1.

EUROPEAN
COMMISSION

Brussels, 28.9.2017
COM(2017) 555 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Tackling Illegal Content Online

Towards an enhanced responsibility of online platforms

1. INTRODUCTION

Online platforms are important drivers of innovation and growth in the digital economy. They have enabled an unprecedented access to information and exchanges as well as new market opportunities, notably for small and medium-sized enterprises (SMEs). Online platforms also provide the main access point to information and other content for most people on the internet today, be it through search engines, social networks, micro-blogging sites, or video-sharing platforms. The business models of platforms have also evolved recently towards closer links between users and content – notably for targeted advertisement. These platforms connect billions of users with vast quantities of content and information[1] and provide innovative services to citizens and business.

However, the important spread of illegal content that can be uploaded and therefore accessed online raises serious concerns that need forceful and effective replies. **What is illegal offline is also illegal online**. Incitement to terrorism, xenophobic and racist speech that publicly incites hatred and violence, as well as child sexual abuse material are illegal in the EU. The increasing availability of terrorist material online and the spreading of such content is a serious threat to security and safety, as well as to the dignity of victims. The European Union has responded to these concerns through a certain number of measures[2]. However, addressing the detection and removal of illegal content online represents an urgent challenge for the digital society today.

Concerned by series of terrorist attacks in the EU and proliferation of online terrorist propaganda, the European Council of 22-23 June 2017 stated that it "*expects industry to … develop new technology and tools to improve the automatic detection and removal of* ***content that incites to terrorist acts****. This should be complemented by the relevant legislative measures at EU level, if necessary*". These calls were echoed by statements issued by the leaders of the G7 and G20 at their recent summits[3]. Similarly, the European Parliament, in its resolution on Online Platforms of June 2017 urged these platforms "*to strengthen measures to tackle illegal and harmful content*", while calling on the Commission to present proposals to address these issues[4].

Those online platforms which mediate access to content for most internet users carry a significant societal responsibility in terms of protecting users and society at large and preventing criminals and other persons involved in infringing activities online from exploiting their services. The open digital spaces they provide must not become breeding grounds for, for instance, terror, illegal hate speech, child abuse or trafficking of human beings, or spaces that escape the rule of law. Clearly, the spreading of illegal content online can undermine citizens' trust and confidence in the digital environment, but it could also threaten the further economic development of platform ecosystems and the Digital Single Market. Online platforms should decisively step up their actions to address this problem, as part of the responsibility which flows from their central role in society.

---

[1] At present, every second around 8,000 tweets are posted on Twitter, 1,000 photos are posted on Instagram, 60,000 Google searches are performed, and 70,000 YouTube videos are viewed. See http://www.internetlivestats.com/

[2] See section 2.

[3] European Council Conclusions, ST 8 2017 INIT, 22 and 23 June 2017, G7 Taormina Statement, 26 May 2017, and G20 leaders declaration , 8 July 2017

[4] European Parliament resolution 15 June 2017 on online platforms (2016/2274(INI))

The fight against illegal content online must be carried out with proper and robust safeguards to ensure protection of the different fundamental rights at stake. Given their increasingly important role in providing access to information, online platforms also have a key role to play in achieving such a balance. The fight against illegal content online within the EU should build on and also take into account EU actions at global level.

This Communication lays down a set of guidelines and principles for online platforms to step up the fight against illegal content online[5] in cooperation with national authorities, Member States and other relevant stakeholders. It aims to facilitate and intensify the implementation of good practices for preventing, detecting, removing and disabling access to illegal content so as to ensure the effective removal of illegal content, increased transparency and the protection of fundamental rights online. It also aims to provide clarifications to platforms on their liability when they take proactive steps to detect, remove or disable access to illegal content (the so-called "Good Samaritan" actions).

2. CONTEXT

The European Union has already responded to the challenge of illegal content online, through both binding and non-binding measures. These policy responses include the Directive to combat the **sexual abuse and sexual exploitation of children and child pornography**[6], the **Terrorism** Directive[7], the proposed measures in the context of the reforms of **copyright**[8] and the **Audiovisual Media Services** Directive (AVMSD)[9].

These existing and proposed legislative measures have been complemented by a range of non-legislative measures, such as the Code of Conduct on Countering **Illegal Hate Speech** Online[10], the work of the **EU Internet Forum**[11] as regards **terrorist propaganda**, the Memorandum of Understanding on the sale of **Counterfeit Goods**[12], the Commission Notice on the **market surveillance of products sold online**[13], online sale of **food chain products**, the EU Action Plan against **Wildlife Trafficking**[14], the Guidance on the **Unfair Commercial Practices** Directive[15] or the joint

[5] The elements presented here have been informed by a broad series of public as well as targeted consultations and stakeholder workshops.
[6] See the recent Report from the Commission to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.
[7] Terrorism Directive (EU) 2017/541 obliges Member States to take the necessary measures to ensure the prompt removal of online content inciting to commit terrorist acts (Article 21). In this area, in the context of the EU Internet Forum, platforms remove voluntarily terrorist content on the basis of referrals sent by the Europol Internet Referral Unit (IRU).
[8] COM(2016) 593
[9] COM(2016) 287
[10] http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
[11] http://europa.eu/rapid/press-release_IP-15-6243_en.htm
[12] http://ec.europa.eu/transparency/regdoc/rep/3/2016/EN/3-2016-3724-EN-F1-1.PDF
[13] JO C 250 of 1.8.2017
[14] http://ec.europa.eu/environment/cites/pdf/WAP_EN_WEB.pdf
[15] SWD(2016)163 of 25.5.2016

actions of the national authorities within the Consumer Protection Cooperation Network[16]. The European Strategy for a **Better Internet for Children**[17] is a self-regulatory initiative aiming to improve the online environment for children and young people, given the risks of exposure to material such as violent or sexually exploitative content, or cyberbullying.

