



Platform Liability in the EU: A Need for Reform?

2020



Platform Liability in the EU: A Need for Reform?

Table of Contents

| | |
|---------------------------------------------------------------------------------------------|----|
| Definitions | 4 |
| 1 Executive summary | 5 |
| 2 Introduction | 7 |
| 2.1 The purpose of the report..... | 8 |
| 2.2 Method..... | 8 |
| 2.3 Overview..... | 8 |
| 2.4 The context of the report..... | 9 |
| 2.4.1 Platforms and the internal market | 9 |
| 2.4.2 Platforms and sustainable development | 10 |
| 3 The regulatory framework for platform content liability in the EU .. | 11 |
| 3.1 The e-Commerce Directive..... | 11 |
| 3.2 The Copyright Directive (2019) | 14 |
| 3.3 The Audiovisual Media Services Directive (2018) | 15 |
| 3.4 The relationship and consistency between the directives | 16 |
| 3.5 Self-regulation | 17 |
| 4 A further harmonised framework for platform liability in the EU.. | 19 |
| 4.1 Evidence of fragmentation between the Member States | 19 |
| 4.2 A harmonised framework for platform liability: issues for further analysis | 24 |
| 5 A stricter level of platform liability in the EU?..... | 25 |
| 5.1 Main arguments in favour of a stricter liability | 26 |
| 5.2 Main arguments against a stricter liability..... | 28 |
| 5.3 Recommendations..... | 31 |
| Bibliography and other sources | 33 |
| Sammanfattning på svenska (Summary in Swedish) | 39 |
| Annex: Platform Liability and the e-Commerce Directive – answers from stakeholders | 41 |

Definitions

The following definitions apply for the purpose of this report.

Platforms: A platform is defined as a “*digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the internet*”.¹ The platform business model is characterised by the fact that platforms act as intermediaries between two or more types of users.² Examples include *e-commerce platforms* that match retailers and customers, *social media platforms* that match users and advertisers and *apartment sharing platforms* that match apartment owners with customers seeking short-term rentals.

Illegal content: Illegal content is defined as content that infringes European Union (EU) law or national laws in the Member States,³ including illegal offers for sale of goods and services. Falling outside the scope of the report are discussions regarding content that is not illegal but rather “harmful”, such as pornographic content. The distinction between illegal and harmful content is of course fluid and changes subject to legislative developments. To take one example, the concept of “fake news” today exists in the grey zone between legal and illegal content. Some countries are taking measures to classify “fake news” as illegal,⁴ a trend that has intensified during the COVID-19 pandemic.⁵ In this report, we will not discuss “fake news” as an issue of illegal content. This is in line with the approach taken by the Commission in the recent consultation on the Digital Services Act.⁶

Liability: When discussing the liability of platforms in this report, we are addressing under what circumstances platforms can or cannot be held liable for the content posted on the platform *by its users*. This is commonly referred to as the *secondary liability* of platforms. If the platform were to publish illegal content on its own, this would concern the *primary liability* of platforms. The primary liability of platforms falls beyond the scope of this report.

Content filtering: When discussing content filtering in this report we are referring to the use of software and algorithms to prevent, screen and remove illegal content from platforms. A common example is the ContentID system used by YouTube, which is a digital fingerprinting system to detect copyright infringements. Content filtering in a wider sense may also refer to measures taken by other actors. Examples include an internet access provider that blocks access to certain websites or a parent who uses software to block certain internet content for children. The latter issues are however not the subject of this paper.

¹ OECD (2019) p. 21.

² See Stefan Larsson & Jonas Andersson Schwarz (2018), p. 20.

³ This is also the definition used in the recommendation by the Commission on measures to tackle illegal content online. See C(2018) 1177.

⁴ Michael-Ross Fiorentino (2018).

⁵ EDRI (2020).

⁶ Commission (2020a).

1 Executive summary

This report discusses the need to reform the European Union (EU) rules on platform liability for illegal content, such as terrorist propaganda, hate speech and illegal products. In this regard, the President of the European Commission Ursula von der Leyen has called for a *Digital Services Act* that will upgrade the liability and safety rules for platforms in the EU. The purpose of this report is to outline key issues and arguments that need to be considered in the upcoming policy process. The report forms part of the work of the National Board of Trade in offering analysis to the Swedish government ahead of upcoming negotiations regarding the internal market.

The analysis presented in this report is supported by the results obtained through a questionnaire sent out by the National Board of Trade to stakeholders in December 2019 (the NBT questionnaire). The questionnaire was answered by 29 stakeholders and will be used to provide a sample of their insights. The questionnaire will not be used to draw statistical conclusions due to the relatively small sample size. The answers to the questionnaire are summarised in a document and can be found as a separate annex to this report.

The analysis in this report is divided into two parts. The first part discusses fragmentation under the current regulatory framework and potential improvements to increase *harmonisation*. The second part discusses the arguments for and against a more large-scale reform of the *level* of liability for platforms. The discussion in this latter part focuses on the need for the introduction of mandatory filtering obligations.

Analysis

In terms of *harmonisation* under the current regulatory framework, we present evidence of fragmentation between the Member States. Indeed, the national regulations have to a certain extent diverged over the 20 years since the e-Commerce Directive was enacted. To address this issue, we highlight the following issues for further analysis:

- The possibility of introducing a harmonised notice and takedown procedure across the EU, including issues such as the territorial scope of takedowns and access to justice.
- The possibility of reforming the scope of the e-Commerce Directive to account for “new services” that were not explicitly addressed in the original directive.

- The possibility of clarifying the distinction between active and passive hosting services. In this regard, the legislator may consider a clarification that good faith efforts from platforms to prevent illegal content will not lead to the loss of the liability exception.
- The possibility of clarifying the distinction between general and specific monitoring obligations, in line with recent case law.
- The possibility of clarifying the relationship between the e-Commerce Directive and other pieces of EU platform legislation, such as the Copyright Directive and the AVMS Directive.

With regard to the *level* of platform liability, there are forceful arguments for and against a reform. The situation is characterised by a complex balancing act between competing interests. This was also reflected in the answers to the NBT questionnaire, where stakeholders were divided as to the need for a large-scale reform of the rules on hosting liability. We present the following recommendations for the policy process moving forward.

First of all we stress the importance of gathering solid evidence. It is crucial that the policy process is not rushed and that proposals are based on solid empirical evidence. Examples of tools that can be used to gather evidence include regulatory sandboxes and public consultations. Second, we note the fact that illegal content is a multi-faceted problem. Some areas of content liability may be more suitable for reform than others. For example, stricter liability might be investigated with regard to child sexual abuse material and illegal goods. Finally, it is important that any reform respects fundamental freedoms, such as the freedom of expression and the freedom to conduct a business.

2 Introduction

This year marks the 20th anniversary of the e-Commerce Directive. The Directive has been a central measure to ensure the free movement of digital services in the EU. Key provisions such as the country of origin principle and the limited liability for intermediaries have paved the way for the digital economy that we see today.

In 2020, there are growing calls to update the rules. One issue that has drawn particular interest is the regulation of platform liability for illegal content, which is the subject of this paper. In this regard, Germany and France have moved forward with national legislation in the past few years. Most recently, the central parts of the French legislation on platform liability were declared unconstitutional by the French Constitutional Council.⁷ In Germany, a similar regulation has been in place since 2018.⁸ Such developments highlight the risk of emerging fragmentation and the need for a strengthened framework ensuring the free movement of platform services in the EU.

Along these lines, the Commission President has called for “[a] new *Digital Services Act [that] will upgrade our liability and safety rules for digital platforms, services and products, and complete our Digital Single Market*”.⁹ The ambition is to present a legislative proposal at the end of 2020.¹⁰

The EU legislator will be challenged to find a good balance between competing interests during the upcoming legislative process. Many believe that platforms should do more to improve safety online. Most recently, this issue has been highlighted with regard to the distribution of harmful COVID-19 testing kits, medicines and herbal drugs on some platforms.¹¹ Another example was the video of the terrorist attack in Christchurch that was livestreamed via social media.¹²

Others are equally convinced that the current regulatory framework needs to be preserved. They frequently refer to the dangers of filtering for innovation and the need to protect freedom of speech.¹³ A stricter liability would risk the removal of legal content. Examples of reported wrongful removals include war footage used by human rights groups

⁷ Aurelien Breeden (2020).

⁸ German Network Enforcement Act (2017).

⁹ Ursula Von der Leyen (2019), p. 13.

¹⁰ Commission (2020b).

¹¹ Irish Tech News (2020).

¹² David Uberti (2019).

¹³ Digital Europe (2020).

taken down in the pursuit of extremist propaganda¹⁴ and victims of abuse being blocked by word filters from describing the abuse they have suffered.¹⁵

2.1 The purpose of the report

The purpose of this report is to contribute to the debate, outlining key issues and arguments that need to be considered in the policy process. We will highlight opportunities for further harmonisation of the regulatory framework and discuss the balancing of the interests involved. The report forms part of the work of the National Board of Trade in providing the Swedish government with analysis ahead of upcoming negotiations concerning the internal market.

The report also forms part of the broader efforts of the National Board of Trade to analyse the platform economy. In this regard, the National Board of Trade has recently been designated as the Swedish agency responsible for facilitating and controlling the implementation of the EU Platform-to-Business Regulation.¹⁶

2.2 Method

The analysis in this report is divided into two main parts. We will discuss the ability of the current regulatory framework to (1) ensure a *harmonised* framework for platforms and their users across the EU and to (2) provide an adequate and proportional *level* of liability for platforms. We consider it important to separate these issues because evidence of a lack of harmonisation does not necessarily indicate a need to impose a stricter level of platform liability in the EU.

The analysis is supported by the results obtained through a questionnaire sent out by the National Board of Trade to stakeholders in December 2019 (the NBT questionnaire). The questionnaire was answered by 29 stakeholders and will not be used to draw statistical conclusions due to the small sample size. It will instead be used to provide a sample of insights from stakeholders in Sweden. The answers to the questionnaire are summarised and can be found in a separate annex to this report.

2.3 Overview

In *section 3* we will give a general description of the regulatory framework on platform liability as it stands today. We will describe the

¹⁴ National Public Radio (2017).

¹⁵ Tracy Jan & Elizabeth Dwoskin (2017).

¹⁶ Regulation (EU) 2019/1150 on promoting fairness and transparency for the business users of online intermediation services.

central legislative instruments, including the e-Commerce Directive (*section 3.1*), the Copyright Directive (*section 3.2*) and the Audiovisual Media Services Directive (*section 3.3*). We will also discuss the relationship and consistency between the directives (*section 3.4*). Finally, we will describe the different self-regulatory efforts made by the industry and the effectiveness of these instruments (*section 3.5*).

We will thereafter discuss the ability of the current framework to provide a *harmonised* framework across the EU (*section 4*). We will present some evidence for fragmentation under the current framework (*section 4.1*) and some recommendations on how to improve the situation (*section 4.2*).

We will then discuss the need for EU reform of the *level* of platform liability, in particular the introduction of mandatory filtering obligations (*section 5*). We will present arguments for (*section 5.1*) and against (*section 5.2*) such a proposal. We will conclude with recommendations for the policy process from a good governance and proportionality perspective (*section 5.3*).

2.4 The context of the report

2.4.1 Platforms and the internal market

The National Board of Trade has the task of working for a well-functioning internal market. From this perspective, platforms offer significant potential when it comes to facilitating cross-border transactions.¹⁷ Platforms can reduce the cost of selling abroad and facilitate matching between buyers and sellers.¹⁸ Swedish customers who use e-commerce platforms can find offers from small vendors across the EU. Platforms facilitate trust in transactions through tools such as payment systems, dispute resolution, rating systems and reviews.¹⁹ As mapped out by McKinsey, platforms have facilitated the rise of so-called micro multinationals, i.e. small and micro firms that start growing internationally from the very start.²⁰

To contribute to the market integration offered by platforms, the EU should provide a harmonised regulative framework. A harmonised framework could prove beneficial to many actors, including platform

¹⁷ One study found that the effect of distance on trade was on average 65% lower on eBay, indicating a positive relationship between e-commerce platforms and international trade. Andreas Lendle et al (2016).

