Some ccTLDs share the lists of newly-registered domain names with public authorities like CSIRTs and consumer protection authorities who examine these lists under their own authority and alert ccTLDs when suspicious activity is detected. If activity that is clearly illegal is detected, ccTLDs take action upon the notice and instruction from a competent public authority.

The WHOIS tool is an important query and response protocol within the DNS system. The WHOIS allows a user to perform a search on a given domain (or IP address) and retrieve various information about its registration. Access to WHOIS is governed by the GDPR, as the WHOIS database contains personal information. Hence publicly available WHOIS information is redacted due to the GDPR. The vast majority of registries provide some form of access to non-public WHOIS. In most cases, access is provided via email for individual requests. Access is available to law enforcement, to parties identified in a court order and parties with 'legitimate interest' according to the GDPR. When providing access based on 'legitimate interest' it is most commonly the legal department that makes the judgement. When responding to individual WHOIS access requests, most ccTLDs respond within 1 - 3 days.

The following questions are open for all respondents

2. Clarifying responsibilities for online platforms and other digital services

5 How should the reappearance of illegal content, goods or services be addressed, in your view? What approaches are effective and proportionate?

5000 character(s) maximum

CENTR answer:

Removing illegal content from the internet is the only effective way to avoid content being accessed and consumed. Two parties have direct access to the content or the device that stores the content: the content publisher and the hosting provider. They should be the first to be contacted.

Where a domain name is used to facilitate access to content, the domain name holder may be the provider of the content and hosting, or be able to identify the provider. The country-code top-level domain registry's (ccTLD) authoritative database has information on all domain names registered under its TLD and may help to identify and contact the domain holder. The registry's database typically contains amongst other information on the domain holder, the domain registration (e.g. date of expiry) and the nameserver addresses related to the domain name.

When it is not possible to remove illegal content from the internet, which is the only effective solution, one might try to make it more difficult for users to find or access the content. On a ccTLD level, deleting or suspending a domain name is the only measure available for registries. The problem with measures at DNS level that are primarily targeted at tackling illegal content is that deleting or suspending a domain name may make it more difficult to find illegal content on the internet but does not solve the issue or the crime, as the content remains available for those who

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

want to find it. Providers of illegal content can anticipate suspension action at ccTLD level and can take precautionary measures to further reduce the effect of the measure: a content provider, for example, might register multiple domain names under the same TLD or under different TLDs in different jurisdictions and let them all resolve to the same content under one or more IP addresses.

Deleting or suspending a domain name has an effect on all services that are reachable under the domain name and its subdomains: e.g. suspending the domain name of a social network will impact all users, not only those who uploaded illegal content. In addition, other services like e-mail also stop working. The technical ease with which domain names can be suspended and deleted raises the risk of over enforcement. The suspension of an entire domain name can have a drastic impact on businesses, institutions and public services that rely on the infrastructure provided by ccTLDs.

Therefore, taking action at DNS level and in connection to a domain name when illegal content is involved should always be the measure of last resort, when all other more effective means have been exhausted and the situation is a matter of urgency, after being assessed so by the competent public authority.

6 Where automated tools are used for detection of illegal content, goods or services, what opportunities and risks does their use represent as regards different types of illegal activities and the specificities of the different types of tools?

3000 character(s) maximum

CENTR answer:

Automated detection systems to proactively seek for online abuse by country-code top-level domain registries (ccTLDs) are not panacea. If reputational feeds and blacklists from security companies are used for these automated detection systems, it is inevitable that some type of false positives can occur when legitimate domain names are flagged as suspicious. Therefore, human oversight is necessary and especially before the action on the infrastructure level is made (e.g. suspension or deletion of a domain name) to avoid disproportionate consequences for domain name holders.

Other proactive detection systems used within a few country-code top-level domain registries (ccTLDs) are used to crawl the domain name zone to seek out potentially abusive trademark infringements (e.g fake webshops). However, the tools used need to be constantly adapted as counterfeiters learn to circumvent these automated checks and adapt to the detection methods.

Additionally, close cooperation with competent authorities is necessary to verify whether the detected website is in fact malicious, as ccTLDs are not able to judge whether any content is in fact illegal. In the cases of using automated detection systems for identifying malicious content by ccTLDs, the actual suspension of a domain name is often performed by registrars. ccTLDs can only suspend a domain name in case of clearly criminal and unlawful content, as determined by court and other public authorities, in times of emergency and if all other available means have been exhausted (e.g. contacting the content provider and/or the hosting service provider, and/or the registrar who has the direct contractual relationship with the domain holder).