In its Communications of 2016 and 2017[18], the Commission stressed the need for online platforms to act more responsibly and step up EU-wide self-regulatory efforts to remove illegal content. In addition, the Commission also committed to improve the coordination of the various sector-specific dialogues with platforms and to explore the need for guidance on formal notice-and-action procedures. This should be done in synergy with, and without prejudice to, dialogues already ongoing and work launched in other areas, such as under the European Agenda on Security or in the area of illegal hate speech.

Recent reports on some of these sector specific initiatives have shown some progress. For the case of illegal hate speech, reports from June 2017 indicated an increase of removals from 28 percent to 59 percent of a sample of notified content across some EU countries over a six months period, but noting important differences across platforms[19]. Some improvements in the speed of removal were also recorded over the same period while still 28 percent of removals took place only after a week[20]. This shows 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. In the framework of the EU Internet Forum tackling terrorist content, approximately 80-90 percent of content flagged by Europol has been removed since its inception[21]. In the context of child sexual abuse material, the INHOPE system of hotlines reported already in 2015 removal efficiencies of 91% within 72 hours, with 1 out of 3 content items being removed within 24 hours[22].

The various ongoing sector-specific dialogues also revealed a significant amount of similarity concerning the procedures that govern the detection, identification, removal and re-upload prevention across the different sectors. These findings have informed the present Communication.

At EU level, the general legal framework for illegal content removal is the E-Commerce Directive[23], which *inter alia* harmonises the conditions under which certain online platforms can benefit from the exception from liability for illegal content which they host across the Digital Single Market.

Illegal content on online platforms can proliferate especially through online services that allow upload of third party content. Such 'hosting' services are, under certain conditions, covered by

---

[16] http://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/consumer_protection_cooperation_network/index_en.htm

[17] Communication COM(2012) 196 final (Better Internet for Kids (BIK)): https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online

[18] COM(2016)288 and COM(2017)228.

19 http://europa.eu/rapid/press-release_IP-17-1471_en.htm

[20] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=71674

[21] http://europa.eu/rapid/press-release_IP-17-544_en.htm.

[22] http://www.inhope.org/Libraries/Annual_reports/INHOPE_Annual_Report_2015.sflb.ashx?download=true

[23] E-Commerce Directive 2000/31/EC of 8 June 2000.

Article 14 of the E-Commerce Directive[24]. This article establishes that hosting service providers[25] cannot be held liable for the information stored at the request of third parties, on condition that (a) they do not have actual knowledge of the illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent or (b), upon obtaining such knowledge or awareness, they act expeditiously to remove or to disable access to the information. At the same time, the Directive should "constitute the appropriate basis for the **development of rapid and reliable procedures for removing and disabling access to illegal information**"[26].

Moreover, Article 15 prohibits Member States from imposing "*a general obligation on providers, **when providing the services covered by [Article 14**], to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.*" At the same time, Recital 47 of the Directive recalls that this only concerns monitoring obligations of a general nature and *'does not automatically cover monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation."*

In this context, in its 2016 Communication on online platforms, the Commission committed itself to maintaining a balanced and predictable liability regime for online platforms, as a key regulatory framework supporting digital innovation across the Digital Single Market.

The guidance in this Communication is without prejudice to EU acquis and relates to the activities of online platforms, and in particular hosting services provided by these platforms[27] in the sense of Article 14 of the E-Commerce Directive, and covers all categories of illegal content while duly taking account of the fact that different types of content may require different treatment.

A harmonised and coherent approach to removing illegal content does not exist at present in the EU. Indeed, different approaches exist in the EU depending on Member States, content category, or type of online platform. A **more aligned approach would make the fight against illegal content more effective. It would also benefit the development of the Digital Single Market** and reduce the cost of compliance with a multitude of rules for online platforms, including for new entrants.

It is important to stress that this legal framework does not define, let alone harmonise, what constitutes "illegal" content. **What is illegal is determined by specific legislation at the EU level, as**

[24] It should be noted that, under the E-Commerce Directive, only those providers of information society services benefit from the liability exemption of Articles 12-14 that qualify as intermediary service providers (i.e. providing mere conduit, caching or hosting services, respectively). Recital 42 clarifies that, for activities to be covered by the liability exemption they must be "of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored."

[25] Most online platforms offer hosting services of content uploaded by their users.

[26] Recital 40 of the E-Commerce Directive. Note that this Communication focuses on hosting service providers, rather than mere conduits (Article 12) or caching service providers (Article 13).

[27] A hosting service is an information society service consisting of the storage of information provided by a recipient of the service. This category can cover a variety of actors, from online marketplaces, video-sharing platforms, social networks, blogging websites or review websites, to users' comments' sections in news pages.

well as by national law.[28] While, for instance, the nature, characteristics and harm connected to terrorism-related material, illegal hate speech or child sexual abuse material or those related to trafficking in human beings are very different from violations of intellectual property rights, product safety rules, illegal commercial practices online, or online activities of a defamatory nature, all these different types of illegal content fall under the same overarching legal framework set by the E-Commerce Directive. In addition, given the significant similarities in the *removal process* for these different content types, this Communication covers the whole range of illegal content online, while **allowing for sector-specific differences where appropriate and justified.**

In the EU, courts and national competent authorities, including law enforcement authorities, are competent to prosecute crimes and impose criminal sanctions under due process relating to the illegality of a given activity or information online. At the same time, online platforms are entitled to prevent that their infrastructure and business is used to commit crimes, have a responsibility to protect their users and prevent illegal content on their platform, and are typically in possession of technical means to identify and remove such content. This is all the more important that online platforms have invested massively to develop elaborated technologies to proactively collect information on content circulated on their premises and on users' behaviour. While swift decisions concerning the removal of illegal content are important, there is also a need to apply adequate safeguards. This also requires a balance of roles between public and private bodies.