¹⁸ See McKinsey (2016), p. 43-44.

¹⁹ Andreas Lendle & Marcelo Olarreaga (2017), p 16.

²⁰ McKinsey (2016), p. 43-55.

business users and consumers. It could also benefit smaller platform players who would have an integrated and large-scale home market.

The positive aspects of platforms highlighted above should not be interpreted as a statement that we think that platforms should not be regulated. Platforms can develop strong positions in the market that require regulation and control. What we are highlighting are the benefits and value of common regulations on the internal market. Proposals for a more harmonised framework will be discussed further in section 4.

2.4.2 Platforms and sustainable development

The Sustainable Development Goals (SDGs) were adopted in 2015 by the United Nations General Assembly. They are a collection of 17 global goals designed to provide a blueprint for peace and prosperity for people and the planet.

The connection between platform content regulation and sustainable development may not be immediately obvious. There is no single goal in the 2030 Agenda that directly addresses platforms or internet regulation. Nevertheless, there are a number of ways in which platforms can contribute either positively or negatively to the attainment of goals and targets in the Agenda. We will illustrate this point with the following fictive examples:

Example 1: Sonia starts up a business in Lithuania selling custom-made yoga pillows. To expand her business, she starts selling her products via an e-commerce platform. The platform helps her gain access to a market of hundreds of millions of consumers. This development supports reaching SDG 8 (decent work and economic growth) and SDG 5.B (enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women).

Example 2: There is an election in the Netherlands. Fabian uses a social media platform to set up a demonstration against certain legislative proposals that are being debated. At the same time, an article is distributed on the platform that wrongfully blames politicians for crimes against the population. These developments contribute both positively and negatively to the ambition of SDG 16.7 (to ensure responsive, inclusive, participatory and representative decision-making at all levels).

Example 3: Sexualised images of children are spread via an image-sharing website located outside the EU. The images are not taken down despite multiple appeals from civil society. This negatively affects the ambition of SDG 16.2 (to end abuse, exploitation, trafficking and all forms of violence against and torture of children).

As exemplified above, the regulation of content on platforms can have both positive and negative effects on the ability to realise the Sustainable Development Goals by 2030. To promote the positive aspects of platforms, it is crucial that the EU provide for a well-balanced regulatory framework that takes all the interests involved into account. The balancing of interests will be further discussed in section 5 below.

3 The regulatory framework for platform content liability in the EU

The central piece of legislation on platform content liability in the EU is the e-Commerce Directive.²¹ This is also the oldest part of the framework still in place. The Directive was enacted in June 2000 and is now 20 years old. The purposes of the Directive are to ensure the free movement of digital services between Member States and to guarantee a high level of protection of objectives of general interest.²² In recent years the framework has been complemented with rules on platform liability in the Audiovisual Media Services Directive²³ (AVMS Directive) and the revised Copyright Directive.²⁴ Below we will introduce each set of rules. We will also present the self-regulatory instruments developed by platforms.

Other pieces of EU legislation also touch upon the liability of platforms, for instance the General Data Protection Regulation²⁵ (GDPR) in relation to the processing of personal data or the EU rules on product safety in the case of illegal goods. However, these rules are not discussed further in this report because they are only indirectly concerned with the liability of platforms.

3.1 The e-Commerce Directive

The e-Commerce Directive contains the main principles governing platform content liability in the EU. These include in particular the

²¹ Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market.

²² Recitals 8 & 10 e-Commerce Directive.

²³ Directive (EU) 2018/1808 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities.

²⁴ Directive (EU) 2019/790 on copyright and related rights in the digital internal market and amending Directives 96/9/EC and 2001/29/EC.

²⁵ Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.

country of origin principle, the liability exception for hosting services and the prohibition on general monitoring obligations.

The country of origin principle

The country of origin principle applies to all “information society services”,²⁶ such as internet access providers,²⁷ cloud service providers²⁸ and platforms. The principle entails that it is primarily up to the home state of the service provider to regulate and control the services. This division of competence is important given the borderless nature of digital services, including platforms.

Nevertheless, the principle is not absolute. Other Member States can impose measures regulating information society services if the measures can be motivated with reference to public policy, the protection of public health, public security or the protection of consumers.²⁹ Derogations need to be imposed on a case-by-case basis and must be notified to the state of establishment and the Commission.³⁰ A further limitation can be found in recital 26 to the e-Commerce Directive, which states that Member States do not need to notify measures imposed under criminal law.

The principle has recently been strengthened by the ruling of the Court of Justice of the European Union (CJEU) in the Airbnb case³¹ in December 2019, where the Court held that measures derogating from the country of origin principle are unenforceable against individuals, unless properly notified to the state of establishment and the Commission.

The application of the country of origin principle to illegal content on platforms will be further discussed in section 4.2.

The liability exception for hosting services

The liability exceptions in the e-Commerce Directive are applicable to three categories of information society services:

²⁶ See Article 1 in Directive 98/48/EC. An information society service is a “service provided at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of a service”.

²⁷ A company that provides internet connections to customers.

²⁸ Can be defined as a company that offers network services, infrastructure, or business applications in the cloud.

²⁹ Article 3.4a e-Commerce Directive.

³⁰ Article 3.4b e-Commerce Directive.

³¹ See case C-390/18, Airbnb Ireland.

- Mere conduits³² (typically internet access providers);
- Caching service providers;³³
- Hosting service providers.

For platforms, the most relevant exception is the liability exception for “hosting services providers”, i.e. services that store information provided by their users. The host is not liable for content uploaded by its user when it does not have knowledge of the illegal content. After gaining knowledge of the illegal content, the host must act expeditiously to remove or to disable access to the information. This is commonly referred to as the *notice and takedown principle*.

A hosting service is defined in the e-Commerce Directive as a service that “consists of the storage of information provided by a recipient of the service”.³⁴ Naturally, this does not cover all activities carried out by platforms. For example, the liability exception does not apply when a platform publishes its own advertising or sells its own products. What is covered is the situation where a platform publishes user-generated content such as offers for sale, texts, pictures, videos and so forth.

On this topic, the CJEU has held that the activity of a hosting service is of a neutral and mere technical, automatic and passive nature.³⁵ The Court has declared that the mere fact that a platform “stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exceptions from liability”.³⁶ By contrast, when a platform provides assistance in optimising the presentation of the offers for sale and promotes these offers, it is considered to be taking an active role and cannot be qualified as a hosting service within the meaning of the e-Commerce Directive.³⁷ The distinction between active and passive host often proves a difficult balancing act for platforms, which will be further discussed in section 4.2.

³² Article 12 e-Commerce Directive. An information society service that consists of the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network.

³³ Article 13 e-Commerce Directive. An information society service that consists of the transmission in a communication network of information provided by a recipient of the service.

³⁴ Article 14.1 e-Commerce Directive.

³⁵ See case C-324/09, L'Oréal and others, para. 113.

³⁶ Ibid. para. 115.

³⁷ Ibid. para. 116.

The prohibition against general monitoring obligations

Intermediaries such as internet access providers, platforms and other hosting services often transmit large amounts of data between users. This is central to their role in the internet infrastructure. To facilitate innovation and the development of intermediary services, the e-Commerce Directive contains a prohibition against imposing general monitoring obligations.³⁸ According to the Directive, platforms and other intermediaries cannot be obliged to monitor all of their data in order to detect any illegal activities.³⁹ This prohibition is necessary to allow many platform business models to survive.

In contrast to general monitoring obligations, Member States are allowed to implement case-by-case injunctions (such as court orders) against platforms, requiring them to terminate or prevent an infringement.⁴⁰ These injunctions constitute specific monitoring obligations. The distinction between general and specific monitoring obligation has recently been subject to interpretation in the Glawischnig-Piesczek case⁴¹ in October 2019. In this case, the CJEU held that an injunction to prevent the reappearance of certain defamatory content (a *stay down obligation*) did not constitute an illegal general monitoring obligation. The case will be discussed further below.

3.2 The Copyright Directive (2019)

In the field of copyright, the liability of *content sharing platforms*⁴² is regulated in the recently revised Copyright Directive. The Directive imposes stricter liability conditions for copyright infringements compared to the e-Commerce Directive. In addition to a notice and takedown regime, the Copyright Directive requires platforms to adopt proactive measures to prevent the (re)appearance of illegal content. The Directive⁴³ requires platforms to:

1. Make best efforts to obtain an authorisation from the right holder;
2. If an authorisation is not granted, make best efforts to ensure the unavailability of the specific works for which the right holder has provided the platform with necessary information; and

³⁸ Article 15 e-Commerce Directive.

³⁹ See case C-360/10, SABAM.

⁴⁰ Recital 47 e-Commerce Directive.

⁴¹ Case C-18/18, Glawischnig-Piesczek.

⁴² Article 2.6 Copyright Directive defines an online content-sharing service provider as “a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes”.

⁴³ Article 17 Copyright Directive.

3. In any case act expeditiously when receiving a notice from the right holder to remove the notified works and make best efforts to prevent their future uploads (a stay down obligation).

In determining the level of effort required from the platform, the Directive prescribes that the regulatory authority shall take into account factors such as the size of the platform and the cost of the efforts required.⁴⁴ Member States are also obliged to provide for an exception for services that are less than three years old and which have an annual turnover below EUR 10 million.⁴⁵ The Directive additionally includes certain provisions to prevent the removal of legal content such as quotation, parody and caricature.⁴⁶

Exactly how this Directive is to be applied is currently up for debate. For example, some argue that it will be impossible for platforms to obtain authorisations for content uploaded by their users⁴⁷ and that the requirements in practice will lead to automatic filtering.⁴⁸ This has however been denied by the European Parliament.⁴⁹ A stakeholder dialogue has been held⁵⁰ and implementation in the Member States is ongoing.

3.3 The Audiovisual Media Services Directive (2018)

The AVMS Directive has recently been revised and now includes *video-sharing platforms*⁵¹ in its scope. The Directive requires Member States to adopt measures against video-sharing platforms to protect minors and the public in general from illegal content, such as hate speech and child sexual abuse material.⁵²

Exactly what these measures should comprise is left to the Member States. The Directive contains a list of possible measures including user rating, flagging and reporting options, age verification and parental

⁴⁴ Article 17.5 Copyright Directive.

⁴⁵ Article 17.6 Copyright Directive.

⁴⁶ Article 17.9 Copyright Directive.

⁴⁷ Till Kreutzer (2020).

⁴⁸ Miquel Peguera (2019)

⁴⁹ European Parliament (2019).

⁵⁰ Commission (2020a)

⁵¹ The AVMS Directive defines a video-sharing platform service as a “service [...] where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks [...] and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing.

⁵² Article 28b AVMS Directive.

control systems.⁵³ Important to note is that these measures should apply proactively to identify illegal content. They differ from the reactive approach taken in the e-Commerce Directive.

The AVMS Directive is subject to the country of origin principle and a video-sharing platform is regulated by its state of establishment.⁵⁴ The requirements imposed on the platforms shall be practicable and proportionate, taking into account the size of the video-sharing platform service and the nature of the service provided. The most dangerous content shall be subject to the strictest access control measures.

The implementation of the Directive is currently ongoing and the Commission has recently issued guidance on the definition of video-sharing platforms.⁵⁵

3.4 The relationship and consistency between the directives

As can be seen above, the directives on platform liability for illegal content adopt different approaches to the handling of illegal content online. In a simplified manner, it can be said that the e-Commerce Directive imposes certain *reactive* requirements on removing illegal content after it has been identified. In addition, the AVMS Directive and the Copyright Directive impose certain *proactive* requirements to apply before illegal content has been notified to the platform. The consistency between these approaches has been questioned in literature.⁵⁶

In particular, it is debatable whether there is a conflict between the liability regime under the Copyright Directive and the prohibition of general monitoring obligation in the e-Commerce Directive. As mentioned above, the Copyright Directive not only requires platforms to remove illegal content but also to employ “best efforts” to prevent the (re)appearance of certain illegal content. As many have argued, an obligation to prevent the (re)appearance of a certain piece of content necessitates the scanning of all content on the platform.⁵⁷ Seen from this point of view, the obligation in the Copyright Directive would appear to be in conflict with prohibited general monitoring.