As a result of the limited effectiveness of these automated tools, their use and availability is very limited across the TLD industry.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

8 What would be appropriate and proportionate measures that digital services acting as online intermediaries, other than online platforms, should take – e.g. other types of hosting services, such as web hosts, or services deeper in the Internet stack, like cloud infrastructure services, content distribution services, DNS services, etc.?

5000 character(s) maximum

CENTR answer:

Country-code top-level domain registries (ccTLDs) are not considered to fall under the notion of 'online intermediary' under the currently valid legal framework in the EU, due to their technical nature and relationship towards the availability of content online. Unlike the purely technical intermediaries referenced in the e-Commerce Directive (ECD) as 'mere conduit' providers, at no point in time is content transmitted through the internet infrastructure managed by ccTLDs. Hence, any activities that ccTLDs might take in connection to illegal content linked to the domain name managed under their TLD, are based on ccTLDs' relevant policies and Terms and Conditions (T&C), derived from the national context and applicable jurisdiction.

National legal frameworks define which content is illegal, who has been given the authority to deal with it and which processes are permissible within the rule of law. Furthermore, ccTLDs have different requirements regarding who can register domain names. The combination of these requirements and the national legal framework influences what policies and initiatives the ccTLD develops to approach the issue of illegal content.

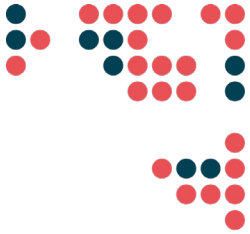
Close collaboration with law enforcement authorities and competent public authorities is of paramount importance to ensure that the essential service of maintaining the critical internet infrastructure is not disproportionately disrupted. As ccTLDs have no control, nor any more insight into online content than any other individual or an organisation surfing the web, most of the time making drastic changes to the internet infrastructure, like the DNS, in order to tackle illegal content (available via URL) is a disproportionate measure to respond to the availability of such content online.

Removing illegal content from the internet is the only effective solution that avoids the content being consumed and further distributed. It can be achieved by either deleting the content from the device on which it is stored or by disconnecting that device from the internet. Two parties have direct access to the content or the device that stores the content: the content publisher and the hosting provider.

ccTLDs only have one available measure to do anything about a domain name, and thus all services connected to the domain name, e.g. email address, all connected subdomains etc: the suspension of a domain name, i.e. its removal from the DNS. Any decision to delete or suspend a domain in connection to the content available on the website linked to the domain name should take into consideration all the consequences and balance with proportionality. The EU Consumer Protection Cooperation (CPC) Regulation clearly states that ordering ccTLDs to delete domain names should only be considered "where no other effective means are available to bring about the cessation or the prohibition of the infringement[...] and in order to avoid the risk of serious harm to the collective interests of consumers." For the legal clarity of operators, the foundation established by Article 9(4)(g) CPC Regulation should be maintained.

Some ccTLDs have established relationships with their domestic law enforcement agencies (LEAs) and/or national CERTs to improve trust and security in their ccTLD by expeditiously deleting or deactivating domain names which are used for criminal purposes, per special agreement or a procedure under the national legislation. A few ccTLDs have also developed automated detection systems to proactively monitor newly-registered domain names for potentially suspicious activity, incl. based on reputational feeds and third-party blacklists for "infrastructure abuse" (e.g. algorithmically registered botnets, malware, phishing). However, it is important to note that the majority of ccTLDs

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org



are SMEs, some of whom primarily perform manual checks of newly-registered domain names to assess whether these conform to the ccTLD T&C (e.g. data verification checks). It is a disproportionate burden on operators of essential services to actively scan their entire zone for all potentially suspicious activity. The latter should be primarily reserved for competent public authorities to assess and mandate an appropriate action, when the illegality of content is established. "Website content abuse" is very difficult to establish for a technical infrastructure operator like ccTLDs and requires specialised knowledge and resources that ccTLDs as SMEs normally do not possess.

Therefore, any potential widening of scope of the ECD and the limited liability regime within needs to evaluate whether bringing in additional actors without effective control over the content will serve the purpose of combating illegal content online. More sector-specific and tailored legislation might be preferable to address the shortcomings derived from the potentially outdated regime, instead of focusing on actors within the internet infrastructure stack.

9 What should be rights and responsibilities of other entities, such as authorities, or interested third-parties such as civil society organisations or equality bodies in contributing to tackle illegal activities online?

5000 character(s) maximum

CENTR answer:

Some country-code top-level domain registries (ccTLDs) have put special cooperation agreements in place with specialised law enforcement agencies or other public authorities who are responsible for seeking out any illegal activity within a particular namespace (e.g. fake webshops). Based on the authorities' research, a ccTLD receives lists of registrations that may be used in a problematic way on a regular basis. For all reported registrations an in-depth verification of the registrant contact data is initiated: This can lead to the activation of a procedure for revoking a domain name in case a domain name holder does not verify their registration details in due time.