The guidelines and principles set out in this Communication therefore do not only target the detection and removal of illegal content; they also seek to address concerns in relation to removal of *legal* content, sometimes called 'over-removal', which in turn impacts freedom of expression and media pluralism. Adequate safeguards should therefore be foreseen, and adapted to the specific type of illegal content concerned.

There are undoubtedly public interest concerns around content which is not necessarily illegal but potentially harmful, such as fake news or content that is harmful for minors[29]. However, the focus of this Communication is on the detection and removal of **illegal content**.

3. DETECTING AND NOTIFYING ILLEGAL CONTENT

The objective of this section is to **set out what online platforms, competent authorities and users should do in order to detect illegal content quickly and efficiently**.

Online platforms may become aware of the existence of illegal content in a number of different ways, through different channels. Such channels for notifications include (i) court orders or administrative decisions; (ii) notices from competent authorities (e.g. law enforcement bodies),

[28] Examples of areas that are covered (or proposed) under EU law include incitement to terrorism, illegal hate speech, child sexual abuse, intellectual property rights, product safety, offer and sales of food or tobacco products and counterfeit medicines, consumer protection rules or product safety measures, etc. In 2016, the Commission also clarified online platforms' transparency and professional diligence obligations under Directive 2005/29/EC on unfair commercial practices where platforms act as traders vis-à-vis consumers.

[29] The proposal for a revision of the Audio-visual Media Services Directive addresses this in the context of audio-visual content.

specialised "trusted flaggers", intellectual property rights holders or ordinary users, or (iii) through the platforms' own investigations or knowledge.

In addition to legal obligations derived from EU and national law and their 'duty of care', as part of their responsibilities, online platforms should ensure a safe online environment for users, hostile to criminal and other illegal exploitation, and which deters as well as prevents criminal and other infringing activities online.

3.1. Courts and competent authorities

In accordance with EU and/or national law, national courts and, in certain cases, competent authorities can issue binding orders or administrative decisions addressed to online platforms requiring them to remove or block access to illegal content.[30]

Given that fast removal of illegal material is often essential in order to limit wider dissemination and harm, online platforms should also be able to take swift decisions as regards possible actions with respect to illegal content online without being required to do so on the basis of a court order or administrative decision, especially where a law enforcement authority identifies and informs them of allegedly illegal content. At the same time, online platforms should put in place adequate safeguards when giving effect to their responsibilities in this regard, in order to guarantee users' right of effective remedy.

Online platforms should therefore have the necessary resources to understand the legal frameworks in which they operate. They should also **cooperate closely with law enforcement and other competent authorities** where appropriate, notably by ensuring that they can be rapidly and effectively contacted for requests to remove illegal content expeditiously and also in order to, where appropriate, alert law enforcement to signs of online criminal activity[31]. To avoid duplication of effort and notices and thus reduce the efficiency and effectiveness of the removal process, law enforcement and other competent authorities should also make every effort to cooperate with one another in the definition of effective digital interfaces which facilitate the fast and reliable submission of notification and to ensure efficient identification and reporting of illegal content. Establishing points of contact by platforms and authorities is key for the proper functioning of such cooperation.

---

[30] Article 14(3) of the E-Commerce Directive clarifies that Article 14 "shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement." For example, Directive 2004/48/EC on the enforcement of intellectual property rights stipulates in its Article 11 that "Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC"

[31] Article 15(2) of the E-Commerce Directive establishes that "Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."

For terrorist content[32], an EU Internet Referral Unit (IRU) has been established at Europol, whereby security experts assess and refer terrorist content to online platform (while some Member States have their own national IRUs).

Online platforms should **systematically enhance their cooperation with competent authorities in Member States, while Member States should ensure that courts are able to effectively react against illegal content online,** as well as **stronger (cross-border) cooperation between authorities.**

Online platforms and law enforcement or other competent authorities should appoint effective points of contact in the EU, and where appropriate define effective digital interfaces to facilitate their interaction.

Platforms and law enforcement authorities are also encouraged to develop **technical interfaces that allow them to cooperate more effectively in the entire content governance cycle**. Cooperation also with the technical community can be beneficial in advancing towards effective and technically sound solutions to this challenge.

3.2. Notices

3.2.1. Trusted flaggers

The removal of illegal content online happens more quickly and reliably where online platforms put in place mechanisms to facilitate a privileged channel for those notice providers which offer particular expertise in notifying the presence of potentially illegal content on their website. These are so-called "trusted flaggers", as specialised entities with specific expertise in identifying illegal content, and dedicated structures for detecting and identifying such content online.

Compared to ordinary users, **trusted flaggers can be expected to bring their expertise and work with high quality standards**, which should result in higher quality notices and faster take-downs. Online platforms are encouraged to make use of existing networks of trusted flaggers. For instance, for terrorist content, the Europol's Internet Referral Unit has the necessary expertise to assess whether a given content constitutes terrorist and violent extremist online content, and uses this expertise to act as a trusted flagger, besides its law enforcement role. The INHOPE network of hotlines for reporting child sexual abuse material is another example of a trusted flagger; for illegal hate speech content, civil society organisations or semi-public bodies are specialised in the identification and reporting of illegal online racist and xenophobic content.