The issue has however come in a different light since the ruling of the CJEU in the Glawischnig-Piesczek case. Here, the CJEU held that an injunction to prevent the reappearance of certain defamatory content (a stay down obligation) did not constitute an illegal general monitoring

⁵³ Article 28b.3 AVMS Directive.

⁵⁴ Article 28a AVMS Directive.

⁵⁵ Commission (2020c).

⁵⁶ See for example Maria Lillà Montagnani & Alina Trapova (2019).

⁵⁷ Miquel Peguera (2019)

obligation. The Court held that, even though such an obligation would necessitate the scanning of all content, it does not amount to general monitoring as long as the specific content in question has been previously declared unlawful.⁵⁸ The interpretation of general monitoring adopted by the Court may indicate that the proactive measures envisioned by the Copyright Directive will not amount to general monitoring. The requirements under the Copyright Directive concern specific content brought to the attention of the platform by right holders. The question is however still up for debate. The Polish government has challenged the obligation under the Copyright Directive as a disproportionate violation of the freedom of expression and information.⁵⁹ It remains to be seen if this challenge is successful. We believe that a revision of the e-Commerce Directive could help clarify the relationship with the Copyright Directive.

3.5 Self-regulation

The e-Commerce Directive encourages the drawing up of codes of conduct by the private sector to contribute to the implementation of the Directive.⁶⁰ We can today find a variety of self-regulatory instruments developed by platforms. These have frequently been produced at the request of the EU legislator. At the EU level,⁶¹ we have the following instruments available:

- *The Product Safety Pledge*, which is a voluntary commitment by six electronic marketplaces to take specific actions to ensure the safety of non-food consumer products sold online by third parties therein.⁶²
- *The Code of Conduct on illegal hate speech*, which entails a commitment to have rules and community standards that prohibit hate speech and put in place systems and teams to review content that is reported to violate these standards and to review the majority of the content flagged within 24 hours. Nine operators apply the code of conduct.⁶³
- *The Memorandum of Understanding on the sale of counterfeit goods*, which is a voluntary agreement between platforms, right

⁵⁸ Case C-18/18, Glawischnig-Piesczek, p. 37. This was also held to be true for “equivalent content” as long as it does not require the host to conduct an independent investigation as to the illegality of the content.

⁵⁹ See case C-401/19, Poland v. Parliament and Council.

⁶⁰ Article 16 e-Commerce Directive.

⁶¹ This is in addition to various initiatives at the national level. For more information, see SEC(2011) 1641, p. 40.

⁶² Commission (2018).

⁶³ Commission (2016).

holders and associations that lays down measures to prevent the sale of counterfeit goods. In particular, the platforms commit to have efficient and effective notice and takedown procedures and to take commercially and technically reasonable proactive measures.⁶⁴

- *The EU Internet Forum on terrorist content online*, which brings together the EU institutions, ministers, the internet industry and Interpol to work together in a voluntary partnership to address terrorist content online. The Forum aims to reduce the availability of terrorist content online and to empower civil society.⁶⁵

In 2017 the Commission commented on the effectiveness of the self-regulatory instruments, holding that the results “*show that a non-regulatory approach may produce some results in particular when flanked with measures to ensuring the facilitation of cooperation between all the operators concerned*”.⁶⁶

The EU legislator has since moved forward with certain sector-specific regulations. In its recent proposal on terrorism content,⁶⁷ the Commission emphasises the benefits and progress made concerning self-regulation in the fields of hate speech, counterfeit products and child sexual abuse. The situation concerning terrorism content is however described as being in more urgent need of reform, as self-regulation does not extend to the whole industry and terrorist content is frequently spread through smaller hosts.⁶⁸ In the context of copyright, the Commission notes that industry practices are not evolving in a suitable manner. According to the Commission, platforms are not engaging in licensing negotiations on a bona fide basis, this being one of the reasons for introducing the revised Copyright Directive.⁶⁹ As for the revision of the AVMS Directive, the proposal from 2016 notes the limited progress of the industry in protecting children from gory and violent videos and hate speech.⁷⁰

As for the horizontal framework, we are seeing growing calls for greater regulation. In the NBT questionnaire from 2019, the self-regulatory approach was in particular criticised for applying to a limited number of platforms on a voluntary basis.⁷¹ In other fora, the approach has been

⁶⁴ Commission (2011).

⁶⁵ Commission (2015)

⁶⁶ COM(2017) 555, p. 4.

⁶⁷ COM(2018) 640.

⁶⁸ SWD(2018) 408, pp. 4-5.

⁶⁹ SWD(2016) 301, p. 144.

⁷⁰ SWD(2016) 168, p. 6.

⁷¹ Annex: National Board of Trade Sweden, Platform Liability and the e-Commerce Directive – answers from stakeholders, p. 46.

criticised for being ineffective,⁷² lacking public oversight⁷³ and lacking human rights accountability.⁷⁴ The need for adopting a stricter approach to platform liability will be further discussed in section 5. Before that, we will discuss the issue of fragmentation and harmonisation under the current framework.

4 A further harmonised framework for platform liability in the EU

EU regulation in the field of platform liability not only strives to provide a proportionate and adequate standard of liability, but aims to ensure that this standard is implemented and applied with conformity across the EU. The latter aim is in fact a requirement for EU intervention to regulate the internal market. Regarding this aspect, many of the respondents to the NBT questionnaire indicated harmonisation as a key priority.⁷⁵ In the following sections we present evidence of fragmentation between the Member States and potential improvements to the situation.

4.1 Evidence of fragmentation between the Member States

As mentioned above, it is now twenty years since the e-Commerce Directive was enacted. Much has happened in the digital economy since then. New business models have emerged and large platforms have established themselves as the central actors online. Perhaps unsurprisingly, Member States have adopted different solutions to the implementation of the e-Commerce Directive. Below we will go through some of the evidence regarding the fragmentation seen between the Member States. First, we will discuss the potential of the country of origin principle to handle some of that fragmentation.

The country of origin principle: a solution to fragmentation?

The idea to facilitate the free movement of digital services on the internal market is not new. In the e-Commerce Directive, this was in particular addressed by the introduction of the country of origin principle. As mentioned above, this principle entails that it is up to the home state to regulate and control digital services. Against this background, it can be questioned whether fragmentation concerning the rules on content

⁷² Melainie Smith (2020) pp. 12-13.

⁷³ Serge Abiteboul et al (2019), p. 12.

⁷⁴ Martin Husovec (2017), p. 233.

⁷⁵ Annex: National Board of Trade Sweden, Platform Liability and the e-Commerce Directive – answers from stakeholders, p. 41.

liability for platforms is a real problem, given that platforms should in principle only be controlled by their state of primary establishment.

However, the application of the country of origin principle to liability for illegal content is not entirely simple. Recent national legislative measures in this field – the German “NetzDG”⁷⁶ and the French “Loi Avia”⁷⁷ – have ignored the country of origin principle. This fact has been questioned by the Commission, which argues that the principle is applicable.⁷⁸ In terms of case law, the CJEU applied Austrian defamation law to Facebook (established in Ireland) in the *Glawischnig-Piesczek* case without any reference to the country of origin principle.⁷⁹

Also relevant is recital 26 of the e-Commerce Directive, which states that measures under criminal law and criminal proceedings do not need to be notified under the Directive. This may indicate that the takedown of illegal content online falls outside the country of origin principle. In this regard, the Swedish law⁸⁰ on the takedown of illegal content seems to be sanctioned as part of criminal law. By contrast, the German NetzDG does not seem to be part of criminal law, but rather is sanctioned as an “Ordnungswidrigkeit”.⁸¹ In conclusion, there does not seem to be a simple answer to the application of the country of origin principle to the regulation of illegal content on platforms. This is something that should be clarified in a revision of the e-Commerce Directive.

All things considered, we believe that Member States will enforce their laws on content policy to protect users in their territories. This will be true regardless of whether the laws are enforced as case-by-case derogations from the country of origin principle or if they fall outside the principle altogether. In this situation, an important intervention from the EU would be to harmonise the procedure and legal framework for takedowns as much as possible. This would help platforms to handle takedown requests from different Member States. Below are some recommendations for harmonisation.

Notice and takedown: procedural fragmentation

As described above, the e-Commerce Directive establishes the notice and takedown principle, which requires platforms to remove or block illegal

⁷⁶ German Network Enforcement Act (2017).

⁷⁷ TRIS-notification 2019/412/F.

⁷⁸ As mentioned above, the French regulation was recently held unconstitutional, see Aurelien Breeden (2020).

⁷⁹ Case C-18/18, *Glawischnig-Piesczek*.

⁸⁰ Swedish Act (1998:112) on Responsibility for Electronic Bulletin Boards.

⁸¹ German Network Enforcement Act (2017). In Germany, an “ordnungswidrigkeit” is a violation of administrative law that is enforced by a fine.

content expeditiously when gaining actual knowledge of the illegal activity. The details of this procedure are however left to be regulated by the Member States. Key questions such as the level of knowledge that triggers liability and when a takedown should occur are not regulated by the Directive. To take one example, Germany applies a 24-hour removal limit for certain types of manifestly illegal content.⁸² The French law, which was recently declared unconstitutional, employed a 24-hour removal limit for illegal content and a 1-hour limit for terrorism content and child sexual abuse.⁸³ No such deadlines are applicable in Sweden, where the national law on responsibility for Electronic Bulletin Boards does not specify the timeframe for the takedown.⁸⁴

The fragmentation was mapped by the Commission in 2018. According to its evidence, the requirements to substantiate actual knowledge vary among Member States, with some requiring that the content is manifestly illegal whereas others require a communication or declaration of illegality from a competent authority.⁸⁵ This issue was also highlighted by one of the respondents to the NBT questionnaire, who noted that courts in different Member States (and sometimes within the same member state) apply different requirements regarding a notice to trigger “actual knowledge” for platforms.⁸⁶

In short, there is evidence that the silence of the e-Commerce Directive concerning the procedure for notice and takedown has led to fragmentation across the Member States. Through legislation and case law, Member States have adopted different solutions to notice and takedown procedures in terms of scope of application, time limits, requirements for actual knowledge, the minimum content of notices, opportunities for counter-notices and more.⁸⁷ A more harmonised approach would facilitate the role of platforms in taking down content across the EU.

A precondition for the EU legislator to be able to intervene in the procedure for notice and takedown is the existence of EU legislative competence. As mentioned in the previous section, this area is closely related to criminal law in the Member States. The EU’s competence is more limited in the field of criminal law and the EU legislator must

⁸² German Network Enforcement Act (2017).

⁸³ BBC (2020).

⁸⁴ Swedish Act (1998:112) on Responsibility for Electronic Bulletin Boards.

⁸⁵ SWD(2018) 408 p. 125-126. See also ICF (2018).

⁸⁶ Annex: National Board of Trade Sweden, Platform Liability and the e-Commerce Directive – answers from stakeholders, p. 51.

⁸⁷ SWD(2018) 408 p. 125-126.

carefully assess whether it can make use of the general internal market competence (article 114 TFEU).

The distinction between active and passive hosts

Limited liability for platforms is only available if they act as passive hosts, i.e. when the hosting is of a neutral and mere technical, automatic and passive nature. On this subject, the CJEU has given some guidance on the characteristics of a passive host, as discussed above in section 3.

