January 2021

DOT Europe Briefing: Limited Liability and the Active-Passive Question

Introduction

In its Communication "Shaping Europe's Digital Future", the European Commission announced its intention to publish new rules to deepen the Internal Market for digital services through a new Digital Services Act. Referred to as a "modern rulebook for digital service", the DSA aims to create a horizontal framework for service providers to address illegal content online.

In advance of its publication, stakeholders published their positions and asks for the DSA – many of which support the key principles of the e-Commerce Directive, such as the limited liability regime and the prohibition on general monitoring. DOT Europe is a long-standing supporter of the e-Commerce Directive, and we believe its key principles will be essential for the success of the DSA.

Though many stakeholders appear to agree with this thinking on a high level, several have very different opinions on the details. The e-Commerce Directive is a twenty-year-old piece of legislation that has been the subject of rigorous legal scrutiny and debate, and the interpretation of its principles has adapted over the years. Consequently, stakeholders now refer to their support of the "limited liability regime" and the "prohibition on general monitoring" very consistently in their positioning but mean something very different in practice.

For the DSA, DOT Europe wants to ensure that all policy-makers are well informed of the evolution of the e-Commerce Directive, how the principles of the Directive are linked, and how it currently applies to modern online services. Below we provide an overview of the purpose of the limited liability regime, a summary of some of the points of confusion around its interpretation, and concrete suggestions to clarify this framework within the DSA proposal.

Background: What is limited liability and the prohibition on general monitoring?

Articles 12-14 of the e-Commerce Directive set out the various conditions under which different categories of information society service providers (ISSPs) are exempt from liability for content provided by a third party, which the service either transmits or hosts.

Hosting providers are exempt from liability under Article 14, where they do not have "actual knowledge" or "awareness" that they are hosting illegal content or activity but do act expeditiously to remove it upon being made aware of that illegality. This places some limits on the potential liability of hosting service providers, for example to instances where they have been properly notified of the presence of illegal content/activity and have not acted expeditiously to remove it.

This limited liability regime benefits the internet ecosystem as a whole – including internet companies and users; it deters illegalities online and ensures the protection of citizens' fundamental rights. Without this regime, internet companies would be forced to monitor their services and check every piece of content or activity before it would be made visible to ensure that there would be no illegality. In an instance where the service provider suspected that content or activity may be illegal, it would be likely to prevent its upload in an effort to reduce any legal risk for itself. Consequently, users' freedom of expression and privacy rights would be seriously impaired. Such systematic monitoring would also require massive investments for internet companies, raising significant barriers to entry which would be detrimental to a healthy competitive environment and to the open internet.

For this reason, the limited liability regime is complemented by the prohibition of a general monitoring obligation under Article 15 of the e-Commerce Directive. Under Article 15, Member States cannot oblige online service providers to introduce measures that will result in blanket monitoring of the activity of users of their service, nor obliged to seek out illegal activity. This offers ISSPs additional legal certainty that is complementary to the limited liability regime, as it ensures that they cannot be obliged to monitor user activity in such a blanket way that could cause them to gain 'actual knowledge' of illegal content or activity, and therefore be held liable for it. Moreover, this provision protects users' fundamental rights by ensuring that service providers cannot be required by governments to generally monitor users' individual interactions or posts on their service, safeguarding the freedom of expression, the freedom of information, and the right to privacy online.

What is the problem?

Over the years, confusion has arisen as to the instances in which service providers, particularly hosting service providers, can qualify for limited liability. This issue stems from the CJEU's interpretation of Recital 42 of the e-Commerce Directive and how it relates to the rest of the limited liability regime - particularly Article 14[1].

The CJEU has often referred to a hosting service provider's eligibility for limited liability by reviewing its "active" or "passive" nature, as cited in Recital 42. These references have fuelled debates around the conditions upon which a host's eligibility for limited liability is based: is it the nature of the service provided, or the knowledge of an illegality that can be reasonably attributed to a service provider in a given case?

In addition, it is becoming increasingly difficult to determine when a service provider can be seen to have knowledge of an illegality, particularly when we look at more modern online services. Today, many online services organise content in some manner, to present it to the user in an understandable and engaging format – should a service provider be considered to be aware of every piece of content on its service if it takes responsibility for organising it and optimising it for presentation? What about service providers who are trying to do more to tackle illegal content and activity on their services – if they make use of content recognition tools or use key word searches to try to reduce the possibility of illegal content appearing on the service, ought they be seen to have sufficient knowledge of an illegality to such a degree that they no longer qualify for limited liability?