In order to ensure a high quality of notices and faster removal of illegal content, **criteria based notably on respect for fundamental rights and of democratic values could be agreed by the industry at EU level**. This can be done through self-regulatory mechanisms or within the EU standardisation framework, **under which a particular entity can be considered a trusted flagger**, allowing for sufficient flexibility to take account of content-specific characteristics and the role of the trusted flagger. Other such criteria could include internal training standards, process standards and

[32] In the sense of Article 5 of Directive (EU) 2017/541 on combating terrorism.

quality assurance, as well as legal safeguards as regards independence, conflicts of interest, protection of privacy and personal data, as a non-exhaustive list. These safeguards are particularly important in the limited number of cases where platforms may remove content upon notification from the trusted flagger without further verifying the legality of the content themselves. In these limited cases, trusted flaggers could also be made auditable against these criteria, and a certification scheme could attest the trusted status. In all cases, sufficient safeguards should be available to prevent abuse of the system, as outlined in section 4.3.

Competent authorities should be offered the possibility to participate in the trusted-flagger reporting mechanisms, where relevant.

A reasonable balance needs to be struck between ensuring a high quality of notices coming from trusted flaggers, the scope of additional measures that companies would take in relation to trusted flaggers and the burden in ensuring these quality standards. Where there are abuses of trusted flagger mechanisms against established standards, the privilege of a trusted flagger status should be removed.

The Commission **encourages the close cooperation between online platforms and trusted flaggers. Notices from trusted flaggers should be able to be fast-tracked by the platform**. This cooperation should provide for mutual information exchange so as to evaluate and improve the removal process over time.

The Commission will further **explore**, in particular in dialogues with the relevant stakeholders, the **potential of agreeing EU-wide criteria for trusted flaggers**.

3.2.2. Notices by users

In the effective fight against illegal content online, ordinary users should be empowered to signal illegal content to online platforms and have confidence that justified notices will be considered and acted upon swiftly.

Online platforms should **establish an easily accessible and user-friendly mechanism that allows their users to notify** content considered to be illegal and which the platforms host.

Where the content is publicly available, such reporting mechanisms should also be available to the general public, without needing to be signed-in as a user. To improve the efficiency and accuracy of the assessment of potentially illegal content, such mechanism should allow for **easy notification by electronic means**.

The Commission's proposal on the revision of the Audiovisual Media Services Directive aims to create an obligation on video-sharing platform providers to establish and operate mechanisms for users to report or flag audio-visual content which may impair the physical, mental or moral development of minors, as well as content containing incitement to violence or hatred.

3.2.3. Ensuring the high quality of notices

Online platforms should **put in place effective mechanisms to facilitate the submission of notices that are sufficiently precise and adequately substantiated** to enable the platforms to take a swift

and informed decision about the follow-up. This should facilitate the provision of notices that contain an **explanation of the reasons** why the notice provider considers the content illegal and a clear indication of the **location** of the potentially illegal content (e.g. the URL address).

Such reporting mechanisms should be visible, easily accessible, **user-friendly and contextual**. They should also allow for **easy reporting** of different content types, e.g. by selection from a list of categories of reasons for which the content is considered illegal. Where technically feasible, elements such as allowing notifications to be made immediately in the context of first encounter of the material or offering the reuse of sign-in credentials can be used.

Such sufficiently substantiated and detailed notice enables the platform to find the potentially illegal content quickly, make a sound assessment of the illegality of the content, and act expeditiously where appropriate. The exact level of detail required by platforms to expeditiously take informed decisions can vary considerably from one type of content to the other.

Users should normally not be obliged to identify themselves when reporting what they consider illegal content, unless this information is required to determine the legality of the content (e.g., asserting ownership for intellectual property rights (IPR)). This is especially the case where their safety can be at risk or where revealing one's identity could have legal implications. Users should be encouraged to raise their notification via trusted flaggers, where these exist, whenever they wish to maintain anonymity vis-à-vis platforms.

However, **notice providers should have the opportunity to voluntarily submit their contact details** in a notification, in order to allow the online platform to ask for additional information or to inform the notice provider about any intended follow-up. In that case, the notice provider should receive a **confirmation of receipt** and a **communication indicating the follow-up given to the notification**.

A confirmation of receipt does not only avoid that the notice provider has to check whether his/her request has been followed-up on, but can also serve as evidence in judicial or out-of-court proceedings in accordance with the rules applicable to such proceedings.

3.3. Proactive measures by online platforms

3.3.1. Proactive measures and the liability exemption

Online platforms should, in light of their central role and capabilities and their associated responsibilities, **adopt effective proactive measures to detect and remove** illegal content online and not only limit themselves to reacting to notices which they receive. Moreover, for certain categories of illegal content, it may not be possible to fully achieve the aim of reducing the risk of serious harm without platforms taking such proactive measures.

The Commission considers that taking such voluntary, proactive measures **does not automatically lead to the online platform losing the benefit of the liability exemption** provided for in Article 14 of the E-Commerce Directive.

Firstly, this liability exemption is only available to providers of 'hosting' services who meet the conditions set out in Article 14 of that Directive; such service providers are those whose activities

consist of the storage of information at the request of third parties and which **do not play an active role** of such a kind as to give it knowledge of, or control over, that information.[33]

Recital 38 of the Commission's proposal for a Directive on copyright in the Digital Single Market of 14 September 2016 states in this regard: "*In respect of Article 14 [of the E-Commerce Directive], it is necessary to verify whether the service provider plays an active role, including by optimising the presentation of the uploaded works or subject-matter or promoting them, irrespective of the nature of means used therefore*".