Despite the guidance of the CJEU, courts in different Member States have taken different views on how to qualify platforms, as was observed by the National Board of Trade in 2015.⁸⁸ When the Commission interviewed judges from various jurisdiction in 2017, there was little consensus on what level of oversight would make a host active.⁸⁹ Recently it has been reported that courts in Member States have issued conflicting opinions on the distinction between active and passive hosts with regard to Dailymotion⁹⁰ and YouTube⁹¹. In the case of YouTube, there is a reference pending before the CJEU that may provide further clarification on whether YouTube can be qualified as a passive hosting service.⁹²

As was stressed by one stakeholder in the NBT questionnaire, the current uncertainty surrounding the active/passive distinction can provide a disincentive for platforms to adopt proactive measures to combat illegal content online.⁹³ Proactive efforts by platforms may lead to them assuming greater liability. This has prompted some to argue for liability protection for good faith efforts to combat illegal content (a good Samaritan clause).⁹⁴

The distinction between general monitoring and specific monitoring obligations

The e-Commerce Directive prohibits the introduction of general monitoring obligations on platforms and other intermediaries. The CJEU has in this respect ruled that a Belgian measure was prohibited because it required a social media site to “*actively monitor almost all the data*

⁸⁸ National Board of Trade (2015) p. 24-25.

⁸⁹ SWD(2018) 408 p. 124.

⁹⁰ Antonella Gentile (2019).

⁹¹ Laura Kayali (2019).

⁹² Case C-682/18, YouTube. On July 16th 2020, Advocate General Saugmandsgaard issued an opinion largely favouring the platforms. The AG held that Youtube and filesharing website Uploaded could be considered as passive hosts.

⁹³ Annex: National Board of Trade Sweden, Platform liability and the e-Commerce Directive – answers from stakeholders, p. 43.

⁹⁴ Ibid.

*relating to all of its service users in order to prevent any future infringement of intellectual-property rights”.*⁹⁵

By contrast, the Member States are allowed to impose “specific” monitoring obligations on a case-by-case basis through injunctions. However, where can the line be found between general and specific? In particular, can a hosting service provider be obliged to prevent the reappearance⁹⁶ of a certain piece of content, even though it necessitates the scanning of all content (*a stay down obligation*)? In this regard, fragmentation across the Member States has been observed by the Commission and others.⁹⁷ Stay down obligations have been considered prohibited in France, in contrast to Germany, where they have been applied under the doctrine of “Störerhaftung”.⁹⁸

This question was recently addressed in the Glawischnig-Piesczek ruling discussed above.⁹⁹ In this case, the CJEU approved a notice and stay down obligation for certain defamatory content, as long as the illegal content is sufficiently identified. This is also in line with recent legislative developments, in particular the new EU Copyright Directive that envisages a type of notice and stay down procedure for copyright. A revision of the e-Commerce Directive could further codify the issue, clarifying under what conditions a notice and stay down obligation is permitted.

Liability of search engines and other services

As mentioned above, the liability exceptions in the e-Commerce Directive (articles 12-14) are applicable to three categories of information society services: mere conduits (typically internet access providers), caching service providers and hosting service providers.

One issue that is not explicitly addressed in the Directive is the liability of search engines. As pointed out by one of the respondents to the NBT questionnaire, this has caused Member States to implement diverging liability exceptions for search engines.¹⁰⁰ For example, Spain and Austria have introduced different liability regimes for search engines in their implementation of the e-Commerce Directive.¹⁰¹ In the case law of the

⁹⁵ Case C-360/10, SABAM.

⁹⁶ As opposed to the first publication of illegal content.

⁹⁷ SWD (2018) 408 final, s. 10. See also Jan Nordemann (2017) p. 17.

⁹⁸ SWD (2018) 408 final, s. 10.

⁹⁹ Case C-18/18, Glawischnig-Piesczek.

¹⁰⁰ Annex: National Board of Trade Sweden, Platform Liability and the e-Commerce Directive – answers from stakeholders, p. 51.

¹⁰¹ Austrian e-Commerce Law (2001) §14. Spanish Law on information society services and e-commerce (2002) Article 17. See also SEC(2011) 1641, p. 26

CJEU, the AdWords-service provided by Google has been addressed as a hosting service.¹⁰² It remains to be seen if the automatic indexing of websites can also be seen as a hosting service for the purpose of the e-Commerce Directive.

The issue of search engine liability serves as an example of potential fragmentation in the handling of services that were not addressed in the drafting of the e-Commerce Directive. In 2012 the Commission mapped fragmentation in the classification of video-sharing services, online marketplaces, blogs and social networks.¹⁰³ In this regard, it has been argued that a revision of the e-Commerce Directive would provide an opportunity to clarify the liability of “new” business models.¹⁰⁴

4.2 A harmonised framework for platform liability: issues for further analysis

Above we have discussed some evidence of fragmentation under the current framework for platform content liability. Moving forward, the Commission and the Member States need to consider possibilities to improve the situation.

In this regard, we would like to highlight the following issues for further analysis:

1. The possibility of introducing a harmonised procedure for notice and takedown in the EU. This would also necessitate an analysis of if, and on what legal basis, the EU has competence to act. Potential issues to harmonise would be:
 - Issues such as actual knowledge, time frames, the content of a valid notification, sanctions against abusive notifications, transparency obligations and opportunities for counter-notices (to avoid over-removal). One important issue to consider would be to make it easier for users to appeal take down decisions to courts or independent tribunals.
 - The harmonisation of the territorial scope of a takedown decision. As evidenced by the Glawischnig-Piesczek case, this is not regulated by the e-Commerce Directive. If possible, it would be desirable to develop principles for this matter. A foundational principle could be that illegal content should only be removed in the Member States where it is illegal.¹⁰⁵

¹⁰² Case C-236/08, Google France and Google.

¹⁰³ SEC(2011) 1641, p. 26-30.

¹⁰⁴ Anja Hoffmann & Alessandro Gasparotti (2020) s. 26.

¹⁰⁵ In this regard, the relationship to the country of origin principle would also need to be considered.

- An even more ambitious approach would be the harmonisation of material rules on illegal content, to determine what is illegal at the EU level. Given the central function of the Member States in determining what is illegal in their territories, we do not expect such a proposal to be realistic in the near future. Content regulation often varies based on the unique cultural and historical experiences of the Member States, something that is difficult and not necessarily desirable to harmonise. It is also unclear whether the EU would have competence to harmonise given that the relevant issues often fall under the criminal laws of the Member States.
2. The Commission should also evaluate the scope of intermediary liability under the e-Commerce Directive, considering any clarifications that can be made in relation to “new” services that were not explicitly addressed in the Directive.
 3. As to the distinction between active and passive hosting services, a codification of the case law of the CJEU should be considered. A set of criteria could be introduced to facilitate the assessment for platforms and other service providers. In this respect, the legislator may also consider the introduction of a clarification that good faith efforts from platforms to prevent illegal content will not lead to the forfeiture of the liability exception.
 4. A clarification of the distinction between general and specific monitoring obligations should be considered, in line with recent CJEU case law. Clear criteria could be introduced to facilitate the distinction for Member State authorities.
 5. To avoid potential legal uncertainty, the legislator should consider clarifying the relationship between the e-Commerce Directive and other pieces of EU platform legislation, such as the Copyright Directive and the AVMS Directive (see section 3.4).

5 A stricter level of platform liability in the EU?

In the previous section, we have discussed different proposals for providing further harmonisation within the current framework of the e-Commerce Directive. The proposals have all been based on the model of notice and takedown that is in place today. In this section, we will consider the introduction of a more large-scale reform of the regulatory framework. We will examine arguments for and against removing the current notice and takedown system and the introduction of proactive filtering. This is a proposal that has recently been discussed in a study

presented to the European Parliament's Committee on Internal Market and Consumer Protection.¹⁰⁶

A filtering obligation would require platforms to adopt software to proactively scan content. This is considerably stricter than the current system where platforms only have to act upon notifications. A filtering obligation is of course not the only policy option available. A nuanced policy process would also consider lighter proactive duties on platforms, such as requirements in terms of flagging and rating of content as well as modifications of terms and conditions and transparency in content moderation. We have chosen to focus on the issue of introducing proactive filtering because it is likely to prove the most contentious issue in the process moving forward.

5.1 Main arguments in favour of a stricter liability

The scale and harm of illegal content online

A central argument in favour of a higher level of accountability for platforms is the vast amount of illegal content which is posted on platforms today. This was also highlighted by stakeholders in the NBT questionnaire from 2019.¹⁰⁷ In this respect, the numbers speak for themselves. During the period of January through June 2019, Twitter suspended 115,861 unique accounts for promoting terrorism.¹⁰⁸ In the last quarter of 2019, YouTube removed 931,438 videos for infringing their policy on child safety.¹⁰⁹ During the third quarter of 2019, Facebook took action against 7.0 million pieces of content for violating their policy on hate speech and 11.4 million pieces of content for violating their policy on child nudity and the sexual exploitation of children.¹¹⁰

Considering these numbers, it can be argued that a system of automatic filtering and removal of illegal content should be imposed on platforms as a matter of necessity. A counterpoint would be that the numbers above indicate that the self-regulation of platforms is effective.

The numbers cited above are from the big platforms, yet illegal activity can be prominent on smaller websites as well. This was highlighted by one respondent to the NBT questionnaire, explaining that the issue of child sexual abuse is problematic on smaller platforms and image hosting

¹⁰⁶ Melanie Smith (2020).

¹⁰⁷ Annex: National Board of Trade Sweden, Platform Liability and the e-Commerce Directive – answers from stakeholders, p. 43.

¹⁰⁸ Twitter (2019).

¹⁰⁹ Google (2019).

¹¹⁰ Facebook (2019a).

websites that lack the ambition to identify and remove illegal content.¹¹¹ From this point of view, it can be argued that a stricter liability should also be applicable to smaller platforms.

The situation is further aggravated by the fact that even a small amount of illegal content can cause a lot of societal harm in a short period of time. Examples include the video of the terrorist attack in Christchurch that was livestreamed on Facebook¹¹² and instances of child exploitation being livestreamed on YouTube.¹¹³

The issue of illegal products on e-commerce platforms has received particular attention during the current COVID-19 pandemic. On this issue, it has been reported that e-commerce platforms are failing to quickly remove potentially harmful COVID-19 testing kits, medicines and herbal drugs. Average removal times range between two and five days, with some products being left up to two weeks.¹¹⁴ The issue of dangerous products was also highlighted by one of the respondents to the NBT questionnaire, pointing out the repeat occurrence of toys with phthalates being made available on e-commerce platforms in Denmark.¹¹⁵ In addition to the individual harm caused, this can compromise consumers' trust in platforms and e-commerce in general.

The difficulties in targeting the primary wrongdoer

Another argument in favour of an extended liability for platforms is connected to the difficulties involved in targeting the primary wrongdoer, whether this be the creator or the consumer of illegal content. The volume of infringements, as described above, renders enforcement very costly. This issue is made even more difficult by the problem of obtaining information from the internet access providers to be able to identify the wrongdoers. Regulations to facilitate access to customer data from internet providers can also run into legal troubles from a privacy point of view.¹¹⁶

Finally, there are methods that online wrongdoers can use to hide from justice, including the use of encryption, anonymity networks (such as

¹¹¹ Annex: National Board of Trade Sweden, Platform Liability and the e-Commerce Directive – answers from stakeholders, p. 46.

¹¹² David Uberti (2019).

¹¹³ Isobel Asher Hamilton (2018).

¹¹⁴ Irish Tech News (2020)

¹¹⁵ Annex: National Board of Trade Sweden, Platform Liability and the e-Commerce Directive – answers from stakeholders, p. 46. The respondent here refers to a test by the Danish Consumer Council in June 2019 that revealed toys with high levels of phthalates on large e-commerce platforms.

¹¹⁶ See for example case C-203/15, Tele2 Sverige, where the Swedish law on data retention was declared to be in conflict with the Directive on Privacy and Electronic Communications and the EU Charter of Fundamental Rights.

