Council of European National Top-Level Domain Registries

Brussels, Belgium
30 March 2021

CENTR comment on the Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC

Summary of CENTR's key recommendations:

1. CENTR calls for an explicit liability exemption for the technical auxiliary function performed by DNS service providers, in the context of the provision of neutral DNS-related services for the functioning of other intermediary services.
2. CENTR calls for a clarification in the definition of illegal content. The current definition includes the vague wording 'by its reference to'. This inclusion could affect lawful reporting activities and even hamper the provision of technical auxiliary functions and, as such, could have a crippling effect on the functioning of the internet.
3. CENTR calls for an alignment of the powers given to Digital Services Coordinators with the criminal procedural law in the respective Member States, and an obligation for Digital Services Coordinators to demonstrate due diligence before resorting to exceptional powers under the Proposal.

Introduction

CENTR is the association of European country code top-level domain registries (hereinafter ccTLDs). All EU Member State and EEA country ccTLDs (such as .de, .ch, and .pt) are members of CENTR.

CENTR members are at the core of the public internet, safeguarding the stability and security of the internet as we know it today. The majority of European ccTLDs are SMEs or non-profit organisations, providing an internet infrastructure service in the interest of and in close cooperation with their local internet communities (i.e. registrars, end-users, rightsholders but also in cooperation with CSIRTs and law enforcement authorities).

ccTLDs are responsible for operating and maintaining the technical Domain Name System (DNS) infrastructure for their top-level domain. The DNS is a well-established network protocol at the heart of the internet infrastructure – commonly thought of as the "phone book of the internet". It provides a navigation function to map user-friendly domain names to numeric IP addresses. ccTLDs only hold information enabling users to navigate the internet but do not store, transmit or enhance any content online.

CENTR welcomes the aims set out by the European Commission in the DSA proposal, such as ensuring the best conditions for the provision of innovative digital services in the internal market, contributing to online safety and the

protection of fundamental rights, and setting up a durable governance structure for the effective supervision of providers of intermediary services by public competent authorities.

CENTR welcomes the attention the European Commission gives to the variety of 'providers of intermediary services', their different roles and size in the Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (hereinafter the DSA Proposal). CENTR welcomes the reinforcement of some of the core principles established by Directive 2000/31/EC (hereinafter 'e-Commerce Directive') in the DSA proposal, such as the limited liability regime and the prohibition of the general monitoring obligation that are essential for the viability of the variety of service providers online.

In order to further strengthen the aims set out above and to reinforce the aimed-for provision of innovative digital services without hampering the provision of the core digital infrastructure which is essential for the functioning of the internal market, CENTR's members would like to share the following feedback with the European Commission and the co-legislators.

1. The role of domain name registries in the light of liability exemptions

ccTLDs are only one of several internet infrastructure actors that enable users to reach content or send emails. ccTLDs enable domain names to point to an IP address on which these services (e.g. a website or an email server) are hosted. Furthermore, ccTLDs maintain a registration database that contains the names and contact details of domain name holders. Elements of this registration database are publicly accessible via the so-called WHOIS. ccTLDs, as technical operators of the internet infrastructure, are not considered to be 'intermediary service providers' under the currently valid e-Commerce Directive. Their role is to operate an essential service ('operators of essential services' under Directive 2016/1148 [NIS Directive]) for the benefit of society, as part of the digital infrastructure.

ccTLDs maintain authoritative name servers on the internet that hold DNS information about a particular domain name. Each ccTLD maintains the authoritative name server for the specific top-level domain(s) managed by that ccTLD. Every authoritative name server managed by a ccTLD provides information about all the delegations and complete DNS information of registered domain names but does not provide information on any of the services referenced by those domain names (such as websites).

A domain name and its management are distinct from, and cannot be equated with the content of any services related to the domain name, that are provided by other intermediaries (such as web hosting companies, mail service providers etc).