Specifically in respect of Article 14 of the E-Commerce Directive, in the case L'Oréal v eBay, the Court of Justice clarified that "*the mere fact that [an online 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 exemptions from liability provided for by [Article 14 of the E-Commerce Directive]*".[34] However, there is such an effect, the Court ruled, "*[w]here, by contrast, the [online platform] has provided assistance which entail, in particular optimising the presentation of the offers for sale in question or promoting those offers*".[35]

This suggests that the mere fact that an online platform takes certain measures relating to the provision of its services in a general manner does not necessarily mean that it plays an active role in respect of the individual content items it stores and that the online platform cannot benefit from the liability exemption for that reason. In the view of the Commission, such measures can; and indeed should, also include proactive measures to detect and remove illegal content online, particularly where those measures are taken as part of the application of the terms of services of the online platform. This will be in line with the balance between the different interests at stake which the E-Commerce Directive seeks to achieve.[36] Indeed, it recalls that it is in the interest of all parties involved to adopt and implement rapid and reliable procedures for removing and disabling access to illegal information.[37] Although that Directive precludes online platforms from being obliged to engage in general active fact-finding,[38] it also acknowledges the importance of voluntary measures.[39]

Secondly, in accordance with Article 14 of the E-Commerce Directive service providers falling within the scope of that provision can only benefit from the liability exemption on **two conditions**, namely: (a) they do not have actual knowledge of the illegal activity or information and, as regards claims for damages, are not aware of facts or circumstances from which the illegal activity or information is apparent or (b), upon obtaining such knowledge or awareness, they act expeditiously to remove or to disable access to the information.

---

[33] Recital 42 of the E-Commerce Directive. See Google France, 114 and 120; Judgment of 12 July 2011, Case C‑324/09, L'Oréal v eBay, para. 113.
[34] eBay 115
[35] eBay 116
[36] Recital 41 of the E-Commerce Directive.
[37] Recital 40 of the E-Commerce Directive.
[38] Article 15(1) of the E-Commerce Directive.
[39] Recital 40 of the E-Commerce Directive.

The Court of Justice has clarified that these conditions cover "*every situation in which the [online platform] concerned becomes aware, in one way or another, of [facts and circumstances on the basis of which a diligent economic operator should have identified the illegality in question]*" and that this includes – besides notification by a third party – the situation where the platform "*uncovers, as the result of an investigation undertaken on its own initiative, an illegal activity or illegal information*".[40]

It follows that proactive measures taken by an online platform to detect and remove illegal content may result in that platform obtaining knowledge or awareness of illegal activities or illegal information, which could thus lead to the loss of the liability exemption in accordance with point (a) of Article 14(1) of the E-Commerce Directive. However, in such cases the online platform continues to have the possibility to act expeditiously to remove or to disable access to the information in question upon obtaining such knowledge or awareness. Where it does so, the online platform continues to benefit from the liability exemption pursuant to point (b) of Article 14(1). Therefore, concerns related to losing the benefit of the liability exemption should not deter or preclude the application of the effective proactive voluntary measures that this Communication seeks to encourage.

3.3.2. Using technology to detect illegal content

Given the volume of material intermediated by online platforms, as well as technological progress in information processing and machine intelligence, the **use of automatic detection and filtering technologies** is becoming an ever more important tool in the fight against illegal content online. Many large platforms are now making use of some form of matching algorithms, based on a range of technologies, from simple metadata filtering, to hashing and fingerprinting content.

The E-Commerce Directive clarifies that the provisions relating to liability do not preclude the development and effective operation of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology.[41] As the Directive also makes clear, such operation must however take place within the limits of the applicable rules of EU and national law, in particular on the protection of privacy and personal data and the prohibition on Member States to impose general monitoring obligations.[42]

Sector-specific legislations can set mandatory rules for online platforms to take measures e.g. on copyright to help ensure the detection and removal of illegal content, also when they are eligible for the liability exemption provided in Article 14 of the E-Commerce Directive.

More generally, the use and further development of such technology is encouraged in particular when serious harm is at stake, as called for by European Council Conclusions on 22 June 2017[43]. Automatic tools and filters can be used to identify potentially infringing content and private and

[40] eBay 120-121
[41] Recital 40 of the E-Commerce Directive.
[42] Recital 40 and Article 15(1) of the E-Commerce Directive.
[43] http://www.consilium.europa.eu/en/press/press-releases/2017/06/22-euco-security-defence/

public research is advancing in developing such tools. For instance, in the field of copyright, automatic content recognition has proven an effective tool for several years.

The **Commission supports further research and innovative approaches** going beyond the state of the art with the objective of improving the accuracy of technical means to identify illegal content[44]. It also **encourages industry to ensure an effective uptake of innovations which may contribute to increased efficiency and effectiveness of automatic detection procedures**.

In most cases, current best industry practice is to use automatic tools to narrow down the set of contentious content for vetting by human experts, who then may need to assess the illegal nature of such content. This human-in-the-loop principle is, in general, an important element of automatic procedures that seek to determine the illegality of a given content, especially in areas where error rates are high or where contextualisation is necessary.

The Commission is of the view that proactive measures taken by those online platforms which fall under Article 14 of the E-commerce Directive to detect and remove illegal content which they host – including the use of automatic tools and tools meant to ensure that previously removed content is not re-uploaded – **do not in and of themselves lead to a loss of the liability exemption**.