Tor)¹¹⁷ and Virtual Private Networks (VPNs).¹¹⁸ These and other issues – including the territorial limitations of national enforcement authorities – can make online enforcement difficult and provide an argument in favour of targeting the platforms which are often easier to find and have the resources to provide compensation for the damage caused.¹¹⁹

The social and economic responsibility of platforms

Another argument highlighted by some of the respondents to the NBT questionnaire was the social responsibility of platforms.¹²⁰ This argument focuses on the central role of platforms in our society and democracy. Content posted on platforms can have profound influence on the democratic process, elections and public debate.¹²¹ Proponents argue that platforms need to assume greater responsibility for illegal content given their central role as regards to democracy, freedom of expression and the market. As a result, some draw parallels with traditional media companies – which are governed by public law – and argue that platforms should also be subject to public law regulations.¹²²

In a similar vein, it can also be held that platforms should take on more responsibility given that they are ultimately the creators and beneficiaries of the forums that enable the spread of illegal content.¹²³ These forums benefit the platforms financially and so the latter should take responsibility for the content that is spread. A stricter liability could also potentially increase trust in e-commerce platforms, with possible advantages for trade.

5.2 Main arguments against a stricter liability

The issue of collateral censorship

One of the most common arguments against increased platform liability is the issue of “collateral censorship”.¹²⁴ This refers to the risk that platforms, in trying to avoid liability, will use filtering systems to remove

¹¹⁷ Tor is a free and open-source software for enabling anonymous communication. Tor directs Internet traffic through a worldwide network to conceal a user’s location and usage.

¹¹⁸ A VPN connects a user’s device to another computer (called a server) and allows the user to browse the internet using that computer’s internet connection while masking their identity.

¹¹⁹ See Sartor (2017) p. 10.

¹²⁰ Annex: National Board of Trade Sweden, Platform Liability and the e-Commerce Directive – answers from stakeholders, p. 43.

¹²¹ See for example Schibsted (2019).

¹²² Smith (2020 pp. 15-17.

¹²³ Sartor (2017) p. 11.

¹²⁴ “Collateral censorship occurs when the state holds one private party A liable for the speech of another private party B, and A has the power to block, censor, or otherwise control access to B’s speech”. See Jack Balkin (2014).

an increasing amount of legal content. This issue was raised by a number of respondents to the NBT questionnaire.¹²⁵

The issue stems from the fact that the cost for a platform to remove a potentially illegal piece of content is much lower than the cost it may face by leaving the content online.¹²⁶ When doubt arises over legality, the platform has an incentive to remove the content rather than to keep it up.

The issue of collateral censorship is present under the notice and takedown system today¹²⁷ but it would arguably become even more common under a stricter liability regime.¹²⁸ If platforms were required to use content filters, wrongful removals would occur automatically rather than after a user notification. As highlighted by one respondent to the NBT questionnaire, filtering systems for identifying issues such as hate speech are still at an early stage of development.¹²⁹ A filter that understands context, history, spoken cues and replicating human judgment is not yet available. An example of wrongful removal by filter is when war footage used by a human rights group is taken down as extremist propaganda.¹³⁰ Another example is victims of abuse being blocked by word filters from recounting the abuse they have suffered.¹³¹

Filtering may also hinder legal trade through automatic removals. With regard to intellectual property (IP) rights, false copyright claims (or “Copyfraud”) have been reported as a very pervasive practice with false claims in the millions,¹³² and some fear that the issue will become even more problematic through automatic removals under the revised Copyright Directive.¹³³

Finally, as pointed out by one respondent to our questionnaire, it is worth noting that the issue of collateral censorship and filtering can be seen in a different light depending on the type of illegal content concerned. Some types of illegal content (for example child sexual abuse) are easier to detect by filter because they are illegal in all contexts. With regard to e-

¹²⁵ Annex: National Board of Trade Sweden, Platform liability and the e-Commerce Directive – answers from stakeholders, p. 52.

¹²⁶ Ibid.

¹²⁷ See for example Sharon Bar-Ziv & Niva Elkin-Koren (2018), “Analysis of the data reveals that the N&TD procedure has been extensively used to remove non-infringing materials, and most removal requests pertained to allegedly inaccurate, defamatory, or misleading content”.

¹²⁸ Giovanni Sartor (2017) p. 14.

¹²⁹ Annex: National Board of Trade Sweden, Platform Liability and the e-Commerce Directive – answers from stakeholders, p. 48.

¹³⁰ National Public Radio (2017).

¹³¹ Tracy Jan & Elizabeth Dwoskin (2017).

¹³² Jason Mazzone (2006).

¹³³ Marion Goller (2019).

commerce platforms, the issue of “censorship” instead concerns the wrongful removal of legal business offers. From this point of view, the harm is to the freedom to conduct a business and consumers’ access to goods and services.

The private enforcement of platforms

The unique position of platforms to control content online has made them essential in combatting illegal content. Platforms are increasingly assuming the role of private law enforcers in the online sphere. This can be seen as problematic because in contrast to public law enforcement, platforms are not under an obligation to be impartial and transparent. They do not necessarily act in the public interest nor are they necessarily equipped to deal with weighing public interests. This issue was raised by some stakeholders in the NBT questionnaire.¹³⁴

In this regard, the organisation European Digital Rights (EDRi) has indicated that the content moderation practices of platforms often disproportionately affect groups such as LGBTQI+¹³⁵ communities, women, migrants, people of colour, religious and ethnic minority groups, human rights defenders, journalists, artists and political activists.¹³⁶

Against this background, it can be argued that we should be cautious before putting even more responsibility on platforms. A counterpoint to this argument would be that it is hard to imagine the public sector being up to the task of enforcing norms online given the scale of the problem. A more moderate option could be the introduction of more public oversight over takedowns such as the facilitation of appeals to a public authority. On this subject, EDRi argues that regular courts in most EU countries are overwhelmed with content moderation cases from big social media platforms. Instead, they wish to see the introduction of specialised tribunals.¹³⁷ Adopting a private sector approach, Facebook has in this regard introduced an independent oversight board for content moderation to improve accountability and impartial decision making.¹³⁸

The cost of filtering solutions

Another issue with imposing a stricter responsibility on platforms is the cost it will entail. As mentioned by one respondent to the NBT

¹³⁴ Annex: National Board of Trade Sweden, Platform Liability and the e-Commerce Directive – answers from stakeholders, p. 46.

¹³⁵ Lesbian, gay, bisexual, transgender, queer and intersex, with the plus representing other sexual identities.

¹³⁶ EDRi (2020) p. 10.

¹³⁷ EDRi (2020) p. 5.

¹³⁸ Facebook (2019b)

questionnaire, filtering solutions can be expensive to develop or license.¹³⁹ In this regard, it has been reported that the advanced ContentID system created by Google cost 60 million USD to develop¹⁴⁰ while Soundcloud spent more than 5 million EUR developing its own filtering system.¹⁴¹ Third-party filters such as Audible Magic have been recommended as cheaper alternatives.¹⁴² However, others have reported that the cost of third-party filters will increase significantly as a platform grows.¹⁴³

One concern with the cost of filtering systems is that they may cement current market positions by creating a barrier for newcomers to enter the market. This may lead to a decrease in competition and an opportunity for dominant actors to abuse their position and monopolise innovation.

5.3 Recommendations

From a good governance and proportionality perspective, it is difficult to give a clear answer on whether there is a need to horizontally impose a stricter standard of liability such as a filtering obligation on platforms. There are credible and forceful arguments on both sides of the debate. This was also reflected in the answers to our questionnaire, as stakeholders were divided as to the need to reform the rules on hosting liability. Ultimately, where the balance should be placed is a political decision. If the legislator were to choose to further investigate the issue, we would recommend the following:

1. *Evidence-based:* Given the difficult balancing act described above, it is crucial that any proposal is built on a solid foundation of evidence. We consider it important that time is given to design and analyse proposals. From this point of view, the ambition of the Commission to present a proposal during fourth quarter of 2020¹⁴⁴ might be an overly narrow time frame. Other measures to inform the policy process could include:
 - a. A thorough analysis of the current self-regulatory approach, highlighting the problems identified. We think that a clear problem definition would benefit the policy process moving forward.

¹³⁹ Annex: National Board of Trade Sweden, Platform Liability and the e-Commerce Directive – answers from stakeholders, p. 48.

¹⁴⁰ Google (2016).

¹⁴¹ Evan Engstrom & Nick Feamster (2017) p. 23.

¹⁴² SWD(2016) 301, p. 152.

¹⁴³ Evan Engstrom & Nick Feamster (2017) pp. 22-23.

¹⁴⁴ Commission (2020b).

- b. Regulatory sandboxes¹⁴⁵ (real or artificial), whereby a stricter liability/filtering is imposed on an experimental basis, evaluating the results.
 - c. A thorough public consultation, giving empirical evidence on the need for change.
- 2. *Specific*: The issue of illegal content is a multifaceted problem covering many different areas of the law.
 - a. Different types of content have different characteristics and pose diverse risks to society. Some types of illegal content are easier to detect through filtering than others. Examples of content that might, from a proportionality perspective, be more suitable for general monitoring include child sexual abuse material (given that it is illegal in all circumstances) and illegal products (given that wrongful removals affect the freedom to do business rather than the freedom of expression).
 - b. Differentiation can also be made in terms of the size of the platform. On the one hand, some would argue that the issue of illegal content is especially harmful on larger platforms and that these need to be regulated more strictly. On the other hand, only targeting big platforms may lead smaller platforms to become safe havens for illegal content. The legislator will be required to find a delicate balance. A heavy-handed approach to big platforms might also reinforce market positions by giving incentives to smaller platforms to stay small.
- 3. *Legality*: Finally, any reform must comply with the protection of fundamental rights, in particular the freedom of expression and the freedom to conduct a business. In this regard, platforms and other internet intermediaries form an essential part in providing the infrastructure online. Whereas in previous centuries the central measures for controlling speech might have concerned the licensing of printing presses (another intermediary), today the regulation of platforms may take centre stage. As highlighted by the ruling of the French Constitutional Council on Loi Avia, a proposal that includes short deadlines, lack of judicial overview and significant penalties creates a risk of collateral censorship on platforms, which can be considered a disproportionate limitation of freedom of expression online.¹⁴⁶

¹⁴⁵ A regulatory sandbox can be described as a policy tool whereby a certain regulatory solution is imposed on an experimental basis to analyse the practical outcomes.

¹⁴⁶ Aurelien Breeden (2020).

Bibliography and other sources

Case Law

Case C-236/08, Google France and Google

Case C-390/18, Airbnb Ireland.

Case C-324/09, L'Oréal and Others.

Case C-360/10, SABAM.

Case C-18/18, Gławischnig-Piesczek.

Case C-401/19, Poland v. Parliament and Council.

Case C-682/18, YouTube.

Case C-203/15, Tele2 Sverige

Recommendations, communications and other documents from the European Commission

COM(2017) 555, *Tackling Illegal Content Online Towards an enhanced responsibility of online platforms*, September 2017.

COM(2018) 640, *On preventing the dissemination of terrorist content online A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018*, September 2018.

SWD(2018) 408, *Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online*, September 2018.

SWD(2016) 301, *Impact Assessment on the modernisation of EU copyright rules*, September 2016.

SWD(2016) 168, *Impact Assessment AVMS Directive*, May 2016.

SEC(2011) 1641, *Staff Working Document Online services, including e-commerce, in the Single Market*, January 2012.

C(2018) 1177, *Recommendation on measures to effectively tackle illegal content online*, March 2018.

Commission (2020a), *Consultation on the Digital Services Act package*, June 2020.

Commission (2020b), *Shaping Europe's Digital Future*, February 2020.

Commission (2020c), *Guidelines on the Revised Audiovisual Media Services Directive – Questions and Answers*, July 2020.

Commission (2018), *Product Safety Pledge: Voluntary commitment of online marketplaces with respect to the safety of non-food consumer products sold online by third party sellers*, June 2018.

Commission (2016), *The EU Code of conduct on countering illegal hate speech online*, May 2016.

Commission (2011), *Memorandum of Understanding on the sale of counterfeit goods via the internet*, May 2011.