These competent authorities must have the duty and responsibility to conduct due diligence when detecting the problematic use of domain names. This in return can provide legal clarity for domain name holders who can object and provide additional information if their domain names have been wrongly flagged.

Only 4 ccTLDs (BG, CZ, DK, EE) also use state-provided solutions or private solutions for the electronic identification of registrants (depending on the availability of such solutions in a concrete Member State). Some others are currently evaluating the integration of such solutions. With the use of eID solutions, a barrier for registering a domain name for the purpose of malicious activity is created in the first step of registration.

14 In special cases, where crises emerge and involve systemic threats to society, such as a health pandemic, and fast-spread of illegal and harmful activities online, what are, in your view, the appropriate cooperation mechanisms between digital services and authorities?

3000 character(s) maximum

CENTR answer:

Since the beginning of the COVID-19 pandemic, country-code top-level domain registries (ccTLDs) have been closely monitoring the numbers of domain name registrations, especially related to COVID-19. As the managers of top-level domains without any technical control over the content of websites, ccTLDs rely on close cooperation with public authorities in responding to COVID-19 related abuse linked to the websites under specific domain names in special

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

circumstances like the health pandemic. In estimating the real harm and risk to the public, only competent public authorities can assess whether an activity on a website is illegal or not and have the mandate to act accordingly.

The cooperation mechanisms with competent public authorities depend on ccTLDs and the specifics of their local jurisdiction. Some ccTLDs share the lists of newly-registered domains with law enforcement, CSIRT, and/or consumer and health protection authorities on a regular basis. However such an approach is not always permissible under national data protection legislation.

Special agreements are also concluded with the competent authorities, e.g. law enforcement, consumer and health protection, for a swifter cooperation in addressing malicious activity associated with domain names (such as fake webshops, counterfeit goods and medicine etc).

The key to these collaboration agreements is the fact that these competent authorities assess the malicious activity connected to a specific domain name and notify a ccTLD if it is in fact malicious and requires an action at DNS level. Additionally, any liability or accountability from such a decision is also reserved for the competent public authority who does the assessment and whose responsibility it is to ensure consumer protection in the EU.

15 What would be effective measures service providers should take, in your view, for protecting the freedom of expression of their users? Please rate from 1 (not at all necessary) to 5 (very necessary).

- High standards of transparency on their terms of service and removal decisions - **5**
- Diligence in assessing the content notified to them for removal or blocking – **5**
- Maintaining an effective complaint and redress mechanism - **5**
- Diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended - **5**
- High accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users' accounts - **5**
- Enabling third party insight – e.g. by academics – of main content moderation systems - **4**
- Other. Please specify - **5**

16 Please explain.

3000 character(s) maximum

CENTR answer:

It is important to ensure that any illegal content is identified as such by impartial investigators, such as public competent authorities (e.g. courts) who have adequate powers to investigate and mandate an action from the service provider, including country-code top-level domain registries (ccTLDs), rooted within their local jurisdiction. Otherwise there is a threat of increase in the removal of lawful expression online, without due process for domain name holders. Considering the global nature of the internet and the fact that suspending a domain name will have a global and far-reaching consequence on all end-users, it is by default disproportionate to mandate changes to the underlying internet infrastructure to address the availability of specific content that might be unlawful in one Member State but not in another. Apart from issues relating to child sexual abuse, there is little international consensus on what clearly

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

constitutes illegal content that private parties should react and act upon. What is allowed in one jurisdiction may be prohibited in another. To ensure that fundamental rights and freedoms (e.g. freedom of expression) are considered, it should be the courts that decide if online content is illegal or not. In this way, the EU and Member States uphold the interest of legal certainty for private parties and individuals. When the courts decide if content is illegal or not, they also consider important principles such as proportionality and necessity, which is vital when taking action against online content.

17 Are there other concerns and mechanisms to address risks to other fundamental rights such as freedom of assembly, non-discrimination, gender equality, freedom to conduct a business, or rights of the child? How could these be addressed?

5000 character(s) maximum

CENTR answer:

To ensure that other fundamental rights (e.g. freedom to conduct business and right to a fair trial stemming from Articles 16 and 47 of the EU Charter on Fundamental Rights respectively) are adequately taken into consideration in disputes around potentially illegal content, it should primarily be the courts that decide if online content is illegal or not. In this way, the EU and Member States uphold the interest of legal certainty for private parties and individuals. It is also noteworthy that in the cases of disputes regarding striking a balance between two or more competing fundamental rights, it is primarily a task for the courts.