The DSA proposal considers that "providers of services establishing and facilitating the underlying logical architecture and proper functioning of the internet, including technical auxiliary functions, can also benefit from the exemptions from liability set out in this Regulation, to the extent that their services qualify as 'mere conduits', 'caching' or 'hosting' services. Such services include, as the case may be,[...] domain name system (DNS) services, top–level domain name registries,[...] that enable or improve the functions of other providers of intermediary services" (Recital 27).

CENTR welcomes the vigilant attention given by the European Commission to the technical auxiliary function of TLD registries in the DSA proposal and the recognition of that role to enable the provision of other intermediary services.

However, the limitation of the liability exemptions to 'mere conduit', 'caching' and 'hosting', which such technical auxiliary function providers can in principle benefit from, does not reflect the technological reality of the services provided by operators like ccTLDs.

As ccTLDs do not provide access to communication networks, do not store, nor transmit any content beyond technical DNS information through their managed infrastructure, they cannot at any point of time be considered 'mere conduit', 'caching' nor 'hosting' service providers under the DSA proposal due to the technical functioning of the DNS protocol.

None of the liability exceptions were intended to cover DNS actors, including ccTLDs, at the point of their introduction in the e-Commerce Directive. Furthermore, as ccTLDs have not been considered to be 'intermediary service providers' under the e-Commerce Directive either, while the liability exemptions have been transferred from the e-Commerce directive to the DSA almost untouched, the DSA proposal creates legal uncertainty for DNS operators, as their technical DNS-related service cannot be shielded from liability in practice, despite the opposite intention from the legislators to recognise their purely technical auxiliary function which is necessary for the provision of many other intermediary services.

This leaves technical operators like ccTLDs in a legally uncertain position, as they do not have any technical means to target specific content. They can only suspend the underlying technical infrastructure that will have a disproportionate effect on all services linked to a specific domain name, including its lawful and legitimate use. There is no way specific unlawful content can be targeted at the registry level, except for suspending the domain name together with all the services linked to it, such as Wikipedia.org or europa.eu, which would have an effect on the accessibility of the service by all end-users globally.

Additionally, the proposal for the e-Evidence Regulation (namely Article 2) recognises the specific function of internet domain name services in the context of the cross-border gathering of electronic evidence in criminal matters by considering domain name registries as part of a separate category. For the sake of uniformity, we recommend adding a similar distinction in the function categories of the liability exemptions under the DSA.

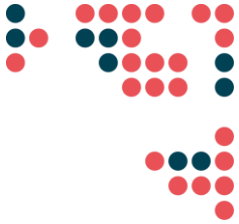
It is, therefore, of paramount importance for the objectives of the DSA proposal, as identified above, to introduce clarity on the role of ccTLDs **by introducing a fourth category for the liability exemption reserved for the technical auxiliary function of DNS providers, including ccTLD registries, that consists of a neutral function to provide DNS-related services for the functioning of other intermediary services,** and to pinpoint the location of particular content through a globally unique identifier (i.e. domain name or IP address allocation).

Finally, Chapter II of the DSA proposal is titled "Liability of providers of intermediary services'', while Recital 17 of the proposal clearly states that the intention of the DSA is not to establish liability for intermediary service providers. The chapter itself outlines the liability exemptions of specified function categories. Hence, CENTR recommends renaming Chapter II to reflect the provisions enshrined within, i.e. "Liability exemptions for providers of intermediary services".

2. Definition of illegal content

CENTR welcomes the limitation of the scope of the DSA proposal to the rules pertaining to the issues of illegal content to ensure consistency with existing EU and national legislation and for greater clarity for service providers and the wider public.

Recital 12 and Article 2(g) of the DSA proposal define "illegal content" as broadly as possible, encompassing the information relating to illegal content, products, services and activities. According to Recital 12, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that relates to activities that are illegal, such as the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the non-authorised use of copyrighted material or activities involving infringements of consumer protection law.