In particular, the taking of such measures need not imply that the online platform concerned plays an active role which would no longer allow it to benefit from that exemption. Whenever the taking of such measures lead to the online platform obtaining actual knowledge or awareness of illegal activities or illegal information, it needs to act expeditiously to remove or to disable access to the illegal information in question to satisfy the condition for the continued availability of that exemption.

Online platforms should do their utmost to proactively detect, identify and remove illegal content online. The Commission strongly encourages online platforms to use voluntary, proactive measures aimed at the detection and removal of illegal content and to step up cooperation and investment in, and use of, automatic detection technologies

4. REMOVING ILLEGAL CONTENT

It is in the entire society's interest that **platforms should remove illegal content as fast as possible**. At the same time, removal of such content **should not impede the prosecution of or other follow-up to any underlying breach of law**. Evidence sharing amongst public authorities and online platforms is an important policy in this regard. Cross-border access to evidence should be facilitated by the

[44] Current R&I efforts deployed by industry are directed towards the development of analytical tools for a better understanding of natural language, information cascades in social networks, the identification of sources of information, dissemination patterns and fake identities. The Commission has also supported R&I in this field by funding projects aimed at developing automatic verification tools to check the veracity of user generated content on social networks. These tools may help the identification of potential falsehoods in texts, images or videos and support the tracking of fake news. However the establishment of the illegal nature of such content goes beyond their current functional capabilities.

forthcoming legislative initiative on this issue[45]. The removal of illegal content by platforms should not affect investigations into or the prosecution of offences based on Union or national law.

Robust safeguards to limit the risk of removal of legal content also should be available, supported by a set of meaningful transparency obligations to increase accountability of the removal processes.

4.1. Ensuring expeditious removal and reporting crime to law enforcement authorities

The E-Commerce Directive requires online platforms to act "expeditiously" to remove illegal content after they have obtained knowledge thereof, if they wish to continue to benefit from the liability exemption. What this means in practice depends on the specifics of the case at hand, in particular the type of illegal content, the accuracy of the notice and the potential damage caused.

In practice, different content types require a different amount of contextual information to determine the legality of a given content item. For instance, while it is easier to determine the illegal nature of child sexual abuse material, the determination of the illegality of defamatory statements generally requires careful analysis of the context in which it was made.

Where serious harm **is at stake, for instance in cases of incitement to terrorism acts, fast removal is particularly important and can be subject to specific timeframes.**

Some voluntary processes such as the Code of Conduct on countering illegal hate speech online have provided indicative targets for removal times, in the case of this Code of Conduct, 24 hours for the majority of cases.

Fully automated deletion or suspension of content can be particularly effective and should be applied where the circumstances leave little doubt about the illegality of the material, e.g. in cases of material whose removal is notified by law enforcement authorities, or of known illegal content which has previously been removed subject to the safeguards referred to in Section 4.3.

As a general rule, **removal deriving from trusted flagger notices should be addressed more quickly**, due to the quality and accuracy of the information provided in the notice and the trusted status of the flaggers.

In cases where economic damage is at stake due to infringing intellectual property right, the potential economic damage arising from such an infringement may be closely related to the speed of its removal.

Clear reporting by platforms about the time taken for processing takedown requests according to the type of content will facilitate the assessment of the expeditiousness of the action taken and increase the wider accountability of platforms.

In certain cases, especially where online platforms find it difficult to assess the legality of a particular content item and it concerns a potentially contentious decision, they could benefit from submitting

[45] See https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en and https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en for more information.

cases of doubt to a third party to obtain advice. Self-regulatory bodies or competent authorities play this role in different Member States. As part of the reinforced cooperation between online platforms and competent authorities, such cooperation is strongly encouraged.

Finally **online platforms should report to law enforcement authorities** whenever they are made aware of or encounter evidence of criminal or other offences in order to alert and enable the relevant authorities to investigate and prosecute individuals generating such content or the abuse of the services by organised criminal or terrorist groups. In doing so, they should comply with the applicable legal requirements, including Regulation (EU) 2016/679 on the protection of personal data[46]., This may also be appropriate in cases of offers and sales of products and commercial practices that are non-compliant with EU legislation.

The need to cooperate with law enforcement authorities in the investigation and prosecution of crimes may also in some cases lead to platforms abstaining from removing the illegal content at hand, when this is required in the framework of a specific investigation underway, under close supervision by national authorities and in full compliance with national criminal procedure rules.

Law enforcement authorities should build up the necessary capacity to take appropriate action on these reports.[47] A best practice example concerning points of contact is the SIRIUS portal[48] established by Europol to support Member States in online counter terrorism investigations, including facilitating co-operation between platforms and EU law enforcement [49]

In accordance with Article 14 of the E-Commerce Directive, online platforms must take down illegal content expeditiously once they are made or become aware of its existence if they wish to be exempt from liability. Particularly fast removal is important in the case of illegal content where serious harm is at stake, for instance in cases of incitement to terrorism acts. Removal times and procedure for different forms of illegal content should be clearly reported in transparency reports.

The issue of fixed timeframes for removal will be further analysed by the Commission.

Evidence of criminal offences obtained in the context of illegal content removal should be transmitted to law enforcement authorities, provided this is in compliance in particular with the requirements laid down in Regulation (EU) 2016/679, especially the lawful grounds for processing personal data.

[46] Article 6(1)(c) in conjunction with Article 6(4).

[47] According to Article 15(2) of the E-Commerce Directive, "Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."

[48] Shaping Internet Research Investigations Unified System

[49] Europol will further facilitate the creation of new Single Point of Contacts by providing relevant trainings to law enforcement authorities in countries where SPOCs are not yet established.