For the DSA debate, these are some of the key questions that stakeholders are asking about e-Commerce Directive and its place in the future online framework.

Why does it matter?

To create a DSA framework that supports innovation, provides legal certainty to businesses, and protects users online, policy-makers must take stock of the problems that need to be addressed, and be informed of the consequences of changes to the existing rules.

In this context, many stakeholders have voiced their support for the limited liability regime and the prohibition of a general monitoring obligation under the e-Commerce Directive, proactively calling for them to be maintained in the DSA. However, some of the same stakeholders are simultaneously calling for the DSA to "clarify" that both of these principles should only apply to "passive" service providers in the online ecosystem. While this position is based on the confusion linked to the active/passive distinction

[1] There is also an argument to be made that when read in its entirety, Recital 42's reference to a service provider's "passive nature" appears more likely to refer to conduit and caching services under Articles 12 and 13 of the e-Commerce Directive, see AG Jääskinen in the Opinion on Case C-324/09 - *L'Oréal v eBay*, paragraphs 138-141.

and the questions regarding knowledge outlined above, it would in fact lead to outcomes that run counter to the purpose of the e-Commerce Directive and could result in negative consequences for both users and businesses if carried forward in the DSA.

This is because the principles and purposes of Articles 14 and 15 of the e-Commerce Directive are linked – they are both designed to (a) enable the growth of digital services on the Internal Market and (b) ensure the protection of fundamental rights online. In creating this Directive, the legislator intended to allow ISSPs to supply their services without disproportionate risk of liability for the massive volumes of information they process and store. Simultaneously, service providers would never be obliged to monitor the information they transmit or store but must act expeditiously to remove that information when they obtain actual knowledge or awareness of illegal activity, thereby protecting the freedom of expression, the freedom of information, the freedom to conduct a business and right to privacy[2]. Each Article is dependent on the other, and this interrelationship needs to be kept in mind when considering how we want any new rules to apply to online services.

In a hypothetical scenario in which service providers under Article 14 are suddenly liable for the content uploaded by their users, these service providers would consequently have to check every user's post and upload for potentially illegal content or face potential liability for every user interaction on the service. If this scenario is contrasted against the purpose of Article 14: this would mean that (a) the service would face a massive challenge to grow as the cost and scale of these checks would often be insurmountable, and (b) that the service would be violating their users' rights and freedoms. This scenario can also be examined from the perspective of Article 15 - which states that a service provider should not be obliged to generally monitor its service nor seek facts or circumstances indicating illegal activity; this is to ensure that the service is not found to have potential knowledge of an illegality for every user upload on its service, ensuring that (a) it can still grow, and (b) it does not infringe on its users' fundamental rights.

We are aware that some stakeholders argue that limited liability as described under Article 14 should only apply to "passive services". We would counter that the interrelationship between Articles 14 and 15 is what demonstrates that this argument is unworkable in practice. This is because most modern services can be defined as "active", if for example "active" is defined by the fact that a service "organises" or "optimises" content in some way (even if it is done in an automated manner). Furthermore, a single provider can provide at the same time certain services which can be defined as active while otherwise proving passive services for another part of their operations. In short, there is no binary approach to the active/passive distinction for online providers. If being "active" was the only requirement necessary to fall outside the scope of Article 14, most of today's services would (a) not be able to scale for fear of liability for every user interaction and would (b) have to monitor their services in a way that ultimately impacts on their users' fundamental rights.

Similarly, in a situation in which all services "organising" content in some manner are considered to be active and thus fall outside of Article 14's protection, in practice Article 15 is made redundant – these services will be potentially liable for every user interaction, meaning that they will have to check every user's post or alternatively restrict their service offerings and offer fewer possibilities to interact on the platform (i.e. moving more towards the model of a closed online service).

For the DSA, policy-makers need to keep the relationship between Article 14 and Article 15 of the e-Commerce Directive in mind when considering different stakeholder positions and examining the new regime under Articles 5-7 of the DSA proposal. Both principles seek to strike a balance between competing interests in order to protect fundamental rights: it is not possible to make changes to one without

[2] See also Recitals 40, 41 and 46 of the e-Commerce Directive.

impacting on the other, and consequently having a broader impact on the protection of users' rights online and the development of online services in the Internal Market.

What is needed going forward?