Commission (2015), *EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online*, December 2015.

Laws and regulations

German Network Enforcement Act (2017), Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) 536/17.

Austrian e-Commerce Law (2001), Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG).

Spanish Law on information society services and e-commerce (2002), Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico ("LSSI").

Swedish Act (1998:112) on Responsibility for Electronic Bulletin Boards.

Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market.

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for the business users of online intermediation services.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.

Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member

States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the digital internal market and amending Directives 96/9/EC and 2001/29/EC.

Literature

Stefan Larsson & Jonas Andersson Schwarz (2018), *Developing Platform Economies: A European Policy Landscape*, Brussels, European Liberal Forum.

Martin Husovec (2017), *Injunctions Against Intermediaries in the European Union: Accountable But Not Liable?*, Cambridge, Cambridge University Press.

News articles

Aurelien Breeden (2020), French Court Strikes Down Most of Online Hate Speech Law, The New York Times, June 2020, <https://www.nytimes.com/2020/06/18/world/europe/france-internet-hate-speech-regulation.html> (visited on 2020-07-17).

David Uberti (2019), *The Christchurch Terror Attack Video Is Still Spreading on Facebook*, Vice News, November 2019, https://www.vice.com/en_uk/article/wjw93n/the-christchurch-terror-attack-video-is-still-spreading-on-facebook (visited on 2020-07-17)

Laura Kayali (2019), *Copyright Wounds to be Reopened in EU Top Court*, Politico, November 2019, <https://www.politico.eu/article/copyright-fight-cjeu-rightholders-google-youtube/> (visited on 2020-07-21).

Isobel Asher Hamilton (2018), *YouTube failed to take down live videos of child exploitation after they were flagged to moderators*, Business Insider, December 2018, <https://www.businessinsider.com/youtube-failed-to-take-down-flagged-videos-of-child-exploitation-2018-12?r=US&IR=T> (visited on 2020-07-21).

Irish Tech News (2020), *Investigation Reveals Major eCommerce Sites Taking up to Two Weeks to Remove Harmful COVID-19 Products*, April 2020, <https://irishtechnews.ie/ecommerce-sites-taking-up-to-two-weeks-to-remove-harmful-covid-19-products/> (visited on 2020-07-17)

Michael-Ross Fiorentino (2018), *France Passes Controversial 'Fake News' Law*, Euronews, November 2018, <https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law> (visited on 2020-07-17).

National Public Radio (2017), *YouTube Inadvertently Erases Syrian War Videos In Purge Of Extremist Propaganda*, September 2017, <https://www.npr.org/transcripts/550757777> (visited on 2020-07-17).

Tracy Jan & Elizabeth Dwoskin (2017), *A white man called her kids the n-word. Facebook stopped her from sharing it*, The Washington Post, July 2017, https://www.washingtonpost.com/business/economy/for-facebook-erasing-hate-speech-proves-a-daunting-challenge/2017/07/31/922d9bc6-6e3b-11e7-9c15-177740635e83_story.html (visited on 2020-07-17).

BBC (2020), *France Gives Online Firms One Hour to Pull 'Terrorist' content*, May 2020, <https://www.bbc.com/news/technology-52664609> (visited on 2020-07-20).

Reports

National Board of Trade (2015), *Online Trade, Offline Rules: A Review of Barriers to e-commerce in the EU*, May 2015.

OECD (2019), *An Introduction to Online Platforms and Their Role in the Digital transformation*, May 2019.

McKinsey (2016), *Digital Globalization: The New Era of Global Flows*, March 2016.

ICF Consulting (2018), *Overview of the legal framework of notice-and-action procedures in Member States SMART 2016/0039*, July 2018.

Melanie Smith (2020), *Enforcement and cooperation between Member States: E-Commerce and the future Digital Services Act*, Study requested by Europeans Parliament's IMCO committee, April 2020.

Jan Nordemann (2017), *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?*, Study requested by Europeans Parliament's IMCO committee, November 2017.

Giovanni Sartor (2017), *Providers Liability: From the e-Commerce Directive to the Future*, Study requested by Europeans Parliament's IMCO committee, October 2017.

Serge Abiteboul et al (2019), *Interim mission report: Creating a French Framework to Make Social Media Platforms More Accountable: Acting in France with a European Vision*, May 2019.

Anja Hoffmann & Alessandro Gasparotti (2020), *Liability for illegal content online: Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a "Digital Services Act"*, March 2020.

Policy papers

EDRi (2020), *COVID-Tech: COVID infodemic and the lure of censorship*, May 2020.

Digital Europe (2020), *Towards a more responsible and innovative internet - Digital Services Act position paper*, May 2020.

Ursula Von der Leyen (2019), *Political Guidelines for the Next European Commission 2019-2024: A Union that strives for more – My agenda for Europe*, July 2019.

Schibsted (2019), *Ensuring Democracy and Freedom of Speech Online – A Need for a Balanced Regulation of Social Networks*, November 2019.

Google (2016), *Continuing to create value while fighting piracy: an update*, July 2016.

Scientific articles and working papers

Andreas Lendle, Marcelo Olarreaga, Simon Schropp & Pierre-Louis Vézina (2016), *There Goes Gravity: eBay and the Death of Distance*, The Economic Journal, Volume 126, Issue 591, pp. 406-441, <https://doi.org/10.1111/eoj.12286>.

Andreas Lendle & Marcelo Olarreaga (2017), *Can Online Markets Make Trade More Inclusive*, ADBI Working Paper Series No. 742, <https://www.adb.org/publications/can-online-markets-make-trade-more-inclusive> (visited on 2020-07-17).

Maria Lillà Montagnani & Alina Trapova (2019), *New Obligations for Internet Intermediaries in the Digital Internal Market – Safe Harbours in Turmoil?*, Journal of Internet Law, Vol. 22 Issue 7, pp. 3-11, <http://dx.doi.org/10.2139/ssrn.3361073>.

Jack Balkin (2014), *Old-School/New-School Speech Regulation*, Harvard Law Review, Vol. 127 Issue 8, pp. 2296-2342, <https://www.jstor.org/stable/23742038?seq=1> (visited on 2020-07-21).

Sharon Bar-Ziv & Niva Elkin-Koren (2018), *Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown*, Connecticut Law Review, Vol. 50 Issue 2, pp. 339-385, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3214214 (visited on 2020-07-21).

Jason Mazzone (2006), *CopyFraud*, New York University Law Review, Vol. 81 Issue 3, pp. 1026-1100, <https://www.nyulawreview.org/issues/volume-81-number-3/copyfraud/> (visited on 2020-07-21).

Other sources

European Parliament (2019), *Questions and Answers on issues about the digital copyright directive*, <https://www.europarl.europa.eu/news/en/press-room/20190111IPR23225/questions-and-answers-on-issues-about-the-digital-copyright-directive>, March 2019, (visited on 2020-08-13).

Till Kreutzer (2020), *The EU copyright Directive and its potential impact on cultural diversity on the internet – Part I*, Kluwer Copyright Blog, January 2020, <http://copyrightblog.kluweriplaw.com/2020/01/22/the-eu-copyright->

directive-and-its-potential-impact-on-cultural-diversity-on-the-internet-part-i/?doing_wp_cron=1595251791.0803730487823486328125 (visited on 2020-07-20).

Miquel Peguera (2019), *The New Copyright Directive: Online Content-Sharing Service Providers lose eCommerce Directive immunity and are forced to monitor content uploaded by users (Article 17)*, Kluwer Copyright Blog, September 2019, http://copyrightblog.kluweriplaw.com/2020/01/22/the-eu-copyright-directive-and-its-potential-impact-on-cultural-diversity-on-the-internet-part-i/?doing_wp_cron=1595251791.0803730487823486328125 (visited on 2020-07-20).

Marion Goller (2019), *Copyfraud and Overclaiming – What to watch out for when implementing the EU copyright directive*, iRights.info, September 2019, <https://irights.info/artikel/copyfraud-and-overclaiming-what-to-watch-out-for-when-implementing-the-eu-copyright-directive/29654> (visited on 2020-07-21).

Antonella Gentile (2019), *Rome Court finds videosharing platform directly liable for content uploaded by users*, IPKat Blog, July 2019, <http://ipkitten.blogspot.com/2019/07/rome-court-finds-videosharing-platform.html> (visited on 2020-07-21).

Evan Engstrom & Nick Feamster (2017) *The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools*, <https://www.engine.is/the-limits-of-filtering> (visited on 2020-07-21).

Twitter (2019), *Transparency Report*, January-June 2019, <https://transparency.twitter.com/en/twitter-rules-enforcement.html#twitter-rules-enforcement-jan-jun-2019>, (visited on 2020-07-21).

Google (2019), *Transparency Report*, October-December 2019, https://transparencyreport.google.com/youtube-policy/removals?total_removed_videos=period:Y2019Q4;exclude_automated:all&lu=total_removed_videos, (visited on 2020-07-21).

Facebook (2019a), *Transparency Report*, July-September 2019, <https://transparency.facebook.com/community-standards-enforcement#child-nudity-and-sexual-exploitation>, (visited on 2020-07-21).

Facebook (2019b), *Establishing Structure and Governance for an Independent Oversight Board*, September 2019, <https://about.fb.com/news/2019/09/oversight-board-structure/> (visited on 2020-07-21).

Sammanfattning på svenska (Summary in Swedish)

I den här rapporten analyserar vi behovet av att reformera EU:s lagstiftning om plattformars ansvar för olagligt innehåll (exempelvis terrorisminnehåll, hatbrott och skadliga varor). Kommissionen har på detta område tagit initiativ till en ”Digital Services Act” som ska uppdatera EU:s lagstiftning. Den här rapporten diskuterar de centrala frågorna som behöver analyseras i den kommande lagstiftningsprocessen. Rapporten är en del av Kommerskollegiums arbete med att stödja den svenska regeringen med analyser inför kommande förhandlingar om EU:s lagstiftning på den inre marknaden.

Analysen i rapporten tar stöd i underlag från en enkät som skickades ut av Kommerskollegium i slutet av 2019. Enkäten besvarades av 29 intressenter (plattformar, företag och intresseorganisationer) och används för att ge ett stickprov av intressenternas åsikter. Svaren används dock inte för att dra statistiska slutsatser.

I rapporten analyserar vi fragmenteringen mellan olika medlemsstater under det nuvarande regelverket. Vi presenterar också förslag för att uppnå en större harmonisering inom EU. Vi rekommenderar följande åtgärder för närmare analys:

- Möjligheten att introducera harmoniserade procedurer för att ta bort olagligt innehåll från plattformar inom EU.
- Möjligheten att se över tillämpningsområdet för e-handelsdirektivet för att hantera tjänster som inte beaktas i det ursprungliga direktivet.
- Möjligheten att förtydliga gränsdragningen mellan aktiva och passiva plattformar i e-handelsdirektivet.
- Möjligheten att förtydliga distinktionen mellan generell och specifik övervakning i e-handelsdirektivet.
- Möjligheten att förtydliga förhållandet mellan e-handelsdirektivet och andra delar av EU:s regelverk, exempelvis det nya upphovsrättsdirektivet och direktivet om audiovisuella medietjänster.

I rapporten diskuterar vi också argument för och emot en större reform av kraven på plattformar. Vi utreder om det finns ett behov av att introducera krav på innehållsfilter hos plattformar. Frågan innebär en komplex avvägning mellan motstående intressen. Detta avspeglas också i svaren på enkäten från 2019 där åsikterna går isär om det finns ett behov

av en större reform. Vi presenterar följande rekommendationer för EU:s kommande lagstiftningsprocess.

Först belyser vi vikten av att underbygga eventuella förslag med en bred evidensbas. Det är viktigt att lagstiftningsprocessen inte stressas fram. Exempel på verktyg som kan användas för att samla in empirisk evidens är regulativa ”sandlådor” och offentliga samråd. Vidare understryker vi att olika typer av olagligt innehåll kan behöva regleras på olika sätt. Exempelvis kan en striktare ansvarsnivå utredas särskilt vad gäller sexuella övergrepp mot barn och skadliga produkter på e-handelsplattformar. Slutligen betonar vi att varje förslag på detta område måste vara förenligt med dem grundläggande rättigheterna, särskilt yttrandefriheten och näringsfriheten.