4.2. Enhancing transparency

4.2.1. Transparency on the online platforms' content policy

The question of whether content is legal or illegal is governed by EU and national laws. At the same time the online platforms' own terms of service can consider specific types of content undesirable or objectionable.

Online platforms should disclose their detailed content policies in their terms of service and clearly communicate this to their users. These terms should not only define the policy for removing or disabling access to content, but also spell out the safeguards that ensure that content-related measures do not lead to over-removal. In particular, online platforms' terms of service should clearly spell out any possibility for the users to contest removal decisions as part of an enhanced transparency of the platforms' general removal policies. This should help reduce the potential negative effect on the users' fundamental right to freedom of expression and information.[50]

Online platforms should provide a **clear, easily understandable and sufficiently detailed explanation of their content policy in their terms of service**. These should reflect both the treatment of illegal content, and content which does not respect the platform's terms of service. All restrictions on the kind of content permitted on a particular platform should be clearly stated and communicated to their users. This explanation should also cover the procedures in place to contest removal decisions, including those triggered by trusted flaggers.

4.2.2. Transparency on notice-and-action procedures

Transparency reporting should also cover the *outcome* of the application of the platforms' content management policies.

Online platforms should **publish transparency reports** with sufficiently detailed **information on the number and type of notices received and actions taken**, as well as the **time taken for processing,** and the source of the notification[51]. These reports should also include information on **counter notices**, if any, and the response given to these. The Commission encourages the publication of this information on a regular basis and at least once per year.

Taking due account of content-specific differences, these transparency reports would benefit from some **standardisation** across the Digital Single Market. This would allow for better monitoring, facilitate the electronic aggregation of such information and could help avoid unnecessary barriers to the cross-border provision of hosting services.

Special attention should be paid to enable smaller online platforms and SMEs to provide such transparency data, and any supporting activity such as standardisation should ensure that administrative burdens are kept to a minimum.

[50] In case personal data are being processed, platforms shall ensure transparent privacy policies according to Article 12 of the General Data Protection Regulation.

[51] Reporting on own investigations, general user notices, notices by law enforcement authorities, etc.

The Commission will further **explore**, in structured dialogues with the industry, **the potential of standardisation** with regard to notification procedures and transparency reporting about removal systems and outcomes.

4.3. Safeguards against over-removal and abuse of the system

Expeditious action, including upload-filtering measures or automated detection aimed at ensuring the prompt removal of illegal content, in particular where there is no "human in the loop", can affect the accuracy of the decision, including the risk that legal content is removed. Therefore it is important to ensure that sufficient safeguards are available so that content which was erroneously removed can be reinstated.

4.3.1. Contesting a notice

In general, those who provided the content should be **given the opportunity to contest this decision via a counter-notice**. This is also valid when content removal has been automated.

For example, according to Article 28a of the proposal to amend the AVMSD, Member States have to ensure that complaint and redress mechanisms are available for the settlement of disputes between users and video-sharing platforms relating to the application of the appropriate measures to be taken by those platforms.

If the counter-notice has provided reasonable grounds to consider that the notified activity or information is not illegal, **the platform provider should restore the content that was removed without undue delay or allow for the re-upload by the user, without prejudice to the platform's terms of service**.

The possibility to contest decisions should lead to a decrease in the number of unjustified removals of legal content and could equally supply documentary evidence for out-of-court dispute resolution mechanisms or to judicial appeal procedures.

In certain circumstances, informing the content provider and/or allowing for a counter-notice would not be appropriate – in particular in cases where this would interfere in the investigative powers of Member States' authorities necessary for the prevention, detection and prosecution of criminal offences, such as in the case of child sexual abuse material.

Online platform should offer simple online counter-notice procedures. When a counter-notice is filed, online platforms should provide a reply, and in case of a negative decision the reasons should be specified. When available in the Member State concerned, platforms are encouraged to allow the use of out-of-court dispute settlement bodies to resolve disputes about counter-notices.

4.3.2. Measures against bad-faith notices and counter-notices

At the same time, notice-and-action procedures can sometimes be abused with bad practices or in bad faith[52]. These practices should be strongly discouraged, for instance by demoting the treatment in priority of notices from a notice provider who sends a high rate of invalid notices or receives a high number of counter-notices, or by revoking the trusted flagger status, according to well-established and transparent criteria. These policies should also be clearly described in the terms of service of an online platform, and be part of the general transparency reporting of online platforms, to increase public accountability. Similar measures should be put in place regarding abusive counter-notices.

5. PREVENTING THE RE-APPEARANCE OF ILLEGAL CONTENT

Illegal content, once detected and taken down, should not re-appear online. Efficient and effective prevention of re-appearance based on existing good practices as well as on appropriate safeguards is essential to a well-functioning system. Preventing known illegal material from being disseminated across platforms requires closer co-operation between online service providers, in full respect of the applicable rules of competition law. It is also important to increase the cooperation by law enforcement authorities with small, less resilient companies, who may become the preferred platform of choice by criminals and other persons involved in infringing activities online if they are deemed more vulnerable than others.

5.1. Measures against repeat infringers

In order to avoid the re-appearance of illegal content by users posting infringing content of the same nature over and over, many online platforms have already put in place measures against repeat infringers, such as the suspension or termination of accounts or shadow-banning measures.[53]

Online platforms should take measures which dissuade users from repeatedly uploading illegal content of the same nature and aim to effectively disrupt the dissemination of such illegal content.