Suspending a domain name in relation to website content is a disproportionate measure taken at the level of the internet infrastructure and before resorting to this measure, an appropriate balancing act needs to be made. Suspending the domain name of a social network or blog site where individual users can post their own content or create a personal blog will impact all end-users; not only those who posted illegal content but also all those who posted their personal pictures, expressed a political opinion, businesses that use the site for promotion and e-commerce, etc. When suspending a domain name, all services linked to the domain name, for example email, immediately stop working. Therefore, suspending a domain name may have a major impact on the opportunity and right to conduct business.

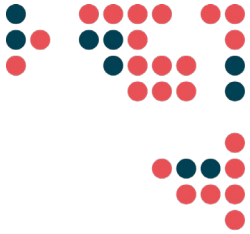
II. Reviewing the liability regime of digital services acting as intermediaries?

2 The liability regime for online intermediaries is primarily established in the ECommerce Directive, which distinguishes between different types of services: so called 'mere conduits', 'caching services', and 'hosting services'. In your understanding, are these categories sufficiently clear and complete for characterising and regulating today's digital intermediary services? Please explain.

5000 character(s) maximum

For hosting services, the liability exemption for third parties' content or activities is conditioned by a knowledge standard (i.e. when they get 'actual knowledge' of the illegal activities, they must 'act expeditiously' to remove it, otherwise they could be found liable).

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org



CENTR answer:

The E-Commerce Directive (ECD) is a cornerstone legislation for governing the freedom to provide information society services across the EU. In the last 20 years it has established several important principles for the currently valid intermediary liability framework. Country-code top-level domain registries (ccTLDs) have never been considered to fall under the scope of the ECD due to their role of operating the underlying internet infrastructure that is needed for the e-commerce services to exist.

The basic underlying idea behind the ECD and the actors it governs is the actual control over illegal content, either by virtue of actually hosting the content on its infrastructure or transmitting the content over the wire by making accidental or temporary copies of it to provide its service. All the principles codified in the ECD, including the Notice & Action procedure, are founded on this underlying principle of actual control over content. None of this happens at any point of time within the infrastructure managed and controlled by ccTLDs (i.e. the Domain Name System). Hence, even if a ccTLD is notified of potentially illegal content online, it can do nothing that effectively removes that particular content.

Before re-opening the ECD, the Commission needs to evaluate whether bringing under its scope any additional actors without effective control over the content will serve the purpose of combating illegal content online. More sector-specific and tailored legislation might be a preferable way to address the shortcomings derived from a potentially outdated regime. The existing rules need to be assessed to see if they are still fit for purpose and it is of paramount importance to retain the technological neutrality that will stand the proof of time, irrespective of new services brought to the market. The underlying principle of control over content and the notion of intermediary need to be retained, as the availability of illegal content needs to be addressed as close to its source as possible.

3 Are there elements that require further legal clarification?

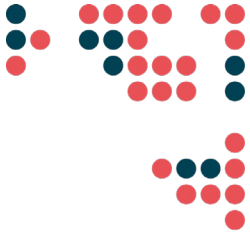
5000 character(s) maximum

CENTR answer:

There has been extensive research in the area of notifications sent to intermediaries to act upon specific content and the lack of clarity therein (so-called notice and action procedure, hereinafter N&A). It is necessary to make sure that the role of all actors within the content moderation ecosystem is assessed, and not only affects service providers: This includes 1) clarity on investigative and enforcement powers for existing competent public authorities when approaching (different) service providers with notifications; 2) the role and technology used by professional service providers in notification activity, e.g. law firms or enforcement agencies; 3) automated notifications; 4) the quality of notifications and potential consequences when the notification does not meet a particular professional standard.

The role of different service providers and their operational specifics, together with an adequate human rights impact assessment needs to be taken into consideration. Service providers differ based on their size, business model and ultimately on their technical level in facilitating the distribution of content. There should be a clear distinction between the role and ultimately the responsibilities of online intermediaries who have effective control over content on the one hand, and the technical infrastructure operators who do not transmit any content on their managed infrastructure on the other. The notification procedures should ultimately differ based on that role of intermediary and their technical and operational capacity.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org



Additionally, since notifiers are an important part of triggering the N&A procedure under the e-Commerce Directive (ECD) and subsequently the potential removal or a take-down, the question of bearing liability for over-removal by notifiers should also be considered, as the liability burden should not only be borne by service providers.