Annex: Platform Liability and the e-Commerce Directive – answers from stakeholders

Executive summary

In December 2019, the National Board of Trade Sweden sent out a questionnaire to stakeholders regarding platform liability. The questionnaire was sent to around 100 companies and organisations and we received 29 answers.¹⁴⁷ The answers do not constitute a representative selection. We caution against drawing quantitative conclusion based on the answers provided. The answers cannot support statements such as “a majority of Swedish stakeholders supports X”. Instead, we argue that the value lies in the qualitative arguments put forward by the participants. In this regard, it should also be noted that some of the answers were less motivated which made them less useful for this purpose.

In general, it can be said that opinions diverge among the respondents on the need to reform the e-commerce directive. Broadly stated one group favours the status quo and argues that it offers a good balance for all interests involved. In particular, they highlight that a reform might negatively impact innovation and freedom of speech online. Another group wants to see reform due to the harms caused by illegal content online. They note issues such as disinformation, child sexual abuse and liability for unsafe goods from third countries. They argue that it should not be left to self-regulation to protect these interests.

There is more agreement regarding some issues. This includes the need to harmonise procedural rules for notice and takedown in the EU. Many respondents favour such harmonisation, albeit with divergence as to the design of the reform. Opinions are also favourable as to the harmonisation of proactive “duties of care” in the EU. Another issue where several agree is that a reform of the liability could lead to censorship of legal content online. Some respondents highlight this issue as particularly important for Sweden. In a similar vein, most respondents do not think that the content filters¹⁴⁸ currently available on the market are effective in removing illegal content online. Some argue that filters let through too much illegal content; others argue that they block too

¹⁴⁷ The questionnaire was sent out based on a mapping of relevant stakeholders. Focus was on stakeholders in Sweden and the ambition was to get a wide range of interests represented, including MSME:s.

¹⁴⁸ Content filters are automatic tools used by platforms to block and remove illegal and unwanted content from its platforms.

much legal content. One stakeholder highlights child sexual abuse material as an area where filters however can be effective.

Finally, many respondents also see a need for harmonising other issues regarding platforms, outside of the e-commerce directive. Examples include digital taxation, data sharing, consumer protection, the gig economy (sharing economy) and reform of competition law (including proactive regulation).

| Group of respondents | No |
|-----------------------------------------------------------------|-----------|
| An online platform | 7 |
| Other business respondent | 7 |
| An association or trade organisation representing civil society | 1 |
| An association or trade organisation representing businesses | 8 |
| An association or trade organisation representing workers | 3 |
| Other | 3 |
| Total | 29 |

Introduction

The general legal framework for platform liability is found in the e-commerce directive. The directive has shaped the development of the digital economy in the EU. It is however soon 20 years since it was adopted and there is a discussion on the need to reform the rules.

The National Board of Trade is now publishing analysing the issue of platform liability and the e-commerce directive. As part of this analysis, we sent out a questionnaire regarding platform liability to stakeholders in Sweden. The questionnaire was open between December 2019 and January 2020. It was sent to around 100 stakeholders and we received 29 answers. Five of the answers were from MSME-enterprises.

In this memorandum, we summarise the results from the questionnaire. The memorandum will strive to present the answers in a neutral way, without providing any additional argumentation from the National Board of Trade.

Please note that the National Board of Trade did not verify the accuracy of the information presented by the respondents. Further analysis and fact checking is necessary before using the answers as grounds for policy proposals.

The notice and takedown regime (Article 14 e-commerce directive)

Today, platforms can avoid liability for content uploaded by their users if the platform has not engaged actively with the content and when gaining knowledge of the illegal content removes it expeditiously. This is commonly referred to as the notice and take down regime.

Question 1: Do you see a need to change the rule described on content liability for platforms (the notice and takedown regime)?

The answers are relatively evenly distributed for and against a need to change the rule. In general, the answers can be divided into two categories.

One group of respondents are satisfied with the current scheme for platform liability based on the notice and takedown principle. This group holds that the current system offers a balanced and proportional solution to the different interests in play. Some contributors highlight the balance between platform liability and the freedom of expression in particular. One stakeholder highlights that the rule of law must be maintained and that private companies are not to determine if online content or behaviour is illegal or not.

The second group of respondents wants to see a revision and modernisation of the platform liability. They highlight the dangers of illegal content, such as disinformation, child sexual abuse and liability for unsafe goods from third countries. Some respondents are of the opinion that we need to sharpen the rules to protect our democracy. One stakeholder wants to see a specific liability regime for social networks, as a new category in mass communication. Regulation cannot be left to voluntary company level self-regulation, due to the importance of this issue. Another respondent wants a reform of the rules for liability for illegal products sold on platforms. One respondent argues that liability rules should be tailored depending on the type of infringement (for example incitement to hatred, terrorism, child sexual abuse material and disinformation). It is argued that using general concepts such as “illegal content” and “harmful content” carries the risk of being overbroad and repressive in the future.

Some highlight that the current regime, based on actual knowledge, poses a disincentive for platforms to act proactively to remove illegal content. They are rather encouraged to wait for the notice before they do anything. They prefer the introduction of a “good Samaritan clause” which shields the platform from liability where they have made good

faith efforts to remove illegal content. This is in particular important for smaller platforms, they argue.

One issue that is highlighted is the relationship between Article 14 e-commerce directive (the notice and take down clause) and Article 17 copyright directive¹⁴⁹. One respondent sees a risk of conflict of laws and argues that the situation is not in conformity with the Union's commitment to better regulation.

Question 2: The procedural rules for a notice and takedown (time limits, content of the notification etc.) are today not harmonised and vary across the Member States. Do you see a need to harmonise these rules?

The answers are generally positive towards harmonised rules for the procedure for notice and takedown. Some stakeholders highlight the need for harmonised rules given the cross-border nature of platforms and that harmonisation of procedural rules can provide clarity, predictably and efficiency and facilitate cooperation within EU.

When it comes to time limits for the take down, one solution that is proposed is a general requirement for takedowns within 1-2 working days. Another solution that is put forward is a limit of 24 hours for "clearly illegal content" whereas in situations where the illegality is unclear the content could be "freezed" for up to 48 hours. One stakeholder argues that any time limit must be technically feasible and guarantee the protection of fundamental rights. It sees a risk that inappropriately short time limits and sweeping removal request will cause a risk of platforms over-blocking legal speech. Platforms will have no choice but to adopt automatic removal system to meet the scale of the challenge they argue, and that a flexible requirement such as "expeditiously" is more appropriate to respect fundamental rights.

When it comes to the content of the notification, some answers underline the need for standardised EU-wide notices with clear requirements on minimum information. One stakeholder highlights the need for the notification to be validated by a third party (court, official or other) before the host is required to act. Another stakeholder wants the notice to: 1. clearly identify the content with URL¹⁵⁰ or other unique identifier

¹⁴⁹ Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC. Article 17 imposes a liability for user-generated content on online content-sharing services. The liability framework under the copyright directive is more stringent than the notice and takedown regime provided for in the e-commerce directive.

¹⁵⁰ A Uniform Resource Locator (URL) is used to identify and locate websites online.

(not top-level domain), 2. clearly state the basis of the legal claim, including the country in which the law applies and 3. attest to the good faith and validity of the claim using the legal form appropriate to the jurisdiction (such as an oath under the penalty of perjury).

One respondent wants to see a stay down regime in line with the European Court of Justice (CJEU) judgement in the Glawischnig-Piesczek case.¹⁵¹ A stay down regime would require the host to prevent the reappearance of “identical” or “equivalent” content for the future. Another contributor highlights that removing “equivalent” content can have an adverse impact on the freedom of speech, since it can be hard for algorithms to distinguish what is “equivalent” and that they will be inclined to remove “too much” rather than “too little”, for liability reasons.

One stakeholder argues that the procedures should focus on removing access to illegal content at the source (the web server that hosts the content) rather than a broader order to a third party platform to block access. Another stakeholder raises the importance of keeping the procedures for different types of illegal content under the monitoring of specialised agencies to avoid generalised procedures for “internet harms” under which many inconveniences can be put. This could be harmful for our democracy according to the respondent.

Question 3: In addition to the notice and takedown regime, many platforms are making voluntary efforts to prevent illegal content online. Do you consider that the self-regulation of platforms is effective in dealing with illegal content?

Views diverge on the effectiveness of current self-regulatory efforts of platforms.

Some are generally positive to self-regulation, and see room for improvements. One stakeholder holds that self-regulation has been very effective in the online environment, where jurisdiction issues often mean that binding provisions cause competition problems. Another stakeholder argues that self-regulation is necessary since technology is developing much faster than any legislator can make rules.

¹⁵¹ Case C-18/18, Glawischnig-Piesczek. The case concerned defamatory content on Facebook against an Austrian politician. The plaintiff had requested an Austrian court to impose an injunction on Facebook to remove the content in question and to remove “identical” or “equivalent” content in the future. The plaintiff had also requested that the content should be removed by Facebook worldwide. The case was brought to the CJEU where the court held that the e-commerce directive did not preclude an injunction such as in the case at hand. The injunction was not considered a general monitoring obligation.

One platform highlights the progress made in terms of self-regulation. The platform emphasises that it removed over 8.7 million videos for violating its Community Guidelines between July and September 2019. It also underlines the progress made in the Global Internet Forum to Counter Terrorism (GIFCT¹⁵²) and under the EU Hate Speech Code of Conduct¹⁵³. It argues that the EU should continue to consider areas where oversight could be managed through self-regulation or co-regulation. Another stakeholder holds that self-regulation could be modelled on a system of regulation via a business coalition, where a jury of representatives can deal with complaints (see the example of the European Advertising Standards Alliance¹⁵⁴).

Some highlight that self-regulation may be working for some platforms, but that it needs to be industry-wide to be effective. In the context of child sexual abuse material, one respondent states that very few platforms do anything to prevent illegal content online.

One group of contributors argues that self-regulation should only be a complementary tool to binding regulation. One respondent holds that binding regulation should apply since private companies should not decide what is illegal and not. Another stakeholder questions the effectiveness of self-regulatory process, with reference to the repetitive occurrence of toys with phthalates on e-commerce platforms in Denmark.¹⁵⁵

It is also argued by one respondent that a way forward could be that platforms that implement a responsible policy to limit and remove illegal content are overseen by a European authority. This could stimulate

¹⁵² The objective of the GIFCT is to combat terrorism content through inter alia joint tech innovation, knowledge sharing, research and incident protocols. Members include Facebook, Microsoft, Twitter, YouTube, Pinterest, Dropbox, Amazon, LinkedIn and WhatsApp.

¹⁵³ The Code entails a commitment to have rules and community standards that prohibit hate speech and put in place systems and teams to review content that is reported. The participants also commit to review the majority of the content flagged within 24 hours. Member include Facebook, Microsoft, Twitter, YouTube, Instagram, Google+, Snapchat, Dailymotion and Jeuxvideo.

¹⁵⁴ The alliance provides guidance on how to design self-regulation for advertising through the development of high operational standards for self-regulatory systems, as set out in the Best Practice Model and EASA's Charter

¹⁵⁵ The respondent refers to a test by the Danish Consumer Council in June 2019 which revealed toys with high levels of phthalates on large e-commerce platforms. The respondent highlights that even though all platforms promised the Danish Environmental Agency to remove the toys from their website, the same toys with the same content of dangerous chemicals was purchased by the Danish Broadcaster DR in August and October.

‘good’ behavior and self-regulation and also make it possible to take the platform to the CJEU if the platform is violating its “duty of care”.