This should also apply where the infringer is the same and the substance of the content in question is of the same nature and, where justified, the user has been promptly notified about the notice(s) received against him/her and about the forthcoming suspension or termination. This would allow the user to contest the decision and facilitate access to judicial redress against the measure, if appropriate under the contract between the user and the platform and the applicable law. In such cases, too, any processing of personal data must fully respect the relevant data protection rules.

Once again, no information or notification of the content provider should be provided where this would interfere in the investigative powers of Member States necessary for the prevention, detection and prosecution of criminal offences, when the necessary legal basis is provided.

---

[52] Evidence suggest that such information is used by competitors (*Notice and Takedown in Everyday Practice,* J Urban *et al.,* UC Berkeley, 2016), and that the practice of automated creation of notices has been abused to link to artificially created content (Google Transparency report).

[53] "Shadow banning" is the act of blocking a user from an online community such that the user does not realise that they have been banned.

5.2. **Automatic re-upload filters**

Besides the technologies used to identify potentially illegal content mentioned in Section 3.3, technological tools can be used with a higher degree of reliability to fingerprint and filter out (take down and stay down) content which has been already identified and assessed as illegal. The Commission therefore strongly encourages the further use of such tools subject to safeguards such as reversibility and exceptions as outlined below.

This is what currently takes place with the "Database of Hashes" being used in relation to terrorist content developed under the EU Internet Forum, or in the field of copyright, or for child sexual abuse material, but also for products which have been flagged by law enforcement authorities as non-compliant with relevant legislation. These practices have shown good results. However, their effectiveness depends on further improvements to limit erroneous identification of content and to facilitate context-aware decisions, as well as the necessary reversibility safeguards.

For instance, basing itself on practice in the field of copyright in the area of automatic content recognition, the Commission proposal on copyright in the Digital Single Market recognises such technologies – as long as they are appropriate and proportionate – as a possible means, *inter alia*, of preventing the availability of non-licensed content on the relevant online services.

Automatic stay-down procedures should allow for context-related exceptions and when content that has been removed is changed and brought into conformity with legal or other requirements.The scope and timing of context-related exceptions should take into account the specific nature of the content and any related security threat, as well as the possibility of temporarily suspending such content pending a more in-depth appraisal.

The Commission strongly encourages the further **use and development of automatic technologies to prevent the re-appearance of illegal content online.**

Where automatic tools are used to prevent re-appearance of illegal content a reversibility safeguard should be available for erroneous decisions, and the use and performance of this technology should be made transparent in the platforms' terms of service.

Access to databases that are used to automatically match and identify reappearing illegal content should be available to all online platforms, subject to compliance of any processing operation with applicable legislation on the protection of personal data and competition. Privacy policies of companies should include transparent information on processing of personal data in case of such databases.

Online platforms should also ensure continuous update of their tools, to ensure all illegal content is captured, in line with changing tactics and behaviour of criminals and other persons involved in infringing activities online. In the case of tools used for terrorist content, these should be adapted to capture new and historical content, ensure its swift review and removal. Such content should be added to cross-platform tools, such as the mentioned Database of Hashes (currently being used in relation to terrorist content). Such technological development should be carried out in cooperation between online platforms, competent authorities and other stakeholders, including civil society.

6. CONCLUSIONS

The increase in illegal content hosted by online platforms creates real harm in society, including risks to our citizens' integrity, dignity and health; if not properly addressed, such harm will also undermine trust in digital services more broadly speaking, and ultimately in the Digital Single Market – a key engine of innovation, growth and jobs. Even if such content is created and uploaded by third parties, the constantly rising influence of online platforms in society, which flows from their role as gatekeepers to content and information, increases their responsibilities towards their users and society at large. They should therefore be proactive in weeding out illegal content, preventing its reappearance, put effective notice-and-action procedures in place, and establish well-functioning interfaces with third parties (such as trusted flaggers) and give a particular priority to notices from national law enforcement authorities. Where online platforms decide which content should be considered illegal, in accordance with the law, adequate checks-and-balances should be put in place.

This Communication provides guidance and does not as such change the applicable legal framework or contain legally binding rules; it primarily aims to guide online platforms on the ways in which they can live up to their responsibility as regards tackling the illegal content they host. It also aims to mainstream good procedural practices across different forms of illegal content, to promote closer cooperation between platforms and competent authorities. As such it outlines a European approach to address illegal content for online platforms, combining the need for fast and effective removals of illegal content and prevention and prosecution of crimes with safeguarding the right to free speech online. This guidance will complement and reinforce the ongoing sector-specific dialogues.

Special attention should be given to ensure that smaller online platforms are able to implement such procedures, and many elements of this Communication have been conceived bearing in mind their specific needs. Nonetheless, the Commission will explore further means to support take-up of the guidance for smaller platforms, too.

The Digital Single Market requires greater coherence of public policy responses across geographical borders. With this Communication, the Commission is therefore, as a first step, providing common tools to address the shared challenge of illegal content removal.

The letter of intent of 13 September 2017 by the President of the European Commission, addressed to the President of the European Parliament and the President of the Council of the European Union, in order to ensure an area of Justice and Fundamental Rights based on mutual trust announced further measures to ensure the swift and proactive detection and removal of illegal content inciting hatred, violence and terrorism. This Communication constitutes a first element of such measures. The Commission expects online platforms to take swift action over the coming months, including in the context of relevant dialogues, in particular in the area of terrorism and illegal hate speech.

The Commission will continue exchanges and dialogues with online platforms and other relevant stakeholders. It will monitor progress and assess whether additional measures are needed, in order to ensure the swift and proactive detection and removal of illegal content online, including possible legislative measures to complement the existing regulatory framework. This work will be completed by May 2018.