1) *Move away from the active/passive distinction, knowledge is what matters:*

For some time, DOT Europe has argued that the active/passive distinction is irrelevant to whether a service can qualify for limited liability, while knowledge has always formed part of the Court's deliberations on this question. Moreover, we believe that the DSA is an opportunity to firmly clarify that knowledge should be the deciding factor when assessing the limited liability for an online service provider in the Internal Market.

To date, the CJEU has used a mixture of references to the passivity and/or activity of a given service, as well as what it knew or was aware of, in its overall assessment as to whether a service provider has liability in respect of a specific illegality. Take for example:

- The case of *Google France*[3]: Here when assessing whether the service provider could avail of Article 14's limited liability regime, the CJEU stated that it would be necessary to determine whether the role played by the service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, *pointing* to a lack of knowledge or control of the data which it stores.
- The case of *L'Oréal v eBay*[4]: Here the CJEU's assessment as to whether the service provider was eligible for limited liability again centred on whether it had played an active role "such of the kind" to give it knowledge of, or control over, the data stored. In its deliberations, the Court even went so far as to say that if the service provider had clearly confined itself to a merely technical and automatic processing of data in question, it could nonetheless only be exempt from liability on the condition that it has not had actual knowledge of illegal activity or information.
- The cases of *Netlog*[5] and *Eva Glawischnig-Piesczek*[6]: In both cases CJEU did not enter into a debate on whether the social networks in question were sufficiently "passive" to fall within the scope of Article 14. It stated that two criteria must be met in order to avail of the limited liability protections: the service provider must not have knowledge of the illegal activity or information, and it must act expeditiously to remove or to disable access to the information as soon as it becomes aware of it.
- The Opinion of Advocate General Saugmandsgaard Øe in the *Peterson* case[7] as a more recent comment on this subject: The Advocate General stated that limited liability does not apply only when the service provider has 'actual knowledge of illegal activity or information' or is 'aware of facts or circumstances from which the illegal activity or information is apparent' and does not act on that information, referring not to what a provider would have known had it been diligent, but to what it really knew[8].

The above cases demonstrate that the criteria of knowledge and awareness have consistently featured in the CJEU's reasoning, even where the concepts of active and passive were being considered by the CJEU.

[3] Joined Cases C-236/08 to C-238/08 *Google France*, paragraphs 112-120.
[4] Case C-324/09 *L'Oréal v eBay*, paragraphs 118-124.
[5] Case C-360/10 *Sabam v Netlog*.
[6] Case C-18/18 *Eva Glawischnig-Piesczek* v Facebook Ireland.
[7] Joined Cases C-682/18 and C-683/18 *Petersen v Google and YouTube, Elsevier v Cyando*
[8] See AG Saugmandsgaard Øe's opinion, paragraphs 169-196.

These various references have created legal uncertainty for online service providers, as it is not certain how far they can go to proactively tackle illegalities on a voluntary basis without falling outside of the scope of the limited liability regime. Rather than getting tangled in the argument of what constitutes an active or passive service, DOT Europe believes that the DSA is an opportunity to clarify conditional liability on the basis of expeditious action upon receipt of actual knowledge of an illegality. Recital 42 is arguably only applicable to the conduit and caching services falling under the scope of Articles 12 and 13 of the Directive, whose limited liability status should remain unaffected by the DSA debate.

By providing this clarity in the DSA, online service providers can be incentivised to do more to address the issues arising from the presence of illegal content on their services. In addition, oversight of these actions could be provided by some form of integrated governance structure as proposed in the DSA, which would examine the success or failure of different service providers' efforts to tackle illegalities across their services, taking a broad view of the overall systems put in place rather than reviewing specific allegations of illegalities[9].

Issues arising from specific illegalities can still be addressed in the DSA through clear and harmonised notice and action rules. Consequently we would argue that the DSA should move away from the active/passive distinction, and rather focus on clarifying the concept of knowledge and how it applies to modern online services.

2) Clarify knowledge and introduce a legal safeguard for service providers

As we demonstrate above, the knowledge standard is an essential criterion for the application of Article 14 of the e-Commerce Directive to hosting service providers.

However, this knowledge standard raises its own questions, particularly when considered in the context of modern online services and some of the technical methods employed to organise content and address possible illegalities. This is because Article 14 of the e-Commerce Directive refers to both "actual knowledge" and "awareness" of an illegality. The CJEU has also examined the knowledge standard in terms of the level of control a service provider has over the content it hosts[10].