We believe that the existing valid EU legislation should guide the inception of the DSA. The existing Consumer Protection Cooperation (CPC) Regulation already envisages an appropriate tiered mechanism when approaching content that poses "serious harm to the collective interests of consumers". We believe a similar approach could also guide the N&A procedures targeted at different service providers: in exceptional circumstances, when specifically grave illegal content poses a serious and actual harm to users collectively, when no other means are available to the competent public authority, a country-code top-level domain registry (ccTLD) can be ordered to transfer a domain name to the competent public authority, upon receiving confirmation from the authority that all other means have been exhausted, including by addressing the online intermediaries with actual control over the content online (Article 9(4)(g)(iii)). As in the CPC regulation, this option should be reserved for exceptional circumstances only due to the potential disproportionate collateral damage to other services benefitting from the same infrastructure and due to the fact that the technical role of ccTLDs is significantly different from the role of online intermediaries under the ECD.

4 Does the current legal framework dis-incentivize service providers to take proactive measures against illegal activities? If yes, please provide your view on how disincentives could be corrected.

5000 character(s) maximum

CENTR answer:

Legal scholars have pointed out that the currently valid framework in the e-Commerce Directive (ECD) does not provide enough incentives for service providers to take proactive measures. Currently the notion of active nature discourages service providers from taking more preventive measures in fear of losing their safe harbour protection (this has been particularly demonstrated by legal scholars in regard to hosting service providers). The notion of the passive/active nature of intermediary service providers needs to be, therefore, further clarified to incentivise service providers to do the right thing. The 'active' role that triggers liability should most likely be transformed to a more editorial role where the service provider uses its unique role to enhance content in the context of "effective control" over that content. Any proactive measures to detect potentially illegal content should not automatically strip the service provider from its liability exemption.

In any case proactive measures should be subject to accountability and transparency provisions. No proactive measures should exist within the legal vacuum, as the overzealous removal of content should not only be avoided at all costs, but also be subject to dispute from end-users and affected parties. The affected party needs to be the first point of contact before any decision towards the ultimate goal of either blocking, removing or preventing access to content is taken by the service provider on the basis of a proactive measure. Service providers need to exercise care and due diligence when taking on proactive measures. It is also important to make sure that the possibility to take proactive measures exists outside the liability framework. Taking or not taking a proactive measure should not establish or exempt a service provider from liability when clearly illegal content is being appropriately flagged to the service provider by a competent public authority. The possibility to take proactive measures in close cooperation with a specialised authority should be promoted by the legislation via established general principles, including transparency and reversibility (if possible) of an assessment conducted outside of judiciary decision.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Furthermore, the concept of 'obtaining knowledge' that triggers the liability of a particular intermediary (relevant for hosting) should also be clarified to make sure that intermediaries are not automatically penalised for taking proactive measures in detecting potentially suspicious activity on their service. 'Obtaining knowledge' and failing to act should exist in the paradigm of a notification to and from a public competent authority. For example, obtaining knowledge of a clearly criminal activity and failing to act upon it in the context of a notification could mean the obligation of a service provider to report on the potentially criminal activity to specialised authorities when detecting such content as a result of proactive measures. If such criminal activity is confirmed by the competent authority as such, the operator is then obliged to act accordingly after being notified by the competent public authority.

It is important to maintain the decision-making over illegal content in the hands of competent public authorities, including courts, and not to shift the role of internet police towards private parties such as service providers. This situation of 'privatised enforcement' conflicts with the states' positive duty to ensure the protection of human rights in a democratic society.

Lastly, any proactive measures need to remain voluntary in their nature.

5 Do you think that the concept characterising intermediary service providers as playing a role of a 'mere technical, automatic and passive nature' in the transmission of information (recital 42 of the E-Commerce Directive) is sufficiently clear and still valid? Please explain.

5000 character(s) maximum

CENTR answer:

Recital 42 of the e-Commerce Directive (ECD) aims to provide liability exemptions for intermediary service providers that have a role of a 'mere technical, automatic and passive nature' when transmitting or storing information. An intermediary role under the ECD is primarily linked to the role of a digital service that stores and/or transmits information online, the notion of passive/active intermediation is of secondary importance when initially establishing the status of liability exemption. These principles are important when considering 'new' services to be defined as online intermediaries, based on their technical role in storing and/or transmitting information.

Legal scholars note that online intermediaries will almost necessarily have some degree of involvement in the information stored and transmitted, at least in the form of making available tools for its uploading, categorisation and display, however this is not necessarily proof of their control over the content itself. AG Jääskinen in his Opinion in the CJEU L'Oréal (CJEU, C-324/09, L'Oréal v eBay International, 12 July 2011) case suggested that "'neutrality' does not appear to be quite the right test" for evaluating liability.

Considering the fact that the scope of the DSA is to encompass all "information society services" under Directive EU 2015/1535, further clarity on the scope of the DSA is needed.