The prohibition against general monitoring obligations (Article 15 e-commerce directive)

The prohibition of general monitoring means that Member States are for example not allowed to require a social media site to actively monitor all its data to avoid any future infringement. A general monitoring obligation has been considered too complicated and costly by the CJEU and the court has also noted the risk of over-removal of legal content. On the other hand there is a trend towards imposing wider monitoring obligations on platforms in the Member States and in EU-legislation, such as the recently revised copyright directive¹⁵⁶.

Question 4: Do you see a need to change the prohibition on general monitoring obligations?

Opinions are divided on the need to modify the prohibition on general monitoring. One group of stakeholders considers it important to preserve the current rules. They highlight that a reform can risk infringing privacy, the freedom of expression and a risk of over-removal of legal content. Some underline that the prohibition protects an open and free society, the free flow of information, innovation, growth, creativity, and the freedom of expression. One contributor argues that monitoring is important for national security and to prevent crime, but that it is not a task for companies.

Another group of respondents is open to a modification of the prohibition for specific issues such as child sexual abuse materials, copyright infringements and unlawful sales of goods from third countries to EU consumers. One opinion provided is that, for child sexual abuse material, using hash-detection¹⁵⁷ of known illegal material removes the risk of over-removal. Considering the benefits of such monitoring, and that the convention of the rights of the child is now integrated into Swedish legislation¹⁵⁸, the stakeholder argues that Sweden should take the lead as a frontrunner country in this area.

¹⁵⁶ As mentioned above, the copyright directive imposes a liability for user-generated content on online content-sharing services. The liability framework under the copyright directive is more stringent than the notice and takedown regime provided for in the e-commerce directive.

¹⁵⁷ A hash detection tool creates a hash sum from a data such as a video or a picture, and compares the sum against hash sums from previously identified child sexual abuse material.

¹⁵⁸ The Convention on the Rights of the Child has recently been enacted into Swedish law. The Swedish law (2018:1197) entered into force on the 1st of January 2020 and the purpose is to improve the influence of the convention in Sweden.

Question 5: Do you consider that the current filtering systems available on the market are effective in dealing with illegal content? Please comment for example if you consider them too costly or if you have identified other effective options of removing illegal content online.

In terms of filtering solutions, views are generally sceptic towards their effectiveness. The reasons behind the answer do however differ. One group is generally negative to filtering, as they see filters as a threat to freedom of expression. One answer argues that filtering and blocking should only be used as a last resort. Another stakeholder highlights that filters cannot yet recognise legal uses of content, or understand context, they can therefore over-block. There is a need for human oversight. A couple of respondents argue that current filtering solutions are not as effective as necessary, citing the risk of circumvention and the availability of pirated and harmful products online. One respondent finds filters too costly and argue that it is hard to find a balance: a too effective filter may block freedom of information; a less effective filter may not find what is needed to block.

Another group is generally positive towards filtering solutions, but see a need to work on improving their efficiency. One solution, highlighted in the context of Child Sexual Abuse Material, is Project Arachnid¹⁵⁹ which is described as a cost-effective solution based on individual hashes. Some stakeholders argue that larger platforms have the resources to use filters in a better way.

One platform describes its own work with filtering. They have put a lot of effort into hash-matching and machine learning. They argue however that such a technology is not a silver bullet for the removal of illegal content. For example, they underline that technology to recognise hate speech is still in its early stages. Certain challenges like understanding context, history, spoken cues and replicating human judgement is still a long way off. Their approach is to use a combination of machines and human oversight.

¹⁵⁹ Project Arachnid is operated by the Canadian Centre for Child Protection and is a tool to combat the proliferation of child sexual abuse material (CSAM) on the internet. It automatically searches websites to identify known CSAM. According to its website, project Arachnid is currently detecting over 100,000 unique images per month that require analyst assessment.

Question 6: Today, the e-commerce directive allows for the imposition of “duties of care” on platforms at the national level. A duty of care is an obligation on platforms to take reasonable measures in order to detect and prevent illegal activities online. Do you see a need for a harmonised “duty of care” at the EU level?

Respondents are in general positive to a harmonised “duty of care”. Some prefer a minimum harmonisation approach, with room for more specific requirements at the national level, to avoid getting into compromise solutions. Others favour a full harmonisation with the same rules to be used in the whole Union, especially to avoid loopholes that are easy to exploit for online actors. One stakeholder argues that the term “duty of care” might cause confusion with legal notions in tort liability¹⁶⁰ and that other terms should be used. Finally one contributor questions if it might be hard for Member States to agree on a common level for the duty of care.

The Country of Origin Principle

The e-commerce directive also provides for the country of origin principle which entails that platforms and other information society services, in principle, are to be regulated in their home states (the state of establishment). The principle is however not without exception and the other states may under certain conditions regulate the service if there is a threat to a public interest.

Question 7: Do you see a need to change the country of origin principle for platforms in the EU?

Opinions differ on the need to reform the country of origin principle. Some stakeholders think that the principle should be preserved as is, with one respondent holding it is as a key piece for the success of the development of the internal market. Others indicate that the principle needs to have clear exceptions, in particular with regards to consumer and child protection rules.

Along this line, some respondents argue that the country of origin should only apply in certain areas of law, whereas other areas should be reserved for the country of destination. Interestingly two stakeholders offer diverging views on whether issues relating to freedom of expression (hate speech) should be subject to the country of origin principle or not.

¹⁶⁰ Simply put, tort liability is a legal duty under tort law to compensate someone for damages caused.

One contributor argues that, when it comes to non-European platforms, a general EU-regulation is preferred.

Question 8: Do you think the scope and application of the country of origin principle is clear in practice?

Most of the respondents submit that they do not have enough information to answer this question. One stakeholder puts forward that recent EU jurisprudence and legislation has caused legal uncertainty surrounding the principle, without referencing specific cases or legislation. Another contributor wants to see a clear exception from the country of origin for the scrutiny of user-generated content.

One answer offered detailed input on the clarification they would like to see, which included:

- It should be clarified that the principle covers all requirements relating to the take up and pursuit of an activity, not only the issues harmonised under the e-commerce directive (e.g. commercial communications, liability rules etc.).¹⁶¹
- It should be clarified that the list of grounds for introducing derogations in individual cases is exhaustive.¹⁶²
- The exempted fields may need to be revised, in particular the exception related to consumer contracts may no longer be justified given recent harmonisation.
- The country of origin principle is applied under more instruments than the e-commerce directive, for example the AV-directive. EU should consider streamlining the derogations/procedures for derogations to reduce legal uncertainty for service providers.

Question 9: If you have identified any problems with the current regulatory framework, do you believe it would be possible to address these problems with additional guidance documents from the European Commission, instead of revising the rules?

Opinions are also divided with regards to the possibility of using additional guidance to solve current problems, rather than revising the rules. One group indicates that they prefer additional guidance as far as possible. One stakeholder favours a mapping of all rules in platform liability to identify overlaps and possible conflicts. Another group holds that additional guidance will not be able to solve the issues they have identified with the e-commerce directive.

¹⁶¹ This is arguably already clear from the text of the e-commerce directive.

¹⁶² This is arguably already clear from the text of the e-commerce directive.

A couple of respondents favour the introduction of a self-regulatory/co-regulatory framework for platforms to introduce proactive measures, to complement the liability framework under the e-commerce directive. The framework would enable platforms to take reasonable, proportionate and feasible actions to mitigate issues on their service. The framework has been outlined in a position paper written by EDiMA¹⁶³, a trade association representing online platforms and other innovative tech companies.

Question 10: Do you see any difference between the regulation of platform liability in different Member States? Please provide examples in the comment section.

Most respondents submit that they do not have any information to provide under this question. A couple highlight recent reforms in Germany (NetzDG) and France (Avia-law) on hate speech. One contributor mentions a strict implementation in Italy, and one respondent names the UK Online Harms White Paper.

One contributor gives a few examples of fragmentation:

- Different case law in Germany/Italy on whether a unique URL is necessary in the notification to give “actual knowledge”.¹⁶⁴
- Different laws on the status of search engines. In Austria they are considered mere conduits for the purpose of the e-commerce directive, in Italy they are qualified as caching services¹⁶⁵. In Spain there is a specific liability exception for search engines whereas in France the hosting exception is frequently applied.

An issue highlighted in one answer is the geographic scope of a takedown request. Some content might be legal in one country and illegal in another. The question is if one member state can request the removal of content in the whole EU, despite it being legal in some Member States. The issue is not regulated in the e-commerce directive.

¹⁶³ EDiMA is a trade association representing online platforms & other innovative tech companies in Europe. The policy paper can be found [here](#).

¹⁶⁴ According to the respondent, some courts require that a notice specifies the URLs for the content to be removed, whereas other courts have in some cases ruled that an online intermediary can gain knowledge of an infringement as a result of receiving generic removal demand letters that list the titles of the allegedly infringed copyright material. See judgment by the Higher Regional Court of Cologne in [redacted] v. Google Inc. 13 October 2016; judgement by the Court of Turin, 7 April 2016 in Delta TV v. YouTube. Compare to judgment by the Court of Appeal of Rome in RTI v. TMT Enterprises LLC (Break Media), 29 April 2017.

¹⁶⁵ Court of Cassation, 19 March 2019 in RTI v Yahoo. Mere conduits and caching services are subject to other provisions on content liability in the e-commerce directive in contrast to the liability regime for platforms that is discussed in this memorandum.

One contributor highlights the risk of diverging implementation of the new copyright directive.

Question 11: Do you believe that the rules discussed should differentiate between bigger and smaller platforms? If so, please comment on what criteria should be used to carry out the distinction between different categories of platforms.

With regard to the possibility for differentiation, most respondents prefer that the same rules apply to big and small platforms. They refer to risks for consumers using small platforms, the risk that small platforms are prevented to grow and the difficulties in drawing a line between big and small. One stakeholder notes the risk of migration of illegal content to smaller platforms, should they be subject to different rules. Others are more positive to differentiation, indicating that platforms that have a big impact on the market or society at large should have stricter requirements. Criteria that are suggested to define a “big” platform include the amount of content on the platform, the number of users, monetary turnover and traffic in terms of data volume. One respondent wants to see an evaluation of the new copyright directive, which distinguishes between big and small platforms,¹⁶⁶ before any new distinction.

Question 12: Do you believe that a reform of the rules, towards a greater liability for platforms, could lead to an increase in the “censorship” of legal content on the platforms?

Most respondents note a risk that a reform could affect the freedom of expression online. Several stakeholders raise that any reform need to be aligned with the strong freedom of expression laws and constitution of Sweden. It is indicated that the Swedish government should carefully consider this in an early stage of the any upcoming negotiation.

A couple answers indicate that the issue of freedom of expression will not be a major issue for certain types of illegal content, in particular child sexual abuse material and physical goods sold through platforms from third country traders. One stakeholder argues that their preferred solution, a stay down system for social networks, would not increase censorship online. Another stakeholder emphasises the need in any reform to impose safeguards for users to challenge takedown decisions and to introduce

¹⁶⁶ The copyright directive provides for a more lenient liability regime for new online content-sharing service providers which have been available to the public in the Union for less than three years and which have an annual turnover below EUR 10 million.

judicial review, since the platforms are not well suited to be judge and jury in take down disputes.

One platform notes a risk for the freedom of expression due to short time limits and overbroad removal requests. Short time limits and harsh penalties creates a risk that platforms will over-block legitimate content they argue. Another respondent argues that the rule of law must apply and that private companies should not decide if content or behavior online is illegal or not.

Question 13: More generally, do you see a need for harmonisation of other platform activities (aside from the questions discussed above) such as data sharing, digital taxes or consumer protection?

Many respondents identify other issues, outside of the e-commerce directive, where there could be a need for EU harmonisation. Some argue that harmonisation is necessary with reference to the cross-border nature of platform activities. Issues highlighted include digital taxation, data sharing, consumer protection, the gig economy (sharing economy) and reform of competition law (including proactive regulation). In many cases, there is no closer information as to the content of the desired harmonisation. One respondent favours a mapping of all rules in platform liability to identify overlaps and possible conflicts.