While the concept of "actual knowledge" is somewhat clearer insofar as it refers to a specific illegal information that is brought to the attention of a service provider, it is not clear to what degree "awareness" is linked to the argument that a service provider ought to have known of a particular illegality – also known as constructive knowledge. This element of constructive knowledge raises additional uncertainties for online service providers when they are trying to introduce proactive measures to prevent illegal activity on their services, or even optimise content for presentation on their services in order to improve the user experience. For example, some service providers deploy algorithms to proactively detect illegal material or use key word searches, some collaborate with trusted flaggers, some have repeat offender policies in place or make use of human review and moderation to varying degrees, and some organise content in a visually appealing manner.

The CJEU is less clear on this subject, although its deliberations do again showcase the interrelationship between Articles 14 and 15 of the e-Commerce Directive:

- In the case of *Eva Glawischnig-Piesczek*[11], the Court ruled that an injunction applying a specific monitoring obligation (which is permitted under Article 15 of the e-Commerce Directive) might

[9] See for example DOT Europe's (formerly EDiMA) proposal for an Online Responsibility Framework.
[10] Again, see the above cases of *Google France*, *L'Oréal v eBay*.
[11] Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland*.

be imposed on a service provider to remove content which is either identical to or "equivalent" to content which has previously been declared unlawful. It is not clear how such a search might be achieved in practice, without giving rise to the question as to what a service provider can be said to be "aware of" on the service as a whole, and which might lead to the loss of a service provider's limited liability protections under Article 14.

- More recently, Advocate General Øe's Opinion on the *Peterson* case provides greater detail on the concept of "actual knowledge" vs awareness, and how it relates to the technological practices of different online service providers. Here the Advocate General highlights that optimising access to the content should not be confused with optimising the content itself – optimising access to information by providing search functions, the categorisation of information and providing automated recommendations would not be sufficient to give the service provider knowledge of the content of that information[12]. The AG also noted that a host's proactive checks to detect the presence of illegal information on its servers should not be sufficient to provide it with knowledge of the stored information[13].
- The current lack of clarity on this issue is also demonstrated by the request for a preliminary ruling in *Puls 4 TV YouTube LLC*[14], in which the referring court is seeking guidance from the CJEU as to whether steps taken by the online service provider (such as sorting, tagging and recommending content to users, and providing assistance in uploading content) are sufficient to justify its loss of the limited liability protection.

Because there is still a question mark over the degree of knowledge required to lose the limited liability protection of Article 14, this legal uncertainty actually creates a perverse incentive similar to that of the active/passive classification: service providers are cautious about implementing any voluntary measures to address illegalities, per chance that it could be inferred that they have knowledge or awareness of any illegalities on the service.

DOT Europe believes that two steps can be taken in the transposed liability regime set out in the DSA to address these concerns:

- The first would be to clarify that the standard for knowledge under Article 14 of the e-Commerce Directive – or Article 5 of the DSA proposal - relates to actual knowledge of specific information on an illegality (for example as acquired through a valid notice), rather than "abstract knowledge" or "awareness" of illegalities on a service more generally.
- The second would be to create a concrete legal safeguard, introducing a presumption that any proactive actions – technological or otherwise – taken in good faith by an online service provider would not attribute to them actual knowledge of a specific illegality on their service, such that they could lose their limited liability protection under Article 14 of the e-Commerce Directive. Article 6 of the DSA can be a starting point for this conversation.

Online service providers should be able to act proactively to address concerns regarding illegal content and activity using the best tools at their disposal, with due regard to fundamental rights. The above safeguards would provide the necessary legal certainty to service providers to act, and to account for the nuance required for freedom of speech concerns, without incentivising the censorship of legitimate content and speech.

---

[12] AG Øe's Opinion paragraph 83.
[13] AG Øe's Opinion paragraph 166.
[14] Case C-500/19 *Puls 4 TV GmbH & Co. KG v YouTube LLC.*

With this briefing, DOT Europe endeavours to showcase the complications of the case law, demonstrate the importance of the relationship between Articles 14 and 15 of the e-Commerce Directive, and identify the pressing questions that ought to be addressed by policy-makers in the DSA. As a voice of the platform economy with years of direct experience advocating on and interpreting the e-Commerce Directive, DOT Europe is in a unique position as a key stakeholder to offer this insight.

The DSA is an opportunity to get the legal framework right - to address concerns in the online space while ensuring innovative services can thrive and citizens feel protected. Going forward, we urge policy-makers to keep the delicate balance and the overall purpose of the e-Commerce Directive in mind when considering what is really needed for the future.