The tackling of illegal content needs to be done as close to the content as possible, as already enshrined in the ECD. A number of new digital services have emerged since the negotiation of the ECD in 1999. However, it is worth stressing that the underlying internet infrastructure that allows the internet to function in a stable, resilient and secure way predates the legislative framework. Operators like country-code top-level domain name registries (ccTLDs) are not part of new digital services that were not in place when the ECD was negotiated. On the contrary, the fact that ccTLDs have consistently been delivering a stable and secure technical service for both end-users, as well as businesses and public services consistently over 3 decades, has significantly contributed to the stability and reliability of the internet in modern society.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

ccTLDs are in favour of creating more legislative clarity for technical actors and especially for the digital services with no effective control over the availability of content online. Hence, no statutory measures should or need to be imposed for purely technical actors without any effective control over content online. To reiterate, ccTLD registries do not host any content and no content passes through their infrastructure. Therefore, ccTLDs cannot be considered as online intermediaries under the ECD.

Furthermore, this clarity would also be beneficial to all public authorities and other stakeholders that wish an appropriate remedy when their rights have been breached online. The legislation should aim to treat the problem, rather than treating the symptoms.

ccTLDs as technical actors and maintainers of a crucial part of the internet infrastructure, the Domain Name System, need to be explicitly exempted from the scope of the DSA and its potential liability rules, due to the nature of the service they provide to the information society. As operators without any control for content availability online and due to their technical nature, it is disproportionate and unnecessary to impose any content moderation obligations on ccTLDs.

6 The E-commerce Directive also prohibits Member States from imposing on intermediary service providers general monitoring obligations or obligations to seek facts or circumstances of illegal activities conducted on their service by their users. In your view, is this approach, balancing risks to different rights and policy objectives, still appropriate today? Is there further clarity needed as to the parameters for 'general monitoring obligations'? Please explain.

5000 character(s) maximum

CENTR answer:

The prohibition of the general monitoring obligation as enshrined in Article 15 of the e-Commerce Directive (ECD) is an important principle that needs to be maintained and upheld in the DSA. It has been subject to extensive interpretation by the CJEU evident from a fairly large amount of jurisprudence on the issue. The principle of prohibition of the general monitoring obligation needs to be upheld and expanded to all digital services under the scope of the DSA in order to maintain the balance between providing a digital service and enforcing public policy interests. These two tasks need to be fundamentally separated from each other.

Additionally, it is noteworthy that unfortunately, there is hardly any CJEU case law which illustrates the difference between general and specific monitoring (the latter being permissible). There have been cases where the CJEU has clearly excluded some forms of monitoring from being imposed on intermediaries - for instance the SABAM cases Scarlet (CJEU, C-70/10, Scarlet Extended SA v SABAM, 24 November 2011) and Netlog (CJEU, C-360/10, SABAM v Netlog, 16 February 2012), where the Court held that requiring intermediaries to install a filtering system would oblige them to actively monitor all the data relating to each of their customers in order to prevent the future infringement of intellectual-property rights. In the view of the court this would be general monitoring, prohibited by Article 15(1) of the ECD. AG Cruz Villalón observed in Netlog that in order to "be effective, a filtering system has to be systematic, universal and progressive." It is clear that detecting illegal content requires scanning of all content, legal and illegal alike. The same is true for the stay-down obligation. To prevent the re-uploading of illegal content, the intermediary would have to continuously ("forever"?) monitor all traffic running through its infrastructure and block illegal uploads every time. Scholars mostly agree that such processes constitute general and not specific monitoring, as in order to "recognise" unwanted content within a collection of content, logically, each piece of content in that collection must be examined. There has been no real suggestion of any other feasible method of complying with the obligation to

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

ensure the unavailability of illegal content and the stay-down obligation. Monitoring in specific cases should be interpreted quite literally: the monitoring of the activity of a specific individual or group of pre-identified users.

Furthermore, imposing any content monitoring obligations on technical operators like country-code top-level domain registries (ccTLDs) who do not have any effective control over content, nor pass or store any content through their infrastructure is meaningless. At the time of domain name registrations, typically no content is even online. Even a specific obligation to monitor domain name registrations would be counterproductive and ineffective, as content can (or cannot) appear at a much later stage.

In absence of any meaningful methods to ensure the stay-down of illegal content, no legal requirement of such type should be included in the legislation.

7 Do you see any other points where an upgrade may be needed for the liability regime of digital services acting as intermediaries?