However, Article 2(g) defines illegal content as "any information, which, in itself *or by its reference to an activity*, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law"[emphasis added].

The definition in Article 2(g), and especially the inclusion of the vague notion of "by its reference to an activity" is unclear and could be subject to further misconception. "By its reference to an activity" can also be understood to mean that any lawful resources that refer, report or make the underlying infrastructure available, and therefore in principle refers to that content, can by default be considered illegal per se.

This overspilling effect is not desirable for the sake of legal clarity and should be abandoned. **It would therefore be appropriate to align recital 12 with Article 2(g) and clarify the Commission's intention directly in the Article** for the definition of 'illegal content'**.** For greater clarity for service providers and the general public, the definition of illegal content under the DSA proposal should reference the wrongdoing by the recipient of the service, i.e. include illegal information supplied by the recipient of the service, which, in itself **or by its reference to an activity of the recipient of the service** is not in compliance with Union law or the law of a Member State.

3. Due diligence obligations

CENTR welcomes the approach taken by the European Commission to establish a gradual set of obligations on different intermediaries, depending on their role, size and proximity to content (i.e. intermediary services, hosting services, online platforms and very large platforms).

CENTR welcomes the inclusion of minimum due diligence obligations in the DSA proposal to support a transparent and safe online environment for all online intermediaries, including the services not in the hosting category, such as services with auxiliary technical functions, including ccTLDs (Article 10 -13).

CENTR welcomes the exclusion of micro- and small enterprises from the transparency reporting obligations in Article 13 to balance the burden on service providers and the objectives set by the DSA proposal. This limitation by size should be maintained in the DSA.

4. Powers of Digital Services Coordinators

4.1 On-site inspections, search and seizure

The DSA proposal envisions the designation of one or more competent authorities responsible for the application and enforcement of the DSA in each Member State. One of these competent authorities, according to the DSA proposal, shall be a designated Digital Services Coordinator (hereinafter DSC). The DSC shall be responsible for all matters relating to the application and enforcement of the DSA in that Member State (Article 31).

Article 41 of the DSA proposal describes a list of extensive powers to be given to the DSC to investigate the conduct of providers of intermediary services. The list of these powers includes the power to require information relating to the suspected infringement, as well as almost unlimited power to carry out on-site inspections of any premises of providers of intermediary services "to examine, seize, take or obtain copies of information relating to a suspected infringement in any form, irrespective of the storage medium".

While the power to require information from an intermediary service provider is a necessary investigative power, it seems overzealous to allow a DSC to enter any premise and seize documents and information of a service provider, which is merely an intermediary and not the primary infringing party. At least such powers should be subject to the same conditions of criminal procedural law in a respective Member State concerning search and seizure by law enforcement authorities and only when the wrongdoing on the part of the intermediary service provider can be

reasonably suspected. Such investigative powers should also be subject to appropriate fundamental rights guarantees, according to the criminal procedural law in the respective Member State.

It is also worth reiterating that the purpose of the DSA is to only establish when the provider of intermediary services cannot be held liable in relation to illegal content provided by the recipients of the service. Those rules should not be understood to provide a positive basis for establishing when a provider can be held liable (Recital 17). Therefore, intermediary service providers cannot be assumed liable for the misconduct of a recipient of their services at all times, when it comes to the far-reaching investigative powers of the DSC. **These powers should be limited to requests for information as a primary means for investigation,** followed by **an opportunity to follow Member States' search and seizure procedures in exceptional circumstances, in cases of serious harm, according to the national criminal procedural law.**

4.2. Additional powers of DSC in cases of persistent infringement with serious harm

Article 41(3) states that where needed for carrying out their tasks, Digital Services Coordinators (DSC) shall also have the power to take additional measures, in respect of providers of intermediary services, where all other powers pursuant to this Article to bring about the cessation of an infringement have been exhausted, or the infringement persists and causes serious harm which cannot be avoided through the exercise of other powers available under Union or national law.