5000 character(s) maximum

CENTR answer:

It is also noteworthy to point out the 'inequality of arms' situation when blocking injunctions concern purely technical intermediaries (e.g. Internet Service Providers (ISPs)) who fall under the 'mere conduit' liability exemption. The e-Commerce Directive (ECD) provides the opportunity to seek a court-ordered or administrative injunction against a service provider, irrespective of their liability exemption, requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it. The fact that a purely technical intermediary can be ordered to terminate or prevent an infringement in a case where the service provider is neither a defendant, nor an applicant, puts a 'mere conduit' intermediary into a peculiar position vis-a-vis Article 47 of the EU Charter and its essential element of equality of arms, where all parties need to be on equal footing. There is a lack of legal certainty in regard to the technical intermediary liability for over-blocking, as Article 12 of ECD exempts a service provider from the liability for the third-party content but not from the liability for over-blocking in case of an overly-broad injunction order. Therefore, the injunctive order should define precisely what measures the technical service providers are required to implement, without the need for technical intermediaries to exercise any discretion in a case where they do not possess enough information or capacity to conduct the balancing act. A level of minimum harmonisation in conditions of injunctions orders (including in the context of private enforcement) against technical intermediaries is needed, including such procedural safeguards as: transparency to affected parties (blocking warning should clearly indicate the party or parties which obtained the order and indicate that the affected users have the right to challenge the order), and access to effective judicial remedy to challenge the injunction order.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

VI. What governance for reinforcing the Single Market for digital services?

Main issues

1 How important are digital services such as accessing websites, social networks, downloading apps, reading news online, shopping online, selling products online in your daily life or your professional transactions? (Options: rate with 5 stars max)

- Overall - **5**
- Those offered from outside of your Member State of establishment - **5**

The following questions are targeted at digital service providers

10 Are there other issues you would consider necessary to facilitate the provision of cross-border digital services in the European Union?

3000 character(s) maximum

CENTR answer:

CENTR, the association of European country-code top-level domain registries (ccTLDs), such as .nl and .ee, supports existing EU efforts in promoting the cross-border provision of electronic identification (eID) under the currently valid eIDAS framework. Some ccTLDs are using state-provided solutions or private solutions for the electronic identification of domain name holders (depending on the availability of such solutions in a concrete Member State). By adopting eID schemes, the Member States can not only support the better provision of cross-border services across the EU, but inadvertently support the provision of more trustworthy information upon registration of domain names. The few ccTLDs that have adopted eID solutions in their registration process report that these have indirectly caused a reduction of online abuse within their namespaces. This not only improves the quality of registration data, but also may have an indirectly positive impact on less abusive behaviour online, as it is unlikely that those with bad intentions would register a domain name using their correct personal information. The EU can play a more invigorating role in ensuring support for the development of public and private eID solutions across all Member States, that can amongst other things also be used to support verification efforts of domain name holders' registration data.

11 What has been the impact of COVID-19 outbreak and crisis management measures on your business' turnover

Significant reduction of turnover

Limited reduction of turnover

No significant change

Modest increase in turnover

Significant increase of turnover

Other

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

14 Please explain

3000 character(s) maximum

CENTR answer:

The COVID-19 pandemic has forced more businesses and individuals to move online. Based on a sample of 25 ccTLDs, the number of new domains registered in April 2020 is up 20% from the same time a year earlier (according to CENTR research). At the same time, COVID-19 related registrations represented just 0.8% of all newly registered domain names across a sample of 12 ccTLDs between January and March 2020. The increased numbers of registrations are most likely explained by the growing need for businesses to move online in times when face-to-face contact is restricted.

More information available here: https://centr.org/news/blog/is-the-lockdown-driving-domain-registrations.html

The following questions are targeted at all respondents

Governance of digital services and aspects of enforcement

4 What information should competent authorities make publicly available about their supervisory and enforcement activity?

3000 character(s) maximum

CENTR answer:

Competent authorities should regularly provide public information and results of their enforcement and supervisory activity. This is important for raising public awareness and for ensuring public accountability of supervisory authorities. The reports need to provide numbers of suspended and blocked accounts, URLs etc as a result of the enforcement activities.

When restraining access to particular URLs, accounts and similar it is important to ensure that warning pages and disclaimers publicly include the reason for such access restriction, including the competent enforcement authority responsible for the action, and information on exercising the judicial remedy. End-users need to know and be informed of why particular content is restricted for them and to recourse to an appropriate judicial action against the enforcement authority responsible for content restriction.

Additionally, individuals behind the suspended accounts and blocked websites need to be able to object and provide additional information when they are being subject to enforcement activities and before the most drastic measure is taken, as their accounts and websites can be compromised without their knowledge and any wrong-doing on their behalf.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

6 In your view, is there a need to ensure similar supervision of digital services established outside of the EU that provide their services to EU users?

Yes, if they intermediate a certain volume of content, goods and services provided in the EU

Yes, if they have a significant number of users in the EU

No

Other

I don't know

7 Please explain

3000 character(s) maximum

CENTR answer:

The approach taken must be global if it is to have the effect of protecting users. If EU companies are subject to different regulatory burdens this risks penalising EU companies. The real solution to this challenge is likely to be moving partner governments globally to a shared position and CENTR members, European national country-code top-level domain registries (ccTLDs), welcome and encourage further efforts to this end.

In order to make sure that non-EU service providers are under the scope of the DSA and adhere to the EU legislation, the existing approach enshrined in the GDPR could be of guidance: i.e. an obligation to designate a representative in the EU.

8 How should the supervision of services established outside of the EU be set up in an efficient and coherent manner, in your view?

3000 character(s) maximum

CENTR answer:

All non-EU service providers providing a service to EU citizens should be required to designate an EU representative. The representative should act on behalf of the service provider and may be addressed by any supervisory authority in its country of establishment.

However, there should be an opportunity for the EU to take collective enforcement action against non-EU digital service providers in cases where the collective interests of many end-users across the EU are at stake.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

9 In your view, what governance structure could ensure that multiple national authorities, in their respective areas of competence, supervise digital services coherently and consistently across borders?

3000 character(s) maximum

CENTR answer:

Any supervision activities should be conducted as closely to the national level as possible, in order to respect the principle of subsidiarity and the need to ensure the decision-making is made as closely to the service provider and in its country of establishment. In the case of non-EU service providers, the country where the EU representative is established should also be the place for its supervision. In order to facilitate the cross-border exchange, a network of national supervision authorities, e.g. similar to a Consumer Protection Cooperation Network, could be desirable for supervision authorities to come together, exchange good practices and where needed to engage in a coordinated cross-border action.

In addition, all supervisory authorities on the national level need to be adequately resourced, staffed and financed in order for them to fulfil their duties in a most effective way. Where necessary, existing public competent authorities like consumer protection, health, data protection, ombudsperson etc need to be engaged in any additional enforcement and supervisory activities that might derive from the DSA. These need to be adequately based on their existing legal bases and reflected by additional resources assigned by the Member States.

Final remarks

Should you wish to upload a position paper, article, report, or other evidence and data you would like to flag to the European Commission, please do so.

CENTR answer:

CENTR paper on domain name registries and online content

2 Other final comments

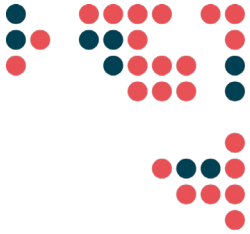
3000 character(s) maximum

CENTR answer:

To summarise:

- ccTLDs, as technical operators of the internet infrastructure are not considered to be 'online intermediaries' under the current valid legislative framework in the EU.
- ccTLDs maintain a crucial part of the internet infrastructure that underlies the provision of e-commerce and other digital services online, the DNS, yet ccTLD registries do not host any content and no content passes through their infrastructure at any point.
- Due to their limited technical role ccTLDs cannot remove illegal content, and there is little they can do to effectively respond to the availability of illegal content online, even if notified of its existence.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org



- ccTLDs, as technical actors responsible for crucial internet infrastructure, need to be explicitly exempted from the scope of the DSA and its potential liability rules. As operators without any control for content availability online, it is disproportionate and unnecessary to impose any content moderation obligations on ccTLDs.
- Actions available for ccTLDs to respond to online abuse do not remove content from the internet and require performing a drastic measure at infrastructure level that can have collateral disproportionate consequences on all end-users.
- When illegal content is linked to an underlying domain name, a valid court order is the only basis for a ccTLD to take action, as the illegality of specific content cannot be established by a ccTLD, nor any other private third party.
- In exceptional circumstances an administrative order by a competent public authority can mandate an action at ccTLD level. However, this measure can only be considered as a last resort, when all other more effective measures have been exhausted (i.e. reaching out to the content provider and hosting service provider) and there is a risk for serious harm.
- Some ccTLDs take proactive measures in order to detect and respond to 'infrastructure abuse' (e.g. malware, phishing, botnets etc). The voluntary measures taken by ccTLDs have proven to be successful against their objective. Therefore, we recommend keeping the voluntary nature of those measures.
- Cooperation with public competent authorities is of paramount importance to contribute to safety online. Specialised public competent authorities need to be adequately equipped, resourced and staffed to perform their public duties.
- Liability exemptions established in the ECD need to be maintained and where necessary, expanded to services not considered by legislators 20 years ago. The prohibition of the general monitoring obligation should encompass all digital services.
- The N&A procedure needs to be harmonised across the EU by establishing overarching general principles, such as transparency and the need to consider the liability of notifiers.
- There needs to be clear guidance for authorities, such as an adequate notification mechanism that takes into consideration the different roles and technical capabilities of service providers.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org