Article 41(3)(b) specifically allows the DSC, where it considers that the provider has not sufficiently complied with the requirements and the infringement persists, causes serious harm, entails a serious criminal offence involving a threat to the life or safety of persons, to request the competent judicial authority of that Member State to order the temporary restriction of access of recipients of the service concerned by the infringement or, only where that is not technically feasible, to the online interface of the provider of intermediary services on which the infringement takes place.

CENTR welcomes the limitation of these additional measures, potentially involving the temporary restriction of access of all recipients of the service, for the infringements that are particularly serious. The appropriate impact assessment must include a balancing act between the serious harm of the infringement and disabling access to a service that can affect the legitimate use of that service by all or several end-users, which should not be taken lightly and should remain under appropriate judicial oversight.

It is important to ensure that such requests for orders disabling access, even temporarily, do not result in disproportionate harm and damage to unsuspecting end-users, businesses and anyone else who relies on that intermediary service in their everyday life. Therefore, it is essential to ensure that proper due diligence is also conducted on the part of the DSC, before resorting to such exceptional measures.

The DSC should be obliged to demonstrate that all other powers available under the DSA and other Union or national laws have been exhausted before resorting to the measure of requesting a judicial order under Article 41(3)(b) and inciting feedback from the intended addressee(s) and any other third party demonstrating a legitimate interest. Such requirements would also mitigate the risk of overburdening judicial authorities with pre-emptive or premature orders from DSC authorities.

Conclusion

To reiterate the points indicated above, CENTR's members would like to put forward the following recommendations in the upcoming legislative debate on the DSA proposal:

- CENTR welcomes the reinforcement of some of the core principles established by the e-Commerce Directive, such as the limited liability regime and the prohibition of a general monitoring obligation that are essential for the viability of a variety of service providers online.
- CENTR welcomes the gradual approach taken by the European Commission in regard to 'providers of intermediary services', depending on their different roles, size and proximity to content online.
- CENTR welcomes the vigilant attention given by the European Commission to the technical auxiliary function of TLD registries in the DSA proposal and the recognition of that role to enable the provision of other intermediary services.
- CENTR reiterates that ccTLDs do not provide access to communication networks, do not store, nor transmit any content beyond technical DNS information through their managed infrastructure. Therefore, ccTLDs cannot at any point of time be considered 'mere conduit', 'caching' nor 'hosting' service providers under the DSA proposal due to the technical functioning of the DNS protocol.
- CENTR calls for clarity on the role of ccTLDs in the internet ecosystem by introducing a fourth category for the liability exemption reserved for the technical auxiliary function of ccTLD registries that consists of a neutral function to provide DNS-related services for the functioning of other intermediary services, in order to align the legislators' intention to enable ccTLDs to benefit from the liability exception for third party misconduct online.
- CENTR recommends renaming Chapter II to reflect the principles enshrined within, i.e. "Liability exemptions for providers for intermediary services".
- CENTR calls for a clarification of the definition of 'illegal content' in Article 2(g) that omits the vague wording and includes the clarification of "in itself and by its reference to an illegal activity of the recipient of the service".
- CENTR welcomes the inclusion of minimum due diligence obligations in the DSA proposal to support a transparent and safe online environment for all online intermediaries, including the services not in the hosting category.
- CENTR welcomes the exclusion of micro- and small enterprises from the transparency reporting obligations.
- CENTR calls for an alignment of the powers given to Digital Services Coordinators with the criminal procedural law in the respective Member States. Digital Services Coordinators should resort to requests of information from intermediary service providers as a primary means for investigation, followed by an opportunity to follow Member States' search and seizure procedures in exceptional circumstances, in cases of serious harm, according to the national criminal procedural law.
- CENTR calls for Digital Services Coordinators to be obliged to demonstrate that all other powers available under the DSA and other Union or national laws have been exhausted, before resorting to the measure of requesting a judicial order under Article 41(3